to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2709. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2710. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2711. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2712. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2713. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2714. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2716. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2717. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2718. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2719. Mr. KOHL (for himself, Mr. WHITEHOUSE, and Mr. COONS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2720. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2721. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2722. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2723. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2724. Ms. MIKULSKI submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2725. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2726. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2727. Mr. BLUMENTHAL (for himself, Mr. SCHUMER, Ms. KLOBUCHAR, Mr. WYDEN, Mr. AKAKA, Mr. SANDERS, and Mrs. SHAHEEN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2728. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2729. Mr. WARNER (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2731. Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) proposed an amendment to the bill S. 3414, supra.

SA 2732. Mr. REID (for Mr. FRANKEN) proposed an amendment to amendment SA 2731 proposed by Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) to the bill S. 3414, supra.

SA 2733. Mr. REID proposed an amendment to the bill S. 3414, supra.

SA 2734. Mr. REID proposed an amendment to amendment SA 2733 proposed by Mr. REID to the bill S. 3414, supra.

SA 2735. Mr. REID proposed an amendment to the bill S. 3414, supra.

SA 2736. Mr. REID proposed an amendment to amendment SA 2735 proposed by Mr. REID to the bill S. 3414, supra.

SA 2737. Mr. REID proposed an amendment to amendment SA 2736 proposed by Mr. REID to the amendment SA 2735 proposed by Mr. REID to the bill S. 3414, supra.

SA 2738. Ms. SNOWE (for herself and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2739. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2740. Mr. LIEBERMAN (for Mr. NELSON of Florida) proposed an amendment to the resolution S. Res. 525, honoring the life and legacy of Oswaldo Paya Sardinas.

SA 2741. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table.

SA 2742. Mr. TESTER submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2665. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. LIMITATION ON REGULATIONS.

(a) IN GENERAL.—The head of a Federal agency may not issue regulations, standards, or practices that are applicable to the private sector under this Act or an amendment made by this Act until after the date on which the Comptroller General of the United States submits to Congress a report stating that the information infrastructure of the Federal agency is in compliance with the regulations, standards, or practices.

(b) GAO REVIEW.—Upon request by the head of a Federal agency, the Comptroller General of the United States shall—

(1) review the information infrastructure of the Federal agency to determine whether the information infrastructure is in compliance with proposed regulations, standards, or practices; and

(2) submit to Congress a report regarding the conclusion of the review under paragraph (1).

SA 2666. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 8, after line 22, insert the following:

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b)(2), this Act and the amendments made by this Act shall not take effect until 60 days after the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act.

(b) CBO SCORE.—

(1) REPORT.—The Congressional Budget Office shall submit to Congress a report regarding the budgetary effects of this Act.

(2) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date of enactment of this Act

(c) PUBLIC HEARINGS.—Not later than 60 days after the date on which the Congressional Budget Office submits the report described in subsection (b)(1) to Congress, the head of each agency with responsibility for regulating the security of critical infrastructure under this Act shall hold a public hearing to allow members of the public and industry to comment on the impact of the budgetary effects of this Act.

SA 2667. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 8, after line 22, insert the following:

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b)(2), this Act and the amendments made by this Act shall not take effect until—

(1) the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act; or

(2) if the report regarding the budgetary effects submitted under subsection (b)(1) determines that the cost of this Act is more than $100,000,000, 60 days after the date on which the determination is published in the Federal Register under subsection (b)(1)(B).

(b) CBO SCORE.—

(1) REPORT.—The Congressional Budget Office shall—

(A) submit to Congress a report regarding the budgetary effects of this Act; and

(B) if the report regarding the budgetary effects described in subparagraph (A) determines that the cost of this Act is more than $100,000,000, publish such determination in the Federal Register and allow public comment during the 60-day period beginning on the date on which such determination is published.

(2) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date of enactment of this Act.

SA 2668. Mr. RUBIO (for himself, Mrs. MCCASKILL, Mr. TOOMEY, Mr. BARRASSO, Ms. AYOTTE, Mrs. SHAHEEN, and Mr. UDALL of New Mexico) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance

the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 165, line 21, strike ''of the United States, including'' and all that follows through line 23 and insert the following:
of the United States.

(b) ADDITIONAL SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) Given the importance of the Internet to the global economy, it is essential that the Internet remain stable, secure, and free from government control.

(B) The world deserves the access to knowledge, services, commerce, and communication, the accompanying benefits to economic development, education, and health care, and the informed discussion that is the bedrock of democratic self-government that the Internet provides.

(C) The structure of Internet governance has profound implications for competition and trade, democratization, free expression, and access to information.

(D) Countries have obligations to protect human rights, which are advanced by online activity as well as offline activity.

(E) The ability to innovate, develop technical capacity, grasp economic opportunities, and promote freedom of expression online is best realized in cooperation with all stakeholders.

(F) Proposals have been put forward for consideration at the 2012 World Conference on International Telecommunications that would fundamentally alter the governance and operation of the Internet.

(G) The proposals, in international bodies such as the United Nations General Assembly, the United Nations Commission on Science and Technology for Development, and the International Telecommunication Union, would attempt to justify increased government control over the Internet and would undermine the current multistakeholder model that has enabled the Internet to flourish and under which the private sector, civil society, academia, and individual users play an important role in charting its direction.

(H) The proposals would diminish the freedom of expression on the Internet in favor of government control over content.

(I) The position of the United States Government has been and is to advocate for the flow of information free from government control.

(J) This and past Administrations have made a strong commitment to the multistakeholder model of Internet governance and the promotion of the global benefits of the Internet.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of State, in consultation with the Secretary of Commerce, should continue working to implement the position of the United States on Internet governance that clearly articulates the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today.

SA 2669. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 154, strike line 9 and all that follows through page 156, line 13.

SA 2670. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike paragraph (10) of section 707(a).

SA 2671. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 124, strike line 7 and all that follows through page 128, line 14.

SA 2672. Mr. BROWN of Massachusetts submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 115, between lines 8 and 9, insert the following:

''(10) assist the development and demonstration of technologies designed to increase the security and resiliency of the electricity transmission and distribution grid;

SA 2673. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CAPPING AND REDUCING THE BALANCE SHEET OF THE FEDERAL RESERVE SYSTEM.

(a) IN GENERAL.—Notwithstanding any other provision of law, no action may be taken by the Board of Governors of the Federal Reserve System or the Federal Open Market Committee on or after the date of enactment of this Act that would result in the total of the factors affecting reserve balances of depository institutions exceeding the balance as of July 27, 2012.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the Federal Reserve System should expeditiously take substantial steps to reduce the size of its balance sheet to levels below those that prevailed prior to the financial crisis of 2008.

SA 2674. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. REPEAL OF DODD-FRANK ACT.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111–203) is repealed, and the provisions of law amended by such Act are revived or restored as if such Act had not been enacted.

SA 2675. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 2645 submitted by Mr. BINGAMAN and intended to be proposed to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

In lieu of the matter proposed to be inserted, insert the following:

SEC. ___. EMERGENCY AUTHORITY RELATING TO CYBER SECURITY THREATS.

Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding at the end the following:

''SEC. 224. EMERGENCY AUTHORITY RELATING TO CYBER SECURITY THREATS.

''(a) DEFINITIONS.—In this section:

''(1) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

''(2) CYBER SECURITY THREAT.—The term 'cyber security threat' means the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

''(3) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

''(b) EMERGENCY AUTHORITY OF SECRETARY.—

''(1) IN GENERAL.—If the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat, the Secretary may require, by order, with or without notice, persons subject to the jurisdiction of the Commission to take such actions as the Secretary determines will best avert or mitigate the cyber security threat.

''(2) COORDINATION WITH CANADA AND MEXICO.—In exercising the authority granted under this subsection, the Secretary is encouraged to consult and coordinate with the appropriate officials in Canada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

''(3) CONSULTATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with any entity that owns, controls, or operates critical electric infrastructure and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security threat.

''(4) COST RECOVERY.—The Commission shall establish a mechanism that permits public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary under this subsection.

''(c) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any order issued by the Secretary under subsection (b) shall remain effective for not more than 90 days unless, during the 90 day-period, the Secretary—

''(1) gives interested persons an opportunity to submit written data, views, or arguments; and

''(2) affirms, amends, or repeals the rule or order.''.

SA 2676. Ms. MURKOWSKI submitted an amendment intended to be proposed

by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 153, strike line 15 and all that follows through page 154, line 8, and insert the following:

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

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, the Secretary, the Director of National Intelligence, and the electric sector coordinating council shall submit to Congress a report on—

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

(2) the existing standards, alerts, and mitigation strategies in place;

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

(4)(A) the interdependency of critical infrastructures; and

(B) the options available to the United States and private sector entities to reconstitute—

(i) as soon as practicable after the disruption, electrical service to provide for the national security of the United States; and

(ii) within a reasonable time frame after the disruption, all electrical service within the United States; and

(5) a plan, building on existing efforts, to prevent disruption of the electric grid of the United States caused by a cyber attack.

(b) REQUIREMENTS.—In preparing the report under subsection (a), the Secretary of Energy shall use any existing studies or reports to avoid duplication of effort.

SA 2677. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 166, line 19, strike ''coordinate'' and insert ''collaborate''.

On page 166, line 23, strike ''to develop'' and insert ''on''.

On page 166, beginning on line 24, strike ''cyberspace, cybersecurity, and cybercrime issues'' and insert ''cyber issues''.

On page 167, line 11, after ''State'' insert ''and the Attorney General''.

On page 168, line 15, after ''State'' insert ''and the Attorney General''.

On page 168, line 17, after ''State'' insert ''and the Attorney General''.

SA 2678. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 91, between lines 12 and 13, insert the following:

''(16) PROTECT.—The term 'protect' means the action of securing, defending, or reducing the vulnerabilities of an information system, or otherwise enhancing information security or the resiliency of information systems or assets.

''(17) PROTECTION.—The term 'protection' means the actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, or otherwise enhance information security or the resiliency of information systems or assets.

''(18) RESPOND AND RESPONSE.—The terms 'respond' and 'response' in relation to cybersecurity threats, vulnerabilities, or incidents do not include directing cybersecurity threat and incident law enforcement investigations or prosecutions.

On page 95, line 10, strike ''security'' and insert ''protection''.

On page 99, after line 25, insert the following:

''(m) LAW ENFORCEMENT AND INTELLIGENCE AUTHORITIES.—Nothing in this section shall be construed to alter or amend the law enforcement or intelligence authorities of any Federal agency.

SA 2679. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

SEC. 416. REPORT ON FEDERAL LAW ENFORCEMENT CYBERSECURITY AND CYBERCRIME RESOURCES.

(a) DEFINITIONS.—In this section—

(1) the term ''covered law enforcement agency'' means each law enforcement component of—

(A) the Department of Justice; and

(B) the Department of Homeland Security; and

(2) the term ''mission'' means the portion of a cybersecurity mission that encompasses law enforcement and intelligence activities.

(b) REPORT.—

(1) IN GENERAL.—The Attorney General shall enter into a contract with the National Research Council, or another federally funded research and development corporation, under which the National Research Council or other corporation shall submit to Congress a report on the current and optimal level and structure of cybersecurity and cybercrime resources of each covered law enforcement agency.

(2) CONTENTS.—The report described in paragraph (1) shall—

(A) identify the elements of the mission of each covered law enforcement agency;

(B) describe the challenges involved in the mission of each covered law enforcement agency, including—

(i) any challenges in cybercrime prosecutions, such as the need for advanced forensics expertise and resources;

(ii) the complexity of relevant Federal laws, State laws, international laws, and treaty obligations of the United States;

(iii) the need to coordinate with members of the intelligence community;

(iv) the need to protect classified or sensitive information while abiding by relevant law regarding the disclosure of exculpatory evidence and other discoverable information to a criminal defendant; and

(v) any other challenges that the report may identify;

(C) identify the current resources brought to bear by each covered law enforcement agency in pursuing the mission of that agency, differentiating between—

(i)(I) personnel who focus exclusively on supporting the mission; and

(II) personnel who hold multiple or competing responsibilities;

(ii)(I) operational personnel; and

(II) personnel who hold primarily management, policy making, or support responsibilities;

(iii)(I) personnel working at headquarters; and

(II) personnel working in the field; and

(iv)(I) personnel with specialized training and duties relating to national cybersecurity; and

(II) personnel with general technical training;

(D) identify areas in which the level and structure of current resources is inadequate for any covered law enforcement agency to perform the mission of that agency;

(E) identify the optimal level of resources that would enable each covered law enforcement agency to perform the mission of that agency most effectively without unnecessary government waste;

(F) identify the optimal structure of the cybersecurity and cybercrime resources of each covered law enforcement agency, considering existing models within—

(i) the Department of Justice, including task forces and strike forces; and

(ii) agencies such as the Drug Enforcement Administration and the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and

(G) evaluate the future or developing needs of each covered law enforcement agency, including the resources that the agency will need to perform the mission of that agency in the future.

(3) TIMING.—The contract entered into under paragraph (1) shall require that the report described in this subsection be submitted not later than 1 year after the date of enactment of this Act.

SA 2680. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VI, insert the following:

SEC. 606. RULE OF CONSTRUCTION.

Nothing in this Act may be construed as authorizing the President to enter the United States into a treaty or binding international agreement on cybersecurity unless such treaty or agreement is approved with the advice and consent of the Senate pursuant to Article II, section 2, clause 2 of the Constitution.

SA 2681. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 46, strike line 6 and all that follows through page 57, line 3, and insert the following:

''(4) provide a mechanism to improve and continuously monitor the security of agency information security programs and systems, subject to the protection of the privacy of individual or customer-specific data, through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''SEC. 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 agency information system continue to be effective over time in light of rapidly changing information technology and threat development. To the maximum extent possible, subject to the protection of the privacy of individual or customer-specific data, 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 agency information or an agency 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 agency 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.

''SEC. 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 agency information systems;

''(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);

''(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); and

''(10) with respect to continuous monitoring reporting, allow operators of agency information systems to use processes that will protect the privacy of individual or nongovernment customer specific data.

''(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, unless the head of an agency determines within a reasonable time, and reports to the President, that such acquisition, interception, retention, use, or disclosure is contrary to the public interest and would seriously undermine important agency goals, activities, or programs.

''(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 cybersecurity crime that has been, is being, or is about to be committed; and

---

SA 2682. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. ANNUAL REPORT ON FOREIGN GOVERNMENT SPONSORS OF ECONOMIC OR INDUSTRIAL ESPIONAGE.

(a) IN GENERAL.—Subject to subsection (c), not later than 180 days after the date of enactment of this Act, and annually thereafter, the National Counterintelligence Executive shall submit to Congress, the President, the National Security Council, the Secretary of State, the Secretary of Defense, the Secretary of the Treasury, and the Secretary of Commerce—

(1) an unclassified report that contains a list of foreign governments that the National Counterintelligence Executive determines engage in, sponsor, or condone economic or industrial espionage against United States businesses or other persons; and

(2) a classified report that includes—

(A) the report submitted under paragraph (1); and

(B) the information upon which the determinations of the National Counterintelligence Executive under paragraph (1) are based.

(b) INFORMATION.—In preparing a report under subsection (a), the National Counterintelligence Executive shall rely primarily on information available to the United States Government.

(c) REVIEW BY SECRETARY OF STATE.—

(1) SUBMISSION OF REPORT FOR REVIEW.—Not later than 30 days before the date on which the National Counterintelligence Executive submits a report required under subsection (a), the National Counterintelligence Executive shall submit the report to the Secretary of State.

(2) FEEDBACK.—The Secretary of State may provide feedback to the National Counterintelligence Executive with respect to a report submitted to the Secretary of State under paragraph (1).

(3) DELAY.—Upon the request of the Secretary of State, the National Counterintelligence Executive shall delay the submission of a report under subsection (a) for a period of not more than 60 days.

SA 2683. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title V, add the following:

SEC. 503. DEPARTMENT OF DEFENSE PROVISION FOR THE COMMON DEFENSE OF FEDERAL INFORMATION INFRASTRUCTURE IN FEDERAL CYBER EMERGENCIES.

(a) AUTHORITY FOR PRESIDENT TO DIRECT.—The President shall have the authority to direct the Department of Defense to provide for the common defense of Federal information infrastructure in the event of a Federal cyber emergency.

(b) FEDERAL CYBER EMERGENCY.—For purposes of this section, a Federal cyber emergency is an incident that threatens the viability of Federal information infrastructure necessary for maintaining critical Federal government functions or operations.

(c) SCOPE.—The authorities exercised by the Department of Defense pursuant to subsection (a) may, as directed by the President under that subsection, including the authorities in section 3553 of title 44, United States Code (as amended by section 201 of this Act).

(d) DURATION OF AUTHORITY.—Any direction of the Department of Defense to provide for the common defense of Federal information infrastructure in the event of a Federal cyber emergency under subsection (a) shall be for such period, not to exceed seven days, as the President shall direct under that subsection.

(e) NOTICE TO CONGRESS.—The President shall notify Congress immediately upon directing the Department of Defense to provide for the common defense of Federal information infrastructure under subsection (a), and shall provide daily updates to Congress thereafter until the authority to provide for such defense expires.

(f) CONSTRUCTION.—Nothing in this section shall be construed to grant the Department of Defense authority, jurisdiction, or control over any non-Federal information infrastructure.

SA 2684. Mr. MCCONNELL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE __—REPEAL OF OBAMACARE

SEC. ___. REPEAL OF OBAMACARE.

(a) FINDINGS.—Congress finds the following with respect to the impact of Public Law 111–148 and related provisions of Public Law 111–152 (collectively referred to in this section as ''the law''):

(1) President Obama promised the American people that if they liked their current health coverage, they could keep it. But even the Obama Administration admits that tens of millions of Americans are at risk of losing their health care coverage, including as many as 8 in 10 plans offered by small businesses.

(2) Despite projected spending of more than two trillion dollars over the next 10 years, cutting Medicare by more than one-half trillion dollars over that period, and increasing taxes by over $800 billion dollars over that period, the law does not lower health care costs. In fact, the law actually makes coverage more expensive for millions of Americans. The average American family already paid a premium increase of approximately $1,200 in the year following passage of the law. The Congressional Budget Office (CBO) predicts that health insurance premiums for individuals buying private health coverage on their own will increase by $2,100 in 2016 compared to what the premiums would have been in 2016 if the law had not passed.

(3) The law cuts more than one-half trillion dollars in Medicare and uses the funds to create a new entitlement program rather than to protect and strengthen the Medicare program. Actuaries at the Centers for Medicare & Medicaid Services (CMS) warn that the Medicare cuts contained in the law are so drastic that ''providers might end their participation in the program (possibly jeopardizing access to care for beneficiaries)''. CBO cautioned that the Medicare cuts ''might be difficult to sustain over a long period of time''. According to the CMS actuaries, 7.4 million Medicare beneficiaries who would have been enrolled in a Medicare Advantage plan in 2017 will lose access to their plan because the law cuts $206 billion in payments to Medicare Advantage plans. The Trustees of the Medicare Trust Funds predict that the law will result in a substantial decline in employer-sponsored retiree drug coverage, and 90 percent of seniors will no longer have access to retiree drug coverage by 2016 as a result of the law.

(4) The law creates a 15-member, unelected Independent Payment Advisory Board that is empowered to make binding decisions regarding what treatments Medicare will cover and how much Medicare will pay for treatments solely to cut spending, restricting access to health care for seniors.

(5) The law and the more than 13,000 pages of related regulations issued before July 11, 2012, are causing great uncertainty, slowing economic growth, and limiting hiring opportunities for the approximately 13 million Americans searching for work. Imposing higher costs on businesses will lead to lower wages, fewer workers, or both.

(6) The law imposes 21 new or higher taxes on American families and businesses, including 12 taxes on families making less than $250,000 a year.

(7) While President Obama promised that nothing in the law would fund elective abortion, the law expands the role of the Federal Government in funding and facilitating abortion and plans that cover abortion. The law appropriates billions of dollars in new funding without explicitly prohibiting the use of these funds for abortion, and it provides Federal subsidies for health plans covering elective abortions. Moreover, the law effectively forces millions of individuals to personally pay a separate abortion premium in violation of their sincerely held religious, ethical, or moral beliefs.

(8) Until enactment of the law, the Federal Government has not sought to impose specific coverage or care requirements that infringe on the rights of conscience of insurers, purchasers of insurance, plan sponsors, beneficiaries, and other stakeholders, such as individual or institutional health care providers. The law creates a new nationwide requirement for health plans to cover ''essential health benefits'' and ''preventive services'', but does not allow stakeholders to opt out of covering items or services to which they have a religious or moral objection, in violation of the Religious Freedom Restoration Act (Public Law 103–141). By creating new barriers to health insurance and causing the loss of existing insurance arrangements, these inflexible mandates jeopardize the ability of institutions and individuals to exercise their rights of conscience and their ability to freely participate in the health insurance and health care marketplace.

(9) The law expands government control over health care, adds trillions of dollars to existing liabilities, drives costs up even further, and too often put Federal bureaucrats, instead of doctors and patients, in charge of health care decisionmaking.

(10) The path to patient-centered care and lower costs for all Americans must begin with a full repeal of the law.

(b) REPEAL.—

(1) PPACA.—Effective as of the enactment of Public Law 111–148, such Act (other than subsection (d) of section 1899A of the Social Security Act, as added and amended by sections 3403 and 10320 of such Public Law) is repealed, and the provisions of law amended or repealed by such Act (other than such subsection (d)) are restored or revived as if such Act had not been enacted.

(2) HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.—Effective as of the enactment of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), title I and subtitle B of title II of such Act are repealed, and the provisions of law amended or repealed by such title or subtitle, respectively, are restored or revived as if such title and subtitle had not been enacted.

SEC. ___. BUDGETARY EFFECTS OF THIS ACT.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

SA 2685. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 110, lines 17 and 18, after ''research laboratories'' insert the following: ''(including the defense laboratories (as defined in section 2199 of title 10, United States Code) and the national laboratories of the Department of Energy)''.

SA 2686. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, insert the following:

SEC. 416. SENSE OF CONGRESS.

(a) FINDINGS.—Congress finds the following:

(1) A report from the Bipartisan Policy Center's Cyber Security Task Force, published in July 2012, found that—

(A) 50,000 cyber attacks were reported to the Department of Homeland Security between October 2011 and February 2012; and

(B) 86 of the attacks described in subparagraph (A) took place on critical infrastructure networks.

(2) The report of the Commission on Cybersecurity for the 44th President from the Center for Strategic and International Studies (referred to in this subsection as ''CSIS''), published in November 2010, concluded that the United States is facing an imminent crisis in cybersecurity human capital.

(3) The November 2010 CSIS report cited another CSIS report, entitled ''A Human Capital Crisis in Cybersecurity'', which estimated that 1,000 specialists who had the specialized cybersecurity skills needed to defend the United States effectively in cyberspace existed in the United States, but the number of cybersecurity specialists needed that year was between 10,000 and 30,000.

(4) Another report published by CSIS, entitled ''Cybersecurity Two Years Later'', noted that ''there has been slow progress in changing the situation from where we were two years ago''.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, recognizing that the United States is currently facing a human capital crisis in cybersecurity, the President should—

(1) develop model standards, in coordination with any existing standards, for nonprofit institutions that provide training programs to develop advanced technical proficiency for individuals seeking careers in computer network defense;

(2) emphasize experiential learning and the opportunity to take on significant real-world casework as essential parts of training and development programs for cybersecurity professions;

(3) recognize institutions which develop advanced technical proficiency and provide real-world casework for individuals seeking careers in computer network defense as examples of excellence in specialized cybersecurity training;

(4) employ resources to support nonprofit institutions to expand the cybersecurity human capital capacity of the United States, particularly by supporting or establishing education and training programs which—

(A) demonstrate current and projected caseload of sufficient, important system and network defense activity to provide real-world training opportunities for trainees, with a heavy emphasis on real-life, hands-on, high-level cybersecurity work;

(B) demonstrate practical computer network defense skills and up-to-date cybersecurity experience of the senior staff proposing to lead the education and training programs;

(C) demonstrate access to hands-on training programs in the most up-to-date computer network defense technologies and techniques; and

(D) collaborate with the Federal Government and private sector companies in the United States in such programs; and

(5) establish a program recognizing citizens who have demonstrated outstanding leadership and service as mentors in the field of cybersecurity.

SA 2687. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of section 301, add the following:

(i) COORDINATION WITH DEPARTMENT OF DEFENSE AND DEPARTMENT OF ENERGY LABORATORIES.—It is the sense of Congress that to avoid duplication of Federal efforts in developing and executing a national cybersecurity research and development plan, the Director should ensure that coordination with other research initiatives under subsection (e) includes coordination with the defense laboratories (as defined in section 2199 of title 10, United States Code) and the national laboratories of the Department of Energy that are addressing challenges similar to the challenges described in subsection (b).

SA 2688. Mr. WYDEN (for himself and Mr. KIRK) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—GEOLOCATION INFORMATION

SEC. 801. SHORT TITLES.

This title may be cited as the ''Geolocational Privacy and Surveillance Act'' or the ''GPS Act''.

SEC. 802. PROTECTION OF GEOLOCATION INFORMATION.

(a) IN GENERAL.—Part 1 of title 18, United States Code, is amended by inserting after chapter 119 the following:

''CHAPTER 120—GEOLOCATION INFORMATION

''§ 2601. Definitions

''In this chapter:

''(1) COVERED SERVICE.—The term 'covered service' means an electronic communication service, a geolocation information service, or a remote computing service.

''(2) ELECTRONIC COMMUNICATION SERVICE.—The term 'electronic communication service' has the meaning given that term in section 2510.

''(3) ELECTRONIC SURVEILLANCE.—The term 'electronic surveillance' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(4) GEOLOCATION INFORMATION.—The term 'geolocation information' means, with respect to a person, any information, that is not the content of a communication, concerning the location of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.

''(5) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

''(6) INTERCEPT.—The term 'intercept' means the acquisition of geolocation information through the use of any electronic, mechanical, or other device.

''(7) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term 'investigative or law enforcement officer' means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

''(8) PERSON.—The term 'person' means any employee or agent of the United States, or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

''(9) REMOTE COMPUTING SERVICE.—The term 'remote computing service' has the meaning given that term in section 2711.

''(10) STATE.—The term 'State' means any State of the United States, the District of

Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

''(11) WIRELESS COMMUNICATION DEVICE.—The term 'wireless communication device' means any device that enables access to, or use of, an electronic communication system or service or a covered service, if that device utilizes a radio or other wireless connection to access such system or service.

''§ 2602. Interception and disclosure of geolocation information

''(a) IN GENERAL.—

''(1) PROHIBITION ON DISCLOSURE OR USE.—Except as otherwise specifically provided in this chapter, it shall be unlawful for any person to—

''(A) intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person;

''(B) intentionally disclose, or endeavor to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph;

''(C) intentionally use, or endeavor to use, any geolocation information, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; or

''(D)(i) intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to another person intercepted by means authorized by subsections (b) through (h), except as provided in such subsections;

''(ii) knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation;

''(iii) having obtained or received the information in connection with a criminal investigation; and

''(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

''(2) PENALTY.—Any person who violates paragraph (1) shall be fined under this title, imprisoned not more than five years, or both.

''(b) EXCEPTION FOR INFORMATION ACQUIRED IN THE NORMAL COURSE OF BUSINESS.—It shall not be unlawful under this chapter for an officer, employee, or agent of a provider of a covered service, whose facilities are used in the transmission of geolocation information, to intercept, disclose, or use that information in the normal course of the officer, employee, or agent's employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of a geolocation information service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

''(c) EXCEPTION FOR CONDUCTING FOREIGN INTELLIGENCE SURVEILLANCE.—Notwithstanding any other provision of this chapter, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of the official duty of the officer, employee, or agent to conduct electronic surveillance, as authorized by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

''(d) EXCEPTION FOR CONSENT.—

''(1) IN GENERAL.—It shall not be unlawful under this chapter for a person to intercept geolocation information pertaining to another person if such other person has given prior consent to such interception unless such information is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

''(2) CHILDREN.—The exception in paragraph (1) permits a parent or legal guardian of a child to intercept geolocation information pertaining to that child or to give consent for another person to intercept such information.

''(e) EXCEPTION FOR PUBLIC INFORMATION.—It shall not be unlawful under this chapter for any person to intercept or access geolocation information relating to another person through any system that is configured so that such information is readily accessible to the general public.

''(f) EXCEPTION FOR EMERGENCY INFORMATION.—It shall not be unlawful under this chapter for any investigative or law enforcement officer or other emergency responder to intercept or access geolocation information relating to a person if such information is used—

''(1) to respond to a request made by such person for assistance; or

''(2) in circumstances in which it is reasonable to believe that the life or safety of the person is threatened, to assist the person.

''(g) EXCEPTION FOR THEFT OR FRAUD.—It shall not be unlawful under this chapter for a person acting under color of law to intercept geolocation information pertaining to the location of another person who has unlawfully taken the device sending the geolocation information if—

''(1) the owner or operator of such device authorizes the interception of the person's geolocation information;

''(2) the person acting under color of law is lawfully engaged in an investigation; and

''(3) the person acting under color of law has reasonable grounds to believe that the geolocation information of the other person will be relevant to the investigation.

''(h) EXCEPTION FOR WARRANT.—

''(1) DEFINITIONS.—In this subsection:

''(A) COURT OF COMPETENT JURISDICTION.—The term 'court of competent jurisdiction' includes—

''(i) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

''(I) has jurisdiction over the offense being investigated;

''(II) is in or for a district in which the provider of a geolocation information service is located or in which the geolocation information is stored; or

''(III) is acting on a request for foreign assistance pursuant to section 3512; or

''(ii) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

''(B) GOVERNMENTAL ENTITY.—The term 'governmental entity' means a department or agency of the United States or any State or political subdivision thereof.

''(2) WARRANT.—A governmental entity may intercept geolocation information or require the disclosure by a provider of a covered service of geolocation information only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction, or as otherwise provided in this chapter or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

''(i) PROHIBITION ON DIVULGING GEOLOCATION INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a person providing a covered service shall not intentionally divulge geolocation information pertaining to another person.

''(2) EXCEPTIONS.—A person providing a covered service may divulge geolocation information—

''(A) as otherwise authorized in subsections (b) through (h);

''(B) with the lawful consent of such other person;

''(C) to another person employed or authorized, or whose facilities are used, to forward such geolocation information to its destination; or

''(D) which was inadvertently obtained by the provider of the covered service and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

''§ 2603. Prohibition of use as evidence of acquired geolocation information

''Whenever any geolocation information has been acquired, no part of such information and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

''§ 2604. Emergency situation exception

''(a) EMERGENCY SITUATION EXCEPTION.—Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, may intercept geolocation information if—

''(1) such officer reasonably determines that an emergency situation exists that—

''(A) involves—

''(i) immediate danger of death or serious physical injury to any person;

''(ii) conspiratorial activities threatening the national security interest; or

''(iii) conspiratorial activities characteristic of organized crime; and

''(B) requires geolocation information be intercepted before an order authorizing such interception can, with due diligence, be obtained;

''(2) there are grounds upon which an order could be entered to authorize such interception; and

''(3) an application for an order approving such interception is made within 48 hours after the interception has occurred or begins to occur.

''(b) FAILURE TO OBTAIN COURT ORDER.—

''(1) TERMINATION OF ACQUISITION.—In the absence of an order, an interception of geolocation information carried out under subsection (a) shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier.

''(2) PROHIBITION ON USE AS EVIDENCE.—In the event such application for approval is denied, the geolocation information shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application.

''§ 2605. Recovery of civil damages authorized

''(a) IN GENERAL.—Any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person, other than the United States, which engaged in that violation such relief as may be appropriate.

''(b) RELIEF.—In an action under this section, appropriate relief includes—

''(1) such preliminary and other equitable or declaratory relief as may be appropriate;

''(2) damages under subsection (c) and punitive damages in appropriate cases; and

''(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

''(c) COMPUTATION OF DAMAGES.—The court may assess as damages under this section whichever is the greater of—

''(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

''(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

''(d) DEFENSE.—It is a complete defense against any civil or criminal action brought against an individual for conduct in violation of this chapter if such individual acted in a good faith reliance on—

''(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

''(2) a request of an investigative or law enforcement officer under section 2604; or

''(3) a good-faith determination that an exception under section 2602 permitted the conduct complained of.

''(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

''(f) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, such head shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

''(g) IMPROPER DISCLOSURE IS VIOLATION.—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by this chapter is a violation of this chapter for purposes of this section.

''(h) CONSTRUCTION.—Nothing in this section may be construed to establish a new cause of action against any electronic communication service provider, remote computing service provider, geolocation service provider, or law enforcement or investigative officer, or eliminate or affect any cause of action that exists under section 2520, section 2707, or any other provision of law.''.

(b) CLERICAL AMENDMENT.—The table of chapters for part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following:

''120. Geolocation information ..... 2601''.

(c) CONFORMING AMENDMENTS.—Section 3512(a) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

''(B) a warrant or order for geolocation information or records related thereto, as provided under section 2602 of this title;''.

SEC. 803. REQUIREMENT FOR SEARCH WARRANTS TO ACQUIRE GEOLOCATION INFORMATION.

Rule 41(a) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2)(A), by striking the period at the end and inserting a comma and ''including geolocation information.''; and

(2) by adding at the end the following:

''(F) 'Geolocation information' has the meaning given that term in section 2601 of title 18, United States Code.''.

SEC. 804. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING GEOLOCATION INFORMATION.

(a) CRIMINAL VIOLATION.—Section 1039(h) of title 18, United States Code, is amended—

(1) in paragraph (2)—

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

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

(C) by adding at the end the following new subparagraph:

''(C) includes any geolocation information service.'';

(2) by redesignating paragraph (4) as paragraph (5); and

(3) by inserting after paragraph (3) the following:

''(4) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' has the meaning given that term in section 2601.''.

(b) CONFORMING AMENDMENTS.—

(1) DEFINITION AMENDMENTS.—Section 1039(h)(1) of title 18, United States Code, is amended—

(A) in the paragraph heading, by inserting ''OR GPS'' after ''PHONE''; and

(B) in the matter preceding subparagraph (A), by inserting ''or GPS'' after ''phone''.

(2) CONFORMING AMENDMENTS.—Section 1039 of title 18, United States Code, is amended—

(A) in the section heading by inserting ''**or GPS**'' after ''**phone**'';

(B) in subsection (a)—

(i) in the matter preceding paragraph (1), by inserting ''or GPS'' after ''phone''; and

(ii) in paragraph (4), by inserting ''or GPS'' after ''phone'';

(C) in subsection (b)—

(i) in the subsection heading, by inserting ''OR GPS'' after ''PHONE'';

(ii) in paragraph (1), by inserting ''or GPS'' after ''phone'' both places that term appears; and

(iii) in paragraph (2), by inserting ''or GPS'' after ''phone''; and

(D) in subsection (c)—

(i) in the subsection heading, by inserting ''OR GPS'' after ''PHONE'';

(ii) in paragraph (1), by inserting ''or GPS'' after ''phone'' both places that term appears; and

(iii) in paragraph (2), by inserting ''or GPS'' after ''phone''.

(3) CHAPTER ANALYSIS.—The table of sections for chapter 47 of title 18, United States Code, is amended by striking the item relating to section 1039 and inserting the following:

''1039. Fraud and related activity in connection with obtaining confidential phone or GPS records information of a covered entity.''.

(c) SENTENCING GUIDELINES.—

(1) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code, as amended by this section.

(2) AUTHORIZATION.—The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

SEC. 805. STATEMENT OF EXCLUSIVE MEANS OF ACQUIRING GEOLOCATION INFORMATION.

(a) IN GENERAL.—No person may acquire the geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, as amended by section 803, or the amendments made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) GEOLOCATION INFORMATION DEFINED.—In this section, the term ''geolocation information'' has the meaning given that term in section 2601 of title 18, United States Code, as amended by section 802.

SA 2689. Mr. BENNET (for himself and Mr. COBURN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—FEDERAL DATA CENTER CONSOLIDATION INITIATIVE

SEC. 801. DEFINITIONS.

In this title:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator for the Office of E-Government and Information Technology within the Office of Management and Budget.

(2) CHIEF INFORMATION OFFICERS COUNCIL.—The term ''Chief Information Officers Council'' means the Chief Information Officers Council established under section 3603 of title 44, United States Code.

(3) DATA CENTER.—

(A) DEFINITION.—The term ''data center'' means a closet, room, floor, or building for the storage, management, and dissemination of data and information, as defined by the Administrator in the ''Implementation Guidance for the Federal Data Center Consolidation Initiative'' memorandum, issued on March 19, 2012.

(B) AUTHORITY TO MODIFY DEFINITION.—The Administrator may promulgate guidance or other clarifications to modify the definition in subparagraph (A) in a manner consistent with this Act, as the Administrator determines necessary.

SEC. 802. FEDERAL DATA CENTER CONSOLIDATION INVENTORIES AND PLANS.

(a) REQUIRED SUBMISSIONS.—

(1) IN GENERAL.—

(A) ANNUAL REPORTS.—Each year, beginning in fiscal year 2013 through the end of fiscal year 2017, the head of each agency that is described in paragraph (2), assisted by the chief information officer of the agency, shall submit to the Administrator—

(i) by June 30th of each year, a comprehensive asset inventory of the data centers owned, operated, or maintained by or on behalf of the agency, even if the center is administered by a third party; and

(ii) by September 30th of each year, an updated consolidation plan that includes—

(I) a technical roadmap and approach for achieving the agency's targets for infrastructure utilization, energy efficiency, cost savings and efficiency;

(II) a detailed timeline for implementation of the data center consolidation plan;

(III) quantitative utilization and efficiency goals for reducing assets and improving use of information technology infrastructure;

(IV) performance metrics by which the progress of the agency toward data center consolidation goals can be measured, including metrics to track any gains in energy utilization as a result of this initiative;

(V) an aggregation of year-by-year investment and cost savings calculations for 5 years past the date of submission of the cost saving assessment, including a description of any initial costs for data center consolidation;

(VI) quantitative progress towards previously stated goals including cost savings and increases in operational efficiencies and utilization; and

(VII) any additional information required by the Administrator.

(B) CERTIFICATION.—Each year, beginning in fiscal year 2013 through the end of fiscal year 2017, the head of an agency, acting through the chief information officer of the agency, shall submit a statement to the Administrator certifying that the agency has complied with the requirements of this section.

(C) INSPECTOR GENERAL REPORT.—

(i) IN GENERAL.—The Inspector General for each agency described in paragraph (2) shall release a public report not later than 6 months after the date on which the agency releases the first updated asset inventory in fiscal year 2013 under subparagraph (A)(i), which shall evaluate the completeness of the inventory of the agency; and

(ii) AGENCY RESPONSE.—The head of each agency shall respond to the report completed by the Inspector General for the agency under clause (i), and complete any inventory identified by the Inspector General for the agency as incomplete, by the time the agency submits the required inventory update for fiscal year 2014.

(D) RESPONSIBILITY OF THE ADMINISTRATOR.—The Administrator shall ensure that each certification submitted under subparagraph (B) and each agency consolidation plan submitted under subparagraph (A)(ii), is made available in a timely fashion to the general public.

(2) AGENCIES DESCRIBED.—The agencies (including all associated components of the agency) described in this paragraph are the—

(A) Department of Agriculture;

(B) Department of Commerce;

(C) Department of Defense;

(D) Department of Education;

(E) Department of Energy;

(F) Department of Health and Human Services;

(G) Department of Homeland Security;

(H) Department of Housing and Urban Development;

(I) Department of the Interior;

(J) Department of Justice;

(K) Department of Labor;

(L) Department of State;

(M) Department of Transportation;

(N) Department of Treasury;

(O) Department of Veterans Affairs;

(P) Environmental Protection Agency;

(Q) General Services Administration;

(R) National Aeronautics and Space Administration;

(S) National Science Foundation;

(T) Nuclear Regulatory Commission;

(U) Office of Personnel Management;

(V) Small Business Administration;

(W) Social Security Administration; and

(X) United States Agency for International Development.

(3) AGENCY IMPLEMENTATION OF CONSOLIDATION PLANS.—Each agency described in paragraph (2), under the direction of the chief information officer of the agency, shall—

(A) implement the consolidation plan required under paragraph (1)(A)(ii); and

(B) provide to the Administrator annual updates on implementation and cost savings realized through such consolidation plan.

(b) ADMINISTRATOR REVIEW.—The Administrator shall—

(1) review the plans submitted under subsection (a) to determine whether each plan is comprehensive and complete;

(2) monitor the implementation of the data center consolidation plan of each agency described in subsection (a)(2); and

(3) update the cumulative cost savings projection on an annual basis as the savings are realized through the implementation of the agency plans.

(c) COST SAVING GOAL AND UPDATES FOR CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, or by September 30th of fiscal year 2013, whichever is later, the Administrator shall develop and publish a goal for the total amount of planned cost savings by the Federal Government through the Federal Data Center Consolidation Initiative during the 5-year period beginning on the date of enactment of this Act, which shall include a breakdown on a year-by-year basis of the projected savings.

(2) ANNUAL UPDATE.—

(A) IN GENERAL.—Not later than 1 year after the date on which the goal described in paragraph (1) is determined and each year thereafter until the end of 2017, the Administrator shall publish a report on the actual savings achieved through the Federal Data Center Consolidation Initiative as compared to the projected savings developed under paragraph (1) (based on data collected from each affected agency under subsection (a)(1)).

(B) UPDATE FOR CONGRESS.—The report required under subparagraph (A) shall be submitted to Congress and shall include an update on the progress made by each agency described in subsection (a)(2) on—

(i) whether each agency has in fact submitted a comprehensive asset inventory;

(ii) whether each agency has submitted a comprehensive consolidation plan with the key elements described in (a)(1)(A)(ii); and

(iii) the progress, if any, of each agency on implementing the consolidation plan of the agency.

(d) GAO REVIEW.—The Comptroller General of the United States shall, on an annual basis, publish a report on—

(1) the quality and completeness of each agency's asset inventory and consolidation plans required under subsection (a)(1)(A);

(2) each agency's progress on implementation of the consolidation plans submitted under subsection (a)(1)(A);

(3) overall planned and actual cost savings realized through implementation of the consolidation plans submitted under subsection (a)(1)(A);

(4) any steps that the Administrator could take to improve implementation of the data center consolidation initiative; and

(5) any matters for Congressional consideration in order to improve or accelerate the implementation of the data center consolidation initiative.

(e) RESPONSE TO GAO.—

(1) IN GENERAL.—If a report required under subsection (d) identifies any deficiencies or delays in any of the elements described in paragraphs (1) through (5) of subsection (d) for an agency, the head of the agency shall respond in writing to the Comptroller General of the United State, not later than 90 days after the date on which the report is published under subsection (d), with a detailed explanation of how the agency will address the deficiency.

(2) ADDITIONAL REQUIREMENTS.—If the Comptroller General identifies an agency that has repeatedly lagged in implementing the data center consolidation initiative, the Comptroller General may require that the head of the agency submit a statement explaining—

(A) why the agency is having difficulty implementing the initiative; and

(B) what structural or personnel changes are needed within the agency to address the problem.

SEC. 803. ENSURING CYBERSECURITY STANDARDS FOR DATA CENTER CONSOLIDATION AND CLOUD COMPUTING.

An agency required to implement a data center consolidation plan under this title and migrate to cloud computing shall do so in a manner that is consistent with Federal guidelines on cloud computing security, including—

(1) applicable provisions found within the Federal Risk and Authorization Management Program of the General Service Administration; and

(2) guidance published by the National Institute of Standards and Technology.

SEC. 804. CLASSIFIED INFORMATION.

The Director of National Intelligence may waive the requirements of this title for any element (or component of an element) of the intelligence community.

SEC. 805. SUNSET.

This title is repealed effective on October 1, 2017.

SA 2690. Ms. MURKOWSKI submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of section 104, add the following:

(d) APPLICATION OF BENEFITS OF CYBERSECURITY PROGRAM TO ENTITIES SUBJECT TO MANDATORY REQUIREMENTS.—

(1) IN GENERAL.—Subject to paragraphs (2) through (4), any entity subject to the jurisdiction of the Federal Energy Regulatory Commission under section 215 of the Federal Power Act (16 U.S.C. 824o) or to any facility subject to cybersecurity measures required by the Nuclear Regulatory Commission under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) shall be entitled to the benefits of certification provided under subsection (c) (other than subsection (c)(1)).

(2) ELIGIBILITY.—To be eligible for the benefits of certification described in paragraph (1), an entity or facility shall demonstrate to the Secretary of Energy that it is an entity or facility described in paragraph (1).

(3) CERTIFIED OWNER OR OPERATOR.—If the Secretary of Energy determines that an entity or facility is an entity or facility described in paragraph (1), the entity or facility shall be considered a certified owner or operator under this section (other than subsection (c)(1)).

(4) EFFECT ON OTHER LAWS.—Nothing in this subsection limits the applicability of any exemption from or limitation of liability or damages that a certified owner may have under any other Federal or State law (including regulations).

(e) FEDERAL ENERGY LAWS.—Except as provided in subsection (d), nothing in this Act authorizes the imposition or modification of requirements relating to—

(1)(A) the bulk-power system;

(B) the promulgation or enforcement of reliability standards for the bulk power system (including for cybersecurity protection) by the certified Electric Reliability Organization; or

(C) the approval or enforcement of the standards by the Federal Energy Regulatory Commission under section 215 of the Federal Power Act (16 U.S.C. 824o); or

(2) nuclear facilities subject to cybersecurity measures required by the Nuclear Regulatory Commission under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SA 2691. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title I.

SA 2692. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 4 and all that follows and insert the following:

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

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

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

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

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) 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 inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''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 National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

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

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

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

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

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

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

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) 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.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted

cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) 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.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under section 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight

Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(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—

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

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide 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) to 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;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

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

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term '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 National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) 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 inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) 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 organization on behalf of an executive agency.

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

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

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

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

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

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

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

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

''(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) 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) 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) LIMITATION.—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).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

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

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) 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.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

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

''(i) information collected 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 on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(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 the policies and directives issued by the Secretary under this subchapter;

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

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. 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 such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

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

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

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

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

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

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

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

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

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

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

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

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment 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 security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

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

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(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 as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 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 access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(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.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (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 pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) 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)(2)''.

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) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of 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)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding 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 AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include 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 information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

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

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

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

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

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

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

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the

court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(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) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and

resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of

Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

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

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

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

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION 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'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; 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) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2693. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 118, line 16, insert '', including legal and behavioral impediments to deployment of proven security policies'' before the semicolon.

SA 2694. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 118, line 25, strike ''and'' and all that follows through page 119, line 2, and insert the following:

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

(8) demonstrated expertise in cybersecurity law, including the legal impediments to adoption of proven security processes; and

(9) demonstrated expertise in social and behavioral research that can assist in developing policies and incentives to help protect against cyber attacks.

SA 2695. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. NOTICE REQUIRED PRIOR TO TRANSFER OF CERTAIN INDIVIDUALS DETAINED AT THE DETENTION FACILITY AT PARWAN, AFGHANISTAN.

(a) NOTICE REQUIRED.—The Secretary of Defense shall submit to the appropriate congressional committees notice in writing of the proposed transfer of any individual detained pursuant to the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note) who is a national of a country other than the United States or Afghanistan from detention at the Detention Facility at Parwan, Afghanistan, to the custody of the Government of Afghanistan or of any other country. Such notice shall be provided not later than 10 days before such a transfer may take place.

(b) ADDITIONAL ASSESSMENTS AND CERTIFICATIONS.—As part of the notice required under subsection (a), the Secretary shall include the following:

(1) In the case of the proposed transfer of such an individual by reason of the individual being released, an assessment of the threat posed by the individual and the security environment of the country to which the individual is to be transferred.

(2) In the case of the proposed transfer of such an individual to a country other than Afghanistan for the purpose of the prosecution of the individual, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of the country with respect to prosecuting similar cases, including a description of the evidence against the individual that is likely to be admissible as part of the prosecution.

(3) In the case of the proposed transfer of such an individual for reintegration or rehabilitation in a country other than Afghanistan, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of the country for reintegrating or rehabilitating similar individuals.

(4) In the case of the proposed transfer of such an individual to the custody of the government of Afghanistan for prosecution or detention, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of Afghanistan to prosecute or detain long-term such individuals.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives; and

(2) the Committee on Armed Services and the Committee on Foreign Relations of the Senate.

SA 2696. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 4 and all that follows and insert the following:

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

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

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

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

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) 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 inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''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 National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

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

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

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

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

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

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

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) 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.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

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

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) 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.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under section 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(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—

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

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide 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) to 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;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs

through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

"§ 3552. Definitions

''In this subchapter:

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

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term '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 National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) 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 inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) 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 organization on behalf of an executive agency.

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

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

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

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

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

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

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

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

''(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) 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) 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) LIMITATION.—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).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

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

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) 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.

"§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

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

''(i) information collected 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 on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(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 the policies and directives issued by the Secretary under this subchapter;

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

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber

threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. 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 such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

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

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

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

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

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

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

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

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

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

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

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

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment 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 security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

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

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(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 as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 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 access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(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.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (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 pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) 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)(2)''.

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) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of 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)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding 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 AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include 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 information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

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

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

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

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

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

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

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure

and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component

Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(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) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force

to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-

performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

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

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

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

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION 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'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; 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) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2697. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. SENSE OF SENATE ON APPOINTMENT BY THE ATTORNEY GENERAL OF AN OUTSIDE SPECIAL COUNSEL TO INVESTIGATE CERTAIN RECENT LEAKS OF APPARENTLY CLASSIFIED AND HIGHLY SENSITIVE INFORMATION ON UNITED STATES MILITARY AND INTELLIGENCE PLANS, PROGRAMS, AND OPERATIONS.

(a) FINDINGS.—The Senate makes the following findings:

(1) Over the past few weeks, several publications have been released that cite several highly sensitive United States military and intelligence counterterrorism plans, programs, and operations.

(2) These publications appear to be based in substantial part on unauthorized disclosures of classified information.

(3) The unauthorized disclosure of classified information is a felony under Federal law.

(4) The identity of the sources in these publications include senior administration officials, participants in these reported plans, programs, and operations, and current American officials who spoke anonymously about these reported plans, programs, and operations because they remain classified, parts of them are ongoing, or both.

(5) Such unauthorized disclosures may inhibit the ability of the United States to employ the same or similar plans, programs, or operations in the future; put at risk the national security of the United States and the safety of the men and women sworn to protect it; and dismay our allies.

(6) Under Federal law, the Attorney General may appoint an outside special counsel when an investigation or prosecution would present a conflict of interest or other extraordinary circumstances and when doing so would serve the public interest.

(7) Investigations of unauthorized disclosures of classified information are ordinarily conducted by the Federal Bureau of Investigation with assistance from prosecutors in the National Security Division of the Department of Justice.

(8) There is precedent for officials in the National Security Division of the Department of Justice to recuse itself from such investigations to avoid even the appearance of impropriety or undue influence, and it appears that there have been such recusals with respect to the investigation of at least one of these unauthorized disclosures.

(9) Such recusals are indicative of the serious complications already facing the Department of Justice in investigating these matters.

(10) The severity of the national security implications of these disclosures; the imperative for investigations of these disclosures to be conducted independently so as to avoid even the appearance of impropriety or undue influence; and the need to conduct these investigations expeditiously to ensure timely mitigation constitute extraordinary circumstances.

(11) For the foregoing reasons, the appointment of an outside special counsel would serve the public interest.

(b) SENSE OF SENATE.—It is the sense of the Senate that—

(1) the Attorney General should—

(A) delegate to an outside special counsel all of the authority of the Attorney General with respect to investigations by the Department of Justice of any and all unauthorized disclosures of classified and highly sensitive information related to various United States military and intelligence plans, programs, and operations reported in recent publications; and

(B) direct an outside special counsel to exercise that authority independently of the supervision or control of any officer of the Department of Justice;

(2) under such authority, the outside special counsel should investigate any and all unauthorized disclosures of classified and highly sensitive information on which such recent publications were based and, where appropriate, prosecute those responsible; and

(3) the President should assess—

(A) whether any such unauthorized disclosures of classified and highly sensitive information damaged the national security of the United States; and

(B) how such damage can be mitigated.

SA 2698. Mr. PORTMAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE ___—RESPONSE TO CONGRESSIONAL INQUIRIES

SEC. ___1. RESPONSE TO CONGRESSIONAL INQUIRIES REGARDING PUBLIC RELATIONS SPENDING BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.

Not later than 7 days after the date of the enactment of this Act, the Secretary of Health and Human Services shall respond in full to the following congressional inquiries:

(1) The letter dated February 28, 2012, from the Chairman and Ranking Member of the Subcommittee on Contracting Oversight of

the Committee on Homeland Security and Governmental Affairs of the Senate, requesting certain information regarding Department of Health and Human Services contracts for the acquisition of public relations, publicity, advertising, communications, or similar services.

(2) The follow-up letter dated May 22, 2012, from the Ranking Member of the Subcommittee on Contracting Oversight of the Committee on Homeland Security and Governmental Affairs of the Senate, requesting information regarding a reported $20,000,000 Department of Health and Human Services contract with a public relations firm.

SA 2699. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—REPEAL OF PPACA

SEC. __01. SHORT TITLE.

This title may be cited as the ''Repealing the Job-Killing Health Care Law Act''.

SEC. __02. REPEAL OF THE JOB-KILLING HEALTH CARE LAW AND HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.

(a) JOB-KILLING HEALTH CARE LAW.—Effective as of the enactment of Public Law 111–148, such Act is repealed, and the provisions of law amended or repealed by such Act are restored or revived as if such Act had not been enacted.

(b) HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.—Effective as of the enactment of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), title I and subtitle B of title II of such Act are repealed, and the provisions of law amended or repealed by such title or subtitle, respectively, are restored or revived as if such title and subtitle had not been enacted.

SEC. __03. BUDGETARY EFFECTS OF THIS ACT.

The budgetary effects of this title, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this title, submitted for printing in the Congressional Record by the Chairman of the Committee on the Budget of the House of Representatives, as long as such statement has been submitted prior to the vote on passage of this Act.

SA 2700. Mr. ROCKEFELLER (for himself, Mrs. FEINSTEIN, and Mr. PRYOR) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 212, after line 6, add the following:

TITLE VIII—DATA SECURITY AND BREACH NOTIFICATION

SEC. 801. SHORT TITLE.

This title may be cited as the ''Data Security and Breach Notification Act of 2012''.

SEC. 802. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity that owns or possesses data containing personal information, or contracts to have any third-party entity maintain such data for such covered entity, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such covered entity;

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information;

(C) the cost of implementing the safeguards under subparagraph (B); and

(D) the impact on small businesses and nonprofits.

(2) REQUIREMENTS.—The regulations shall require the policies and procedures to include the following:

(A) A security policy with respect to the collection, use, sale, other dissemination, and maintenance of personal information.

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in each system maintained by the covered entity that contains such personal information, which shall include regular monitoring for a breach of security of each such system.

(D) A process for taking preventive and corrective action to mitigate any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software.

(E) A process for disposing of data in electronic form containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

(b) LIMITATIONS.—

(1) COVERED ENTITIES SUBJECT TO THE GRAMM-LEACH-BLILEY ACT.—Notwithstanding section 805 of this Act, this section (and any regulations issued pursuant to this section) shall not apply to any financial institution that is subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) with respect to covered information under that Act.

(2) APPLICABILITY OF OTHER INFORMATION SECURITY REQUIREMENTS.—To the extent that the information security requirements of section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or of section 1173(d) of title XI, part C of the Social Security Act (42 U.S.C. 1320d-2(d)) apply in any circumstance to a person who is subject to either of those Acts, and to the extent the person is acting as an entity subject to either of those Acts, the person shall be exempt from the requirements of this section with respect to any data governed by section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or by the Health Insurance Portability and Accountability Act of 1996 Security Rule (45 C.F.R. 160.103 and Part 164).

(3) CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party to the extent that the service provider is engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

SEC. 803. NOTIFICATION OF BREACH OF SECURITY.

(a) NATIONWIDE NOTIFICATION.—A covered entity that owns or possesses data in electronic form containing personal information, following the discovery of a breach of security of the system maintained by the covered entity that contains such data, shall notify—

(1) each individual who is a citizen or resident of the United States and whose personal information was or is reasonably believed to have been acquired or accessed from the covered entity as a result of the breach of security; and

(2) the Commission, unless the covered entity has notified the designated entity under section 804.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY ENTITIES.—In the event of a breach of security of a system maintained by a third-party entity that has been contracted to maintain or process data in electronic form containing personal information on behalf of any other covered entity who owns or possesses such data, the third-party entity shall notify the covered entity of the breach of security. Upon receiving notification from the third party entity, such covered entity shall provide the notification required under subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall notify of the breach of security only the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified. Upon receiving the notification from the service provider, the covered entity shall provide the notification required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 5,000 individuals under subsection (a)(1), the covered entity also shall notify each major credit reporting agency of the timing and distribution of the notices, except when the only personal information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code. Such notice shall be given to each credit reporting agency without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMELINESS OF NOTIFICATION.—Notification under subsection (a) shall be made—

(1) not later than 45 days after the date of discovery of a breach of security; or

(2) as promptly as possible if the covered entity providing notice can show that providing notice within the time frame under paragraph (1) is not feasible due to circumstances necessary—

(A) to accurately identify affected consumers;

(B) to prevent further breach or unauthorized disclosures; or

(C) to reasonably restore the integrity of the data system.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF DIRECT NOTIFICATION.—A covered entity shall be in compliance with the notification requirement under subsection (a)(1) if—

(i) the covered entity provides conspicuous and clearly identified notification—

(I) in writing; or

(II) by e-mail or other electronic means if—

(aa) the covered entity's primary method of communication with the individual is by e-mail or such other electronic means; or

(bb) the individual has consented to receive notification by e-mail or such other electronic means and such notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001); and

(ii) the method of notification selected under clause (i) can reasonably be expected to reach the intended individual.

(B) CONTENT OF DIRECT NOTIFICATION.—Each method of direct notification under subparagraph (A) shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) a telephone number that an individual can use at no cost to the individual to contact the covered entity to inquire about the breach of security or the information the covered entity maintained about that individual;

(iv) notice that the individual may be entitled to consumer credit reports under subsection (e)(1);

(v) instructions how an individual can request consumer credit reports under subsection (e)(1);

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to individuals under subsection (a)(1) may provide substitute notification instead of direct notification under paragraph (1)—

(i) if direct notification is not feasible due to lack of sufficient contact information for the individual required to be notified; or

(ii) if the covered entity owns or possesses data in electronic form containing personal information of fewer than 10,000 individuals and direct notification is not feasible due to excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A).

(B) METHOD OF SUBSTITUTE NOTIFICATION.—Substitute notification under this paragraph shall include—

(i) conspicuous and clearly identified notification by e-mail to the extent the covered entity has an e-mail address for an individual who is entitled to notification under subsection (a)(1);

(ii) conspicuous and clearly identified notification on the Internet Web site of the covered entity if the covered entity maintains an Internet Web site; and

(iii) notification to print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTIFICATION.—Each method of substitute notification under this paragraph shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the types of personal information that were or are reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) notice that an individual may be entitled to consumer credit reports under subsection (e)(1);

(iv) instructions how an individual can request consumer credit reports under subsection (e)(1);

(v) a telephone number that an individual can use at no cost to the individual to learn whether the individual's personal information is included in the breach of security;

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining circumstances under which substitute notification may be provided under section 803(d)(2) of this Act, including criteria for determining if direct notification under section 803(d)(1) of this Act is not feasible due to excessive costs to the covered entity required to provided such notification relative to the resources of such covered entity. The regulations may also identify other circumstances where substitute notification would be appropriate for any covered entity, including circumstances under which the cost of providing direct notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission, in consultation with the Small Business Administration, shall provide and publish general guidance with respect to compliance with this subsection. The guidance shall include—

(i) a description of written or e-mail notification that complies with paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2), including the extent of notification to print and broadcast media that complies with paragraph (2)(B)(iii).

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—Not later than 60 days after the date of request by an individual whose personal information was included in a breach of security and quarterly thereafter for 2 years, a covered entity required to provide notification under subsection (a)(1) shall provide, or arrange for the provision of, to the individual at no cost, consumer credit reports from at least 1 major credit reporting agency.

(2) LIMITATION.—Paragraph (1) shall not apply if the only personal information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—The Commission's rulemaking under subsection (d)(3) shall include—

(A) determination of the circumstances under which a covered entity required to provide notification under subsection (a) must provide or arrange for the provision of free consumer credit reports; and

(B) establishment of a simple process under which a covered entity that is a small business or small non-profit organization may request a full or a partial waiver or a modified or an alternative means of complying with this subsection if providing free consumer credit reports is not feasible due to excessive costs relative to the resources of such covered entity and relative to the level of harm, to affected individuals, caused by the breach of security.

(f) DELAY OF NOTIFICATION AUTHORIZED FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If the United States Secret Service or the Federal Bureau of Investigation determines that notification under this section would impede a criminal investigation or a national security activity, notification shall be delayed upon written notice from the United States Secret Service or the Federal Bureau of Investigation to the covered entity that experienced the breach of security. Written notice from the United States Secret Service or the Federal Bureau of Investigation shall specify the period of delay requested for national security or law enforcement purposes.

(2) SUBSEQUENT DELAY OF NOTIFICATION.—

(A) IN GENERAL.—A covered entity shall provide notification under this section not later than 30 days after the day that the delay was invoked unless a Federal law enforcement or intelligence agency provides subsequent written notice to the covered entity that further delay is necessary.

(B) WRITTEN JUSTIFICATION REQUIREMENTS.—

(i) UNITED STATES SECRET SERVICE.—If the United States Secret Service instructs a covered entity to delay notification under this section beyond the 30 day period under subparagraph (A) (''subsequent delay''), the United States Secret Service shall submit written justification for the subsequent delay to the Secretary of Homeland Security before the subsequent delay begins.

(ii) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation instructs a covered entity to delay notification under this section beyond the 30 day period under subparagraph (A) (''subsequent delay''), the Federal Bureau of Investigation shall submit written justification for the subsequent delay to the U.S. Attorney General before the subsequent delay begins.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the delay of notification for national security or law enforcement purposes under this title.

(g) GENERAL EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if, following a breach of security, the covered entity determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTION.—

(A) IN GENERAL.—There shall be a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security if—

(i) the data is rendered unusable, unreadable, or indecipherable through a security technology or methodology; and

(ii) the security technology or methodology under clause (i) is generally accepted by experts in the information security field.

(B) REBUTTAL.—The presumption under subparagraph (A) may be rebutted by facts demonstrating that the security technology or methodology in a specific case has been or is reasonably likely to be compromised.

(3) TECHNOLOGIES OR METHODOLOGIES.—Not later than 1 year after the date of enactment

of this Act, and biannually thereafter, the Commission, after consultation with the National Institute of Standards and Technology, shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify each security technology and methodology under paragraph (2). In issuing the rules or guidance, the Commission shall—

(A) consult with relevant industries, consumer organizations, data security and identity theft prevention experts, and established standards setting bodies; and

(B) consider whether and in what circumstances a security technology or methodology currently in use, such as encryption, complies with the standards under paragraph (2).

(4) FTC GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission, after consultation with the National Institute of Standards and Technology, shall issue guidance regarding the application of the exemption under paragraph (1).

(h) EXEMPTIONS FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if—

(A) a determination is made—

(i) by the United States Secret Service or the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to reveal sensitive sources and methods or similarly impede the ability of the Government to conduct law enforcement or intelligence investigations; or

(ii) by the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to cause damage to the national security; and

(B) the United States Secret Service or the Federal Bureau of Investigation, as the case may be, provides written notice of its determination under subparagraph (A) to the covered entity.

(2) UNITED STATES SECRET SERVICE.—If the United States Secret Service invokes an exemption under paragraph (1), the United States Secret Service shall submit written justification for invoking the exemption to the Secretary of Homeland Security before the exemption is invoked.

(3) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation invokes an exemption under paragraph (1), the Federal Bureau of Investigation shall submit written justification for invoking the exemption to the U.S. Attorney General before the exemption is invoked.

(4) IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for national security or law enforcement purposes under this title.

(5) REPORTS.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the United States Secret Service and Federal Bureau of Investigation shall submit to Congress a report on the number and nature of breaches of security subject to the exemptions for national security and law enforcement purposes under this subsection.

(i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if the covered entity utilizes or participates in a security program that—

(A) effectively blocks the use of the personal information to initiate an unauthorized financial transaction before it is charged to the account of the individual; and

(B) provides notice to each affected individual after a breach of security that resulted in attempted fraud or an attempted unauthorized transaction.

(2) LIMITATIONS.—An exemption under paragraph (1) shall not apply if—

(A) the breach of security includes personal information, other than a credit card number or credit card security code, of any type; or

(B) the breach of security includes both the individual's credit card number and the individual's first and last name.

(j) FINANCIAL INSTITUTIONS REGULATED BY FEDERAL FUNCTIONAL REGULATORS.—

(1) IN GENERAL.—Nothing in this section shall apply to a covered financial institution if the Federal functional regulator with jurisdiction over the covered financial institution has issued a standard by regulation or guideline under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that—

(A) requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security; and

(B) provides protections substantially similar to, or greater than, those required under this title.

(2) DEFINITIONS.—In this subsection—

(A) the term ''covered financial institution'' means a financial institution that is subject to—

(i) the data security requirements of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(ii) any implementing standard issued by regulation or guideline issued under that Act; and

(iii) the jurisdiction of a Federal functional regulator under that Act;

(B) the term ''Federal functional regulator'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809); and

(C) the term ''financial institution'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(k) EXEMPTION; HEALTH PRIVACY.—

(1) COVERED ENTITY OR BUSINESS ASSOCIATE UNDER HITECH ACT.—To the extent that a covered entity under this title acts as a covered entity or a business associate under section 13402 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17932), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this section shall not apply.

(2) ENTITY SUBJECT TO HITECH ACT.—To the extent that a covered entity under this title acts as a vendor of personal health records, a third party service provider, or other entity subject to section 13407 of the Health Information Technology for Economical and Clinical Health Act (42 U.S.C. 17937), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this section shall not apply.

(3) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this Act may be construed in any way to give effect to the sunset provision under section 13407(g)(2) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937(g)(2)) or to otherwise limit or affect the applicability, under section 13407 of that Act, of the breach notification requirement for vendors of personal health records and each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A) of that Act (42 U.S.C. 17953(b)(1)(A)) .

(l) WEB SITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission, finds that notification of the breach of security via the Commission's Internet Web site would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet Web site.

(m) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness of requiring the direct notification required by subsection (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(n) GENERAL RULEMAKING AUTHORITY.—The Commission may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

SEC. 804. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—Not later than 60 days after the date of enactment of this Act, the Secretary of the Department of Homeland Security shall designate a Federal Government entity to receive notice under this section.

(b) NOTICE.—A covered entity shall notify the designated entity of a breach of security if—

(1) the number of individuals whose personal information was, or is reasonably believed to have been, acquired or assessed as a result of the breach of security exceeds 10,000;

(2) the breach of security involves a database, networked or integrated databases, or other data system containing the personal information of more than 1,000,000 individuals;

(3) the breach of security involves databases owned by the Federal Government; or

(4) the breach of security involves primarily personal information of individuals known to the covered entity to be employees or contractors of the Federal Government involved in national security or law enforcement.

(c) CONTENT OF NOTICES.—

(1) IN GENERAL.—Each notice under subsection (b) shall contain—

(A) the date, estimated date, or estimated date range of the breach of security;

(B) a description of the nature of the breach of security;

(C) a description of each type of personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security; and

(D) a statement of each paragraph under subsection (b) that applies to the breach of security.

(2) CONSTRUCTION.—Nothing in this section shall be construed to require a covered entity to reveal specific or identifying information about an individual as part of the notice under paragraph (1).

(d) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall promptly provide each notice it receives under subsection (b) to—

(1) the United States Secret Service;

(2) the Federal Bureau of Investigation;

(3) the Federal Trade Commission;

(4) the United States Postal Inspection Service, if the breach of security involves mail fraud;

(5) the attorney general of each State affected by the breach of security; and

(6) as appropriate, other Federal agencies for law enforcement, national security, or data security purposes.

(e) TIMING OF NOTICES.—Notice under this section shall be delivered as follows:

(1) Notice under subsection (b) shall be delivered as promptly as possible, but—

(A) not less than 3 business days before notification to an individual pursuant to section 803; and

(B) not later than 10 days after the date of discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered as promptly as possible, but not later than 1 business day after the date that the designated entity receives notice of a breach of security from a covered entity.

SEC. 805. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 802 and 803 apply to—

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.

(b) OPT-IN FOR CERTAIN OTHER ENTITIES.—

(1) IN GENERAL.—Section 803 shall apply to any other person or entity that enters into an agreement with the Commission under which section 803 would apply to that person or entity, with respect to any acts or omissions that occur while the agreement is in effect and that may constitute a violation of section 803, if—

(A) not less than 30 days prior to entering into the agreement with the person or entity, the Commission publishes notice in the Federal Register of the Commission's intent to enter into the agreement; and

(B) not later than 14 business days after entering into the agreement with the person or entity, the Commission publishes in the Federal Register—

(i) notice of the agreement;

(ii) the identify of each person or entity covered by the agreement; and

(iii) the effective date of the agreement.

(2) CONSTRUCTION.—

(A) OTHER FEDERAL LAW.—An agreement under paragraph (1) shall not effect a person's obligation or an entity's obligation to provide notice of a breach of security or similar event under any other Federal law.

(B) NO PREEMPTION PRIOR TO VALID AGREEMENT.—Subsections (a)(2) and (b) of section 807 shall not apply to a breach of security that occurs before a valid agreement under paragraph (1) is in effect.

(c) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 802 or 803 of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title. Any covered entity who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(3) LIMITATION.—In promulgating rules under this title, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(d) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity who violates section 802 or 803 of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

(A) to enjoin further violation of such section by the defendant;

(B) to compel compliance with such section; or

(C) to obtain civil penalties in the amount determined under paragraph (2).

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 802.—For purposes of paragraph (1)(C) with regard to a violation of section 802, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such section by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 803.—For purposes of paragraph (1)(C) with regard to a violation of section 803, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $11,000. Each failure to send notification as required under section 803 to a resident of the State shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) and in clauses (i) and (ii) of subparagraph (C) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection shall not exceed—

(i) $5,000,000 for each violation of section 802; and

(ii) $5,000,000 for all violations of section 803 resulting from a single breach of security.

(3) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon commencing such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this title, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this title alleged in the complaint.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State—

(A) to conduct investigations;

(B) to administer oaths or affirmations; or

(C) to compel the attendance of witnesses or the production of documentary and other evidence.

(e) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 803.—It shall be an affirmative defense to an enforcement action brought under subsection (c), or a civil action brought under subsection (d), based on a violation of section 803, that all of the personal information contained in the data in electronic form that was acquired or accessed as a result of a breach of security of the defendant is public record information that is lawfully made available to the general public from Federal, State, or local government records and was acquired by the defendant from such records.

(f) NOTICE TO LAW ENFORCEMENT; CIVIL ENFORCEMENT BY ATTORNEY GENERAL.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of section 804.

(2) PENALTIES.—

(A) IN GENERAL.—Upon proof of such conduct by a preponderance of the evidence, a covered entity shall be subject to a civil penalty of not more than $1,000 per individual whose personal information was or is reasonably believed to have been accessed or acquired as a result of the breach of security that is the basis of the violation, up to a maximum of $100,000 per day while such violation persists.

(B) LIMITATIONS.—The total amount of the civil penalty assessed under this subsection against a covered entity for acts or omissions relating to a single breach of security shall not exceed $1,000,000, unless the conduct constituting a violation of section 804 was willful or intentional, in which case an additional civil penalty of up to $1,000,000 may be imposed.

(C) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraphs (A) and (B) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) INJUNCTIVE ACTIONS.—If it appears that a covered entity has engaged, or is engaged, in any act or practice that constitutes a violation of section 804, the Attorney General may petition an appropriate United States district court for an order enjoining such practice or enforcing compliance with section 804.

(4) ISSUANCE OF ORDER.—A court may issue such an order under paragraph (3) if it finds that the conduct in question constitutes a violation of section 804.

(g) CONCEALMENT OF BREACHES OF SECURITY.—

(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1041. Concealment of breaches of security involving personal information

''(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act of 2012, intentionally and willfully conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.

''(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of this title.

''(c) ENFORCEMENT AUTHORITY.—

''(1) IN GENERAL.—The United States Secret Service and the Federal Bureau of Investigation shall have the authority to investigate offenses under this section.

''(2) CONSTRUCTION.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.''.

(2) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of breaches of security involving personal information.''.

SEC. 806. DEFINITIONS.

In this title:

(1) BREACH OF SECURITY.—

(A) IN GENERAL.—The term ''breach of security'' means compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of personal information from a covered entity.

(B) EXCLUSIONS.—The term'' breach of security'' does not include—

(i) a good faith acquisition of personal information by a covered entity, or an employee or agent of a covered entity, if the personal information is not subject to further use or unauthorized disclosure;

(ii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or an intelligence agency of the United States, a State, or a political subdivision of a State; or

(iii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) COVERED ENTITY.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes personal information.

(4) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.

(5) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated by the Secretary of Homeland Security under section 804.

(6) ENCRYPTION.—The term ''encryption'' means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management and safeguards of such keys to protect the integrity of the encryption.

(7) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the identity of such other person, including any contact that violates section 1028A of title 18, United States Code.

(8) MAJOR CREDIT REPORTING AGENCY.—The term ''major credit reporting agency'' means a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis within the meaning of section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(9) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means any information or compilation of information in electronic or digital form that includes—

(i) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction; or

(ii) an individual's first and last name or first initial and last name in combination with—

(I) a non-truncated social security number, driver's license number, passport number, or alien registration number, or other similar number issued on a government document used to verify identity;

(II) unique biometric data such as a finger print, voice print, retina or iris image, or any other unique physical representation;

(III) a unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(IV) 2 of the following:

(aa) Home address or telephone number.

(bb) Mother's maiden name, if identified as such.

(cc) Month, day, and year of birth.

(B) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that the definition under subparagraph (A) is not reasonably sufficient to protect individuals from identify theft, fraud, or other unlawful conduct, the Commission by rule promulgated under section 553 of title 5, United States Code, may modify the definition of ''personal information'' under subparagraph (A) to the extent the modification will not unreasonably impede interstate commerce.

(10) PUBLIC RECORD INFORMATION.—The term ''public record information'' means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

(11) SERVICE PROVIDER.—The term ''service provider'' means a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such person transmits, routes, or stores, or for which such person provides connections. Any such person shall be treated as a service provider under this title only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

SEC. 807. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This title supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this title, that expressly—

(1) requires information security practices and treatment of data containing personal information similar to any of those required under section 802; or

(2) requires notification to individuals of a breach of security as defined in section 806.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 805(d) may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this title.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—Except as provided in subsection (a) of this section, this subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This title shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) any other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this title may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 808. APPLICABILITY OF SECTION 631 OF THE COMMUNICATIONS ACT OF 1934.

(a) IN GENERAL.—To the extent that a cable operator (as defined under section 631 of the Communications Act of 1934 (47 U.S.C. 551)) is subject to a requirement regarding personal information (as defined in section 806 of this Act)—

(1) under this title that is in conflict with a requirement under section 631 of the Communications Act of 1934 (47 U.S.C. 551), each applicable section of this Act shall control (including enforcement); and

(2) under section 631 of the Communications Act of 1934 (47 U.S.C. 551) that is in addition to or different from a requirement under this title, each applicable subsection of section 631 of the Communications Act of 1934 (47 U.S.C. 551) shall remain in effect (including enforcement and right of action).

(b) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this title shall preclude the application of section 631 of the Communications Act of 1934 (47 U.S.C. 551), to information that is not included in the definition of personal information under section 806 of this Act.

SEC. 809. EFFECTIVE DATE.

This title shall take effect 1 year after the date of enactment of this Act.

SA 2701. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike section 701.

SA 2702. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 169, strike line 15 and all that follows through page 172, line 25.

Page 189, beginning on line 22, strike ''performing, monitoring, operating countermeasures, or''.

Page 196, strike lines 10, 11, and 12.

Beginning on page 205, strike line 15 and all that follows through page 206, line 2.

SA 2703. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title VII and insert the following:

TITLE VII—INFORMATION SHARING

SEC. 701. 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. 702. 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-Federal 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 703(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 703(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 703(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 703(b) and the special requirements for Federal entities under section 703(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 703, 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 authorities 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. 703. 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 section, 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 obtained 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 received 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 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 enforcement access and use pursuant to paragraph (2);

(ii) a review of the type of information shared with a Federal cybersecurity exchange;

(iii) a review of the actions taken by Federal entities based on such information;

(iv) appropriate metrics to determine the impact of the sharing of such information with a Federal cybersecurity exchange on privacy and civil liberties;

(v) a list of Federal entities receiving such information;

(vi) a review of the sharing of such information among Federal entities to identify inappropriate stovepiping of shared information; and

(vii) any recommendations of the inspectors general for improvements or modifications to the authorities under this title.

(C) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

(6) SANCTIONS.—The head of each Federal entity that conducts activities under this title shall develop 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. 704. SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.

(a) SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.—The procedures established under section 702(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 702(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. 705. 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 the voluntary disclosure of a lawfully obtained cybersecurity threat indicator—

(1) to a cybersecurity exchange pursuant to section 703(a);

(2) by a provider of cybersecurity services to a customer of that provider;

(3) 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

(4) to any other private entity under section 701(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. 706. 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 cybersecurity 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 Government 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 704. 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. 707. 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) CYBERSECURITY CRIME.—The term ''cybersecurity crime'' means the violation of a provision of State or Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, enacted or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99–474; 100 Stat. 1213).

(3) CYBERSECURITY EXCHANGE.—The term ''cybersecurity exchange'' means any governmental entity or private entity designated by the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to receive and distribute cybersecurity threat indicators under section 703(a).

(4) CYBERSECURITY SERVICES.—The term ''cybersecurity services'' means products, goods, or services intended to detect, mitigate, or prevent cybersecurity threats.

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' means any action that may result in unauthorized access to, exfiltration of, manipulation 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) 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.

(12) 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.

(13) 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.

(14) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' means a private entity or a governmental entity other than a Federal entity.

(15) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(16) 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.

(17) 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.

(18) 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.

(19) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(20) THIRD PARTY.—The term ''third party'' includes Federal entities and non-Federal entities.

SA 2704. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 10, strike lines 16 through 25 and insert the following:

and the member agencies; and

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

(d) PRESIDENTIAL AUTHORITY.—The Chairperson may take emergency action to fulfill the responsibilities of the Council if—

(1) the Chairperson determines that the emergency action is necessary to prevent or mitigate an imminent cybersecurity threat; and

(2) the President approves the emergency action.

SA 2705. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 153, strike lines 17 through 20 and insert the following:

Not later than 1 year after the date of enactment of this Act, the Secretary of Energy, in consultation with the Secretary, the Secretary of Defense, the Director of National Intelligence, the Director of the National Institute of Standards and Technology, the Federal Energy Regulatory Commission, and the Electric Reliability Organization (as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)) shall submit to Congress a report on—

SA 2706. Mrs. MURRAY submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, strike lines 12 and 13 and insert the following:

as appropriate;

(7) the National Guard Bureau; and

(8) the Department.

At the end of title IV, add the following:

SEC. 416. REPORT ON ROLES AND MISSIONS OF THE NATIONAL GUARD IN STATE STATUS IN SUPPORT OF THE CYBERSECURITY EFFORTS OF THE FEDERAL GOVERNMENT.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall, in consultation with the Secretary of Defense and the Chief of the National Guard Bureau, submit to the appropriate committees of Congress a report on the roles and missions of the National Guard in State status (commonly referred to as ''title 32 status'') in support of the cybersecurity efforts of the Department of Homeland Security, the Department of Defense, and other departments and agencies of the Federal Government.

(b) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) A description of the current roles and missions of the National Guard in State status in support of the cybersecurity efforts of the Federal Government, and a description of the policies and authorities governing the discharge of such roles and missions.

(2) A description of potential roles and missions for the National Guard in State status in support of the cybersecurity efforts of the Federal Government, a description of the policies and authorities to govern the discharge of such roles and missions, and recommendations for such legislative or administrative actions as may be required to establish and implement such roles and missions.

(3) An assessment of the feasability and advisability of public-private partnerships on homeland cybersecurity missions involving the National Guard in State status, including the advisability of using pilot programs to evaluate feasability and advisability of such partnerships.

(c) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate; and

(2) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives.

SA 2707. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 34, strike lines 3 through 17 and insert the following:

(1) provide a Federal agency with additional or greater authority for regulating the security of critical cyber infrastructure than any authority the Federal agency has under other law;

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

(3) permit any owner (including a certified

SA 2708. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 182, strike lines 7 through 16 and insert the following:

(d) PROTECTION OF INFORMATION FROM DISCLOSURE.—A cybersecurity threat indicator or any other information that was developed, submitted, obtained, or shared in connection with the implementation of this section shall be—

(1) exempt from disclosure under section 552(b)(3) of title 5, United States Code;

(2) exempt from disclosure under any State, local, or tribal law or regulation that requires public disclosure of information or records by a public or quasi-public entity; and

(3) treated as voluntarily shared information under section 552 of title 5, United States Code, or any comparable State, local, or tribal law or regulation.

SA 2709. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 23, strike line 18 and all that follows through page 25, line 8.

SA 2710. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 20, strike line 6 and all that follows through page 22, line 14, and insert the following:

date on which the top-level assessment is completed under section 102(a)(2)(A), 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 organizations, 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 on which the top-level assessment is completed under section 102(a)(2)(A), the Council shall—

(i) adopt any cybersecurity practices proposed under subsection (a) that adequately remediate or mitigate identified cyber risks and any associated consequences 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 on which the top-level assessment is completed under section

102(a)(2)(A), not later than 1 year after the date on which the top-level assessment is completed under section 102(a)(2)(A) the Council shall adopt cybersecurity

---

SA 2711. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 43, beginning on line 14, strike ''section 104(c)(1) and section 106'' and insert the following: ''sections 104(c)(1), 106, and 704(d)''.

SA 2712. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 41, strike line 5 and all that follows through page 42, line 4, and insert the following:

date on which the Council completes the adoption of cybersecurity practices under section 103(b)(2), 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; and

(C) whether additional legislative authority

SA 2713. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—CYBER ATTACKS INVOLVING DRONES

SEC. __01. DEFINITIONS.

In this title—

(1) the term ''drone'' means any aerial vehicle that—

(A) does not carry a human operator;

(B) uses aerodynamic or aerostatic forces to provide vehicle lift;

(C) can fly autonomously or be piloted remotely;

(D) can be expendable or recoverable; and

(E) can carry a lethal or nonlethal payload; and

(2) the term ''law enforcement party'' means a person or entity authorized by law, or funded, in whole or in part, by the Government of the United States, to investigate or prosecute offenses against the United States.

SEC. __02. PROTECTION AGAINST UNAUTHORIZED USE OF DRONES.

(a) IN GENERAL.—No drone may be deployed or otherwise used by any officer, employee, or contractor of the Federal Government or by a person or entity acting under the authority of, or funded in whole or in part by, the Government of the United States, until the National Cybersecurity Council or other person, division, or entity placed in charge of cybersecurity efforts in the United States certifies that any such drone is immune from a cyber attack or other compromise of control, navigation, or data.

(b) EMPLOYMENT OF CERTIFIED DRONES.—Except as provided in section __03, no officer, employee, or contractor of the Federal Government or any person or entity acting under the authority of, or funded in whole or in part by, the Government of the United States shall use a drone to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation, except to the extent authorized in a warrant that satisfies the requirements of the Fourth Amendment to the Constitution of the United States.

SEC. __03. EXCEPTIONS.

This title does not prohibit any of the following:

(1) PATROL OF BORDERS.—The use of a drone certified under section __02(a) to patrol national borders to prevent or deter illegal entry of any persons or illegal substances.

(2) EXIGENT CIRCUMSTANCES.—The use of a drone certified under section __02(a) by a law enforcement party when exigent circumstances exist. For the purposes of this paragraph, exigent circumstances exist when the law enforcement party possesses reasonable suspicion that under particular circumstances, swift action to prevent imminent danger to life is necessary.

(3) HIGH RISK.—The use of a drone certified under section __02(a) to counter a high risk of a terrorist attack by a specific individual or organization, when the Secretary of Homeland Security determines credible intelligence indicates there is such a risk.

SEC. __04. REMEDIES FOR VIOLATION.

Any aggrieved party may in a civil action obtain all appropriate relief to prevent or remedy a violation of this title.

SEC. __05. PROHIBITION ON USE OF EVIDENCE.

No evidence obtained or collected in violation of this title may be admissible as evidence in a criminal prosecution in any court of law in the United States.

SA 2714. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 23, strike line 19 and all that follows through page 34, line 19, and insert the following:

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide a Federal agency that has authority for regulating the security of critical cyber infrastructure any authority in addition to 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 established 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) 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;

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

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

(h) NO LIMITATION ON CONTRACTUAL LIABILITY.—No limitation on liability or good faith defense provided under this section shall apply to any civil claim against a private entity arising under contract law.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 199, between lines 12 and 13, insert the following:

SA 2716. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. DISTRICT OF COLUMBIA PAIN-CAPABLE UNBORN CHILD PROTECTION ACT.

(a) SHORT TITLE.—This section may be cited as the ''District of Columbia Pain-Capable Unborn Child Protection Act''.

(b) LEGISLATIVE FINDINGS.—Congress finds and declares the following:

(1) Pain receptors (nociceptors) are present throughout the unborn child's entire body and nerves link these receptors to the brain's thalamus and subcortical plate by no later than 20 weeks after fertilization.

(2) By 8 weeks after fertilization, the unborn child reacts to touch. After 20 weeks, the unborn child reacts to stimuli that would be recognized as painful if applied to an adult human, for example, by recoiling.

(3) In the unborn child, application of such painful stimuli is associated with significant increases in stress hormones known as the stress response.

(4) Subjection to such painful stimuli is associated with long-term harmful neurodevelopmental effects, such as altered pain sensitivity and, possibly, emotional, behavioral, and learning disabilities later in life.

(5) For the purposes of surgery on unborn children, fetal anesthesia is routinely administered and is associated with a decrease in stress hormones compared to their level when painful stimuli are applied without such anesthesia.

(6) The position, asserted by some medical experts, that the unborn child is incapable of experiencing pain until a point later in pregnancy than 20 weeks after fertilization predominately rests on the assumption that the ability to experience pain depends on the cerebral cortex and requires nerve connections between the thalamus and the cortex. However, recent medical research and analysis, especially since 2007, provides strong evidence for the conclusion that a functioning cortex is not necessary to experience pain.

(7) Substantial evidence indicates that children born missing the bulk of the cerebral cortex, those with hydranencephaly, nevertheless experience pain.

(8) In adult humans and in animals, stimulation or ablation of the cerebral cortex does not alter pain perception, while stimulation or ablation of the thalamus does.

(9) Substantial evidence indicates that structures used for pain processing in early development differ from those of adults, using different neural elements available at specific times during development, such as the subcortical plate, to fulfill the role of pain processing.

(10) The position, asserted by some commentators, that the unborn child remains in a coma-like sleep state that precludes the unborn child experiencing pain is inconsistent with the documented reaction of unborn children to painful stimuli and with the experience of fetal surgeons who have found it necessary to sedate the unborn child with anesthesia to prevent the unborn child from

engaging in vigorous movement in reaction to invasive surgery.

(11) Consequently, there is substantial medical evidence that an unborn child is capable of experiencing pain at least by 20 weeks after fertilization, if not earlier.

(12) It is the purpose of the Congress to assert a compelling governmental interest in protecting the lives of unborn children from the stage at which substantial medical evidence indicates that they are capable of feeling pain.

(13) The compelling governmental interest in protecting the lives of unborn children from the stage at which substantial medical evidence indicates that they are capable of feeling pain is intended to be separate from and independent of the compelling governmental interest in protecting the lives of unborn children from the stage of viability, and neither governmental interest is intended to replace the other.

(14) The District Council of the District of Columbia, operating under authority delegated by Congress, repealed all limitations on abortion at any stage of pregnancy, effective April 29, 2004.

(15) Article I, section 8 of the Constitution of the United States of America provides that the Congress shall ''exercise exclusive Legislation in all Cases whatsoever'' over the District established as the seat of government of the United States, now known as the District of Columbia. The constitutional responsibility for the protection of pain-capable unborn children within the Federal District resides with the Congress.

(c) DISTRICT OF COLUMBIA PAIN-CAPABLE UNBORN CHILD PROTECTION.—

(1) IN GENERAL.—Chapter 74 of title 18, United States Code, is amended by inserting after section 1531 the following:

''§ 1532. District of Columbia pain-capable unborn child protection

''(a) UNLAWFUL CONDUCT.—Notwithstanding any other provision of law, including any legislation of the District of Columbia under authority delegated by Congress, it shall be unlawful for any person to perform an abortion within the District of Columbia, or attempt to do so, unless in conformity with the requirements set forth in subsection (b).

''(b) REQUIREMENTS FOR ABORTIONS.—

''(1) The physician performing or attempting the abortion shall first make a determination of the probable post-fertilization age of the unborn child or reasonably rely upon such a determination made by another physician. In making such a determination, the physician shall make such inquiries of the pregnant woman and perform or cause to be performed such medical examinations and tests as a reasonably prudent physician, knowledgeable about the case and the medical conditions involved, would consider necessary to make an accurate determination of post-fertilization age.

''(2)(A) Except as provided in subparagraph (B), the abortion shall not be performed or attempted, if the probable post-fertilization age, as determined under paragraph (1), of the unborn child is 20 weeks or greater.

''(B) Subject to subparagraph (C), subparagraph (A) does not apply if, in reasonable medical judgment, the abortion is necessary to save the life of a pregnant woman whose life is endangered by a physical disorder, physical illness, or physical injury, including a life-endangering physical condition caused by or arising from the pregnancy itself, but not including psychological or emotional conditions or any claim or diagnosis that the woman will engage in conduct which she intends to result in her death.

''(C) A physician terminating or attempting to terminate a pregnancy under the exception provided by subparagraph (B) may do so only in the manner which, in reasonable medical judgment, provides the best opportunity for the unborn child to survive, unless, in reasonable medical judgment, termination of the pregnancy in that manner would pose a greater risk of—

''(i) the death of the pregnant woman; or

''(ii) the substantial and irreversible physical impairment of a major bodily function, not including psychological or emotional conditions, of the pregnant woman;

than would other available methods.

''(c) CRIMINAL PENALTY.—Whoever violates subsection (a) shall be fined under this title or imprisoned for not more than 2 years, or both.

''(d) BAR TO PROSECUTION.—A woman upon whom an abortion in violation of subsection (a) is performed or attempted may not be prosecuted under, or for a conspiracy to violate, subsection (a), or for an offense under section 2, 3, or 4 based on such a violation.

''(e) CIVIL REMEDIES.—

''(1) CIVIL ACTION BY WOMAN ON WHOM THE ABORTION IS PERFORMED.—A woman upon whom an abortion has been performed or attempted in violation of subsection (a), may in a civil action against any person who engaged in the violation obtain appropriate relief.

''(2) CIVIL ACTION BY RELATIVES.—The father of an unborn child who is the subject of an abortion performed or attempted in violation of subsection (a), or a maternal grandparent of the unborn child if the pregnant woman is an unemancipated minor, may in a civil action against any person who engaged in the violation, obtain appropriate relief, unless the pregnancy resulted from the plaintiff's criminal conduct or the plaintiff consented to the abortion.

''(3) APPROPRIATE RELIEF.—Appropriate relief in a civil action under this subsection includes—

''(A) objectively verifiable money damages for all injuries, psychological and physical, occasioned by the violation of this section;

''(B) statutory damages equal to three times the cost of the abortion; and

''(C) punitive damages.

''(4) INJUNCTIVE RELIEF.—

''(A) IN GENERAL.—A qualified plaintiff may in a civil action obtain injunctive relief to prevent an abortion provider from performing or attempting further abortions in violation of this section.

''(B) DEFINITION.—In this paragraph the term 'qualified plaintiff' means—

''(i) a woman upon whom an abortion is performed or attempted in violation of this section;

''(ii) any person who is the spouse, parent, sibling or guardian of, or a current or former licensed health care provider of, that woman; or

''(iii) the United States Attorney for the District of Columbia.

''(5) ATTORNEYS FEES FOR PLAINTIFF.—The court shall award a reasonable attorney's fee as part of the costs to a prevailing plaintiff in a civil action under this subsection.

''(6) ATTORNEYS FEES FOR DEFENDANT.—If a defendant in a civil action under this section prevails and the court finds that the plaintiff's suit was frivolous and brought in bad faith, the court shall also render judgment for a reasonable attorney's fee in favor of the defendant against the plaintiff.

''(7) AWARDS AGAINST WOMAN.—Except under paragraph (6), in a civil action under this subsection, no damages, attorney's fee or other monetary relief may be assessed against the woman upon whom the abortion was performed or attempted.

''(f) PROTECTION OF PRIVACY IN COURT PROCEEDINGS.—

''(1) IN GENERAL.—Except to the extent the Constitution or other similarly compelling reason requires, in every civil or criminal action under this section, the court shall make such orders as are necessary to protect the anonymity of any woman upon whom an abortion has been performed or attempted if she does not give her written consent to such disclosure. Such orders may be made upon motion, but shall be made sua sponte if not otherwise sought by a party.

''(2) ORDERS TO PARTIES, WITNESSES, AND COUNSEL.—The court shall issue appropriate orders under paragraph (1) to the parties, witnesses, and counsel and shall direct the sealing of the record and exclusion of individuals from courtrooms or hearing rooms to the extent necessary to safeguard her identity from public disclosure. Each such order shall be accompanied by specific written findings explaining why the anonymity of the woman must be preserved from public disclosure, why the order is essential to that end, how the order is narrowly tailored to serve that interest, and why no reasonable less restrictive alternative exists.

''(3) PSEUDONYM REQUIRED.—In the absence of written consent of the woman upon whom an abortion has been performed or attempted, any party, other than a public official, who brings an action under paragraphs (1), (2), or (4) of subsection (e) shall do so under a pseudonym.

''(4) LIMITATION.—This subsection shall not be construed to conceal the identity of the plaintiff or of witnesses from the defendant or from attorneys for the defendant.

''(g) REPORTING.—

''(1) DUTY TO REPORT.—Any physician who performs or attempts an abortion within the District of Columbia shall report that abortion to the relevant District of Columbia health agency (hereinafter in this section referred to as the 'health agency') on a schedule and in accordance with forms and regulations prescribed by the health agency.

''(2) CONTENTS OF REPORT.—The report shall include the following:

''(A) POST-FERTILIZATION AGE.—For the determination of probable postfertilization age of the unborn child, whether ultrasound was employed in making the determination, and the week of probable post-fertilization age that was determined.

''(B) METHOD OF ABORTION.—Which of the following methods or combination of methods was employed:

''(i) Dilation, dismemberment, and evacuation of fetal parts also known as 'dilation and evacuation'.

''(ii) Intra-amniotic instillation of saline, urea, or other substance (specify substance) to kill the unborn child, followed by induction of labor.

''(iii) Intracardiac or other intra-fetal injection of digoxin, potassium chloride, or other substance (specify substance) intended to kill the unborn child, followed by induction of labor.

''(iv) Partial-birth abortion, as defined in section 1531.

''(v) Manual vacuum aspiration without other methods.

''(vi) Electrical vacuum aspiration without other methods.

''(vii) Abortion induced by use of mifepristone in combination with misoprostol; or

''(viii) if none of the methods described in the other clauses of this subparagraph was employed, whatever method was employed.

''(C) AGE OF WOMAN.—The age or approximate age of the pregnant woman.

''(D) COMPLIANCE WITH REQUIREMENTS FOR EXCEPTION.—The facts relied upon and the basis for any determinations required to establish compliance with the requirements

for the exception provided by subsection (b)(2).

''(3) EXCLUSIONS FROM REPORTS.—

''(A) A report required under this subsection shall not contain the name or the address of the woman whose pregnancy was terminated, nor shall the report contain any other information identifying the woman.

''(B) Such report shall contain a unique Medical Record Number, to enable matching the report to the woman's medical records.

''(C) Such reports shall be maintained in strict confidence by the health agency, shall not be available for public inspection, and shall not be made available except—

''(i) to the United States Attorney for the District of Columbia or that Attorney's delegate for a criminal investigation or a civil investigation of conduct that may violate this section; or

''(ii) pursuant to court order in an action under subsection (e).

''(4) PUBLIC REPORT.—Not later than June 30 of each year beginning after the date of enactment of this paragraph, the health agency shall issue a public report providing statistics for the previous calendar year compiled from all of the reports made to the health agency under this subsection for that year for each of the items listed in paragraph (2). The report shall also provide the statistics for all previous calendar years during which this section was in effect, adjusted to reflect any additional information from late or corrected reports. The health agency shall take care to ensure that none of the information included in the public reports could reasonably lead to the identification of any pregnant woman upon whom an abortion was performed or attempted.

''(5) FAILURE TO SUBMIT REPORT.—

''(A) LATE FEE.—Any physician who fails to submit a report not later than 30 days after the date that report is due shall be subject to a late fee of $1,000 for each additional 30-day period or portion of a 30-day period the report is overdue.

''(B) COURT ORDER TO COMPLY.—A court of competent jurisdiction may, in a civil action commenced by the health agency, direct any physician whose report under this subsection is still not filed as required, or is incomplete, more than 180 days after the date the report was due, to comply with the requirements of this section under penalty of civil contempt.

''(C) DISCIPLINARY ACTION.—Intentional or reckless failure by any physician to comply with any requirement of this subsection, other than late filing of a report, constitutes sufficient cause for any disciplinary sanction which the Health Professional Licensing Administration of the District of Columbia determines is appropriate, including suspension or revocation of any license granted by the Administration.

''(6) FORMS AND REGULATIONS.—Not later than 90 days after the date of the enactment of this section, the health agency shall prescribe forms and regulations to assist in compliance with this subsection.

''(7) EFFECTIVE DATE OF REQUIREMENT.—Paragraph (1) of this subsection takes effect with respect to all abortions performed on and after the first day of the first calendar month beginning after the effective date of such forms and regulations.

''(h) DEFINITIONS.—In this section the following definitions apply:

''(1) ABORTION.—The term 'abortion' means the use or prescription of any instrument, medicine, drug, or any other substance or device—

''(A) to intentionally kill the unborn child of a woman known to be pregnant; or

''(B) to otherwise intentionally terminate the pregnancy of a woman known to be pregnant with an intention other than to increase the probability of a live birth, to preserve the life or health of the child after live birth, or to remove a dead unborn child who died as the result of natural causes in utero, accidental trauma, or a criminal assault on the pregnant woman or her unborn child, and which causes the premature termination of the pregnancy.

''(2) ATTEMPT AN ABORTION.—The term 'attempt', with respect to an abortion, means conduct that, under the circumstances as the actor believes them to be, constitutes a substantial step in a course of conduct planned to culminate in performing an abortion in the District of Columbia.

''(3) FERTILIZATION.—The term 'fertilization' means the fusion of human spermatozoon with a human ovum.

''(4) HEALTH AGENCY.—The term 'health agency' means the Department of Health of the District of Columbia or any successor agency responsible for the regulation of medical practice.

''(5) PERFORM.—The term 'perform', with respect to an abortion, includes induce an abortion through a medical or chemical intervention including writing a prescription for a drug or device intended to result in an abortion.

''(6) PHYSICIAN.—The term 'physician' means a person licensed to practice medicine and surgery or osteopathic medicine and surgery, or otherwise licensed to legally perform an abortion.

''(7) POST-FERTILIZATION AGE.—The term 'post-fertilization age' means the age of the unborn child as calculated from the fusion of a human spermatozoon with a human ovum.

''(8) PROBABLE POST-FERTILIZATION AGE OF THE UNBORN CHILD.—The term 'probable postfertilization age of the unborn child' means what, in reasonable medical judgment, will with reasonable probability be the postfertilization age of the unborn child at the time the abortion is planned to be performed or induced.

''(9) REASONABLE MEDICAL JUDGMENT.—The term 'reasonable medical judgment' means a medical judgment that would be made by a reasonably prudent physician, knowledgeable about the case and the treatment possibilities with respect to the medical conditions involved.

''(10) UNBORN CHILD.—The term 'unborn child' means an individual organism of the species homo sapiens, beginning at fertilization, until the point of being born alive as defined in section 8(b) of title 1.

''(11) UNEMANCIPATED MINOR.—The term 'unemancipated minor' means a minor who is subject to the control, authority, and supervision of a parent or guardian, as determined under the law of the State in which the minor resides.

''(12) WOMAN.—The term 'woman' means a female human being whether or not she has reached the age of majority.''.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 74 of title 18, United States Code, is amended by adding at the end the following new item:

''1532. District of Columbia pain-capable unborn child protection.''.

(3) CHAPTER HEADING AMENDMENTS.—

(A) CHAPTER HEADING IN CHAPTER.—The chapter heading for chapter 74 of title 18, United States Code, is amended by striking ''**PARTIAL BIRTH ABORTIONS**'' and inserting ''**ABORTIONS**''.

(B) TABLE OF CHAPTERS FOR PART I.—The item relating to chapter 74 in the table of chapters at the beginning of part I of title 18, United States Code, is amended by striking ''**PARTIAL BIRTH ABORTIONS**'' and inserting ''**ABORTIONS**''.

SA 2717. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 121, beginning on line 16, strike ''summer enrichment programs, to be provided by nonprofit organizations, in math, computer programming'' and insert ''summer enrichment programs and programs offered before or after normal school hours, to be provided by nonprofit organizations, in math, computer science, computer programming''.

On page 125, line 12, insert '', such as mentors from private sector entities'' after ''appropriate''.

SA 2718. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VI, add the following:

SEC. 606. COOPERATION WITH NATO ON CYBER DEFENSE.

(a) FINDINGS.—Congress makes the following findings:

(1) The November 2010 NATO Lisbon Summit Declaration asserts, ''Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber-attack against systems of critical importance to the Alliance.''

(2) In an April 2012 speech, Secretary of State Hillary Clinton stated, ''There is a steady drumbeat of [cyber] attacks on governments, on businesses, on all kinds of networks every single day. And we have to be in a position to protect ourselves and, under Article 5, protect our NATO partners. There have been some rather significant attacks on NATO partners over the last several years that have caused consternation because of the damage done to classified information, and so therefore we are in the process of working toward a joint capability.''

(b) SENSE OF CONGRESS.—It is the sense of Congress that it is in the interest of the United States to continue to work with NATO members, partners, and allies to develop the necessary cyber capabilities, including prevention, detection, recovery, and response, to deter aggression and prevent coercion through the cyber domain.

(c) CONGRESSIONAL BRIEFING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, after consultation with the heads of relevant Federal agencies, shall brief Congress on—

(A) the ability of NATO to detect, assess, prevent, defend, and recover from cyber attacks to its critical systems, networks, and other combat equipment;

(B) implementation of the NATO Policy on Cyber Defense;

(C) development of NATO's Computer Incident Response Capability;

(D) development and contributions of NATO's Cooperative Cyber Defense Center of Excellence; and

(E) NATO cooperation with other international organizations, including the European Union, the Council of Europe, the United Nations, and the Organization for the Security and Co-operation in Europe.

(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 Secretary of State, in coordination with the Secretary of Defense, shall consult with and obtain information relevant to the briefing from the head of each relevant Federal agency.

(3) PERIODIC UPDATES.—The Secretary of State shall provide periodic briefings to Congress to highlight significant developments relating to the issues described in paragraph (1).

SA 2719. Mr. KOHL (for himself, Mr. WHITEHOUSE, and Mr. COONS) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE __—ECONOMIC ESPIONAGE PENALTY ENHANCEMENT

SEC. __01. SHORT TITLE.

This title may be cited as the ''Economic Espionage Penalty Enhancement Act of 2012''.

SEC. __02. PROTECTING U.S. BUSINESSES FROM FOREIGN ESPIONAGE.

(a) FOR OFFENSES COMMITTED BY INDIVIDUALS.—Section 1831(a) of title 18, United States Code, is amended in the matter following paragraph (5)—

(1) by striking ''15 years'' and inserting ''20 years''; and

(2) by striking ''not more than $500,000'' and inserting ''not more than $5,000,000''.

(b) FOR OFFENSES COMMITTED BY ORGANIZATIONS.—Section 1831(b) of title 18, United States Code, is amended by striking ''not more than $10,000,000'' and inserting ''not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided''.

SEC. __03. REVIEW BY THE UNITED STATES SENTENCING COMMISSION.

(a) IN GENERAL.—Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of offenses relating to the transmission or attempted transmission of a stolen trade secret outside of the United States or economic espionage, in order to reflect the intent of Congress that penalties for such offenses under the Federal sentencing guidelines and policy statements appropriately reflect the seriousness of these offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses.

(b) REQUIREMENTS.—In carrying out this section, the United States Sentencing Commission shall—

(1) consider the extent to which the Federal sentencing guidelines and policy statements appropriately account for the simple misappropriation of a trade secret, including the sufficiency of the existing enhancement for these offenses to address the seriousness of this conduct;

(2) consider whether additional enhancements in the Federal sentencing guidelines and policy statements are appropriate to account for—

(A) the transmission or attempted transmission of a stolen trade secret outside of the United States; and

(B) the transmission or attempted transmission of a stolen trade secret outside of the United States that is committed or attempted to be committed for the benefit of a foreign government, foreign instrumentality, or foreign agent;

(3) ensure the Federal sentencing guidelines and policy statements reflect the seriousness of these offenses and the need to deter such conduct;

(4) ensure reasonable consistency with other relevant directives, Federal sentencing guidelines and policy statements, and related Federal statutes;

(5) make any necessary conforming changes to the Federal sentencing guidelines and policy statements; and

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

(c) CONSULTATION.—In carrying out the review required under this section, the Commission shall consult with individuals or groups representing law enforcement, owners of trade secrets, victims of economic espionage offenses, the Department of Justice, the Department of State, the Department of Homeland Security, and the Office of the United States Trade Representative.

(d) REVIEW.—Not later than 180 days after the date of enactment of this title, the Commission shall complete its consideration and review under this section.

SA 2720. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 106, line 15, insert '', the Director of the Office of Management and Budget,'' after ''the Secretary''.

On page 110, line 8, strike ''to the extent practicable,''.

On page 115, line 22, strike '', to the extent practicable,''.

SA 2721. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PERFORMANCE OF CYBERSECURITY AUTHORITIES BY GOVERNMENT EMPLOYEES.

(a) CYBERSECURITY FUNCTIONS.—Section 5(2) of the Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) is amended—

(1) by redesignating subparagraph (C) as subparagraph (D); and

(2) by inserting after subparagraph (B) the following:

''(C) CYBERSECURITY FUNCTIONS INCLUDED.—The term includes any authority provided to the Federal Government under title I, II, V, or VII, or an amendment made by title I, II, V, or VII, of the Cybersecurity Act of 2012 that is not explicitly authorized to be performed by a non-Federal individual or entity.''.

(b) CLARIFICATION OF PROHIBITION ON CONTRACTORS PERFORMING INHERENTLY GOVERNMENTAL FUNCTIONS.—The Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) is amended by inserting after section 2 the following:

''SEC. 2A. PROHIBITION ON CONTRACTORS PERFORMING INHERENTLY GOVERNMENTAL FUNCTIONS.

''The head of an executive agency or employee of an executive agency may not enter into a contract or any other agreement under which an individual or entity that is not an employee of the Federal Government performs an inherently governmental function.''.

SA 2722. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 137, strike line 6 and all that follows through page 139, line 15, and insert the following:

SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

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

SA 2723. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

SEC. 416. GAO STUDY AND REPORT ON SMALL BUSINESS CYBERSECURITY ISSUES.

(a) STUDY.—The Comptroller General of the United States shall conduct a study identifying—

(1) small business cybersecurity concerns;

(2) existing efforts by Federal agencies having responsibility to assist small businesses with cybersecurity issues (including the Department of Homeland Security, the Federal Trade Commission, the Small Business Administration, and the National Institute of Standards and Technology) to raise small business awareness of cybersecurity issues; and

(3) ways the Federal agencies described in paragraph (2) plan to improve small business awareness of and preparedness for cybersecurity issues.

(b) REPORT.—Not later than 18 months after the date of enactment of this Act, the Comptroller General shall submit to Congress a report containing—

(1) the results of the study conducted under subsection (a); and

(2) recommendations, if any, based on the results of the study conducted under subsection (a).

SA 2724. Ms. MIKULSKI submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike section 404 and insert the following:

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

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary and the Director of the Office of Personnel Management, shall carry out a Federal Cyber Scholarship-for-Service program—

(1) to increase the capacity of institutions of higher education to produce cybersecurity professionals; and

(2) to recruit and train the next generation of information technology professionals, industry control 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 carried out under subsection (a) shall—

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

(2) provide institutions of higher education, including community colleges, with sufficient funding to carry out a scholarship program, as described in subsection (c); and

(3) provide assistance to institutions of higher education in establishing or expanding educational opportunities and resources in cybersecurity, as authorized under section 5 of the Cyber Security Research and Development Act (15 U.S.C. 7404).

(c) SCHOLARSHIP PROGRAM.—

(1) INSTITUTIONS OF HIGHER EDUCATION.—An institution of higher education that carries out a scholarship program under subsection (b)(2) shall—

(A) provide 2- or 3-year scholarships to students who are enrolled in a program of study at the institution of higher education leading to a degree, credential, 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;

(B) require each scholarship recipient, as a condition of receiving a scholarship under the program—

(i) 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, credential, or specialized program certification; and

(ii) to refund any scholarship payments received by the recipient, in accordance with rules established by the Director of the National Science Foundation, in coordination with the Secretary, if a recipient does not meet the terms of the scholarship program; and

(C) provide clearly documented evidence of a strong existing program in cybersecurity, which may include designation as a Center of Academic Excellence in Information Assurance Education by the National Security Agency and the Department of Homeland Security.

(2) SCHOLARSHIP ELIGIBILITY.—To be eligible to receive a scholarship under a scholarship program carried out by an institution of higher education under subsection (b)(2), an individual shall—

(A) be a full-time student of the institution of higher education who is likely to receive a baccalaureate degree, a masters degree, or a research-based doctoral degree during the 3-year period beginning on the date on which the individual receives the scholarship;

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

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

(D) have demonstrated a high level of proficiency in fields relevant to the cybersecurity profession, which may include mathematics, engineering, business, public policy, social sciences, law, or computer sciences.

(3) OTHER PROGRAM REQUIREMENTS.—The Director of the National Science Foundation, in coordination with the Secretary and the Director of the Office of Personnel Management, shall ensure that each scholarship program carried out under subsection (b)(2)—

(A) provides 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 scholarships recipients, including providing for clearances during summer internships and after the recipient receives the degree, credential, or specialized program certification; and

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

(4) HIRING AUTHORITY.—

(A) 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 a scholarship program carried out by an institution of higher education under subsection (b)(2), the individual shall be—

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

(ii) exempt from competitive service.

(B) COMPETITIVE SERVICE POSITION.—Upon satisfactory fulfillment of the service term of an individual hired under subparagraph (A), the individual may be converted to a competitive service position with competition if the individual meets the requirements for that position.

(5) EVALUATION AND REPORT.—The Director of the National Science Foundation shall evaluate and report periodically to Congress on—

(A) the success of any scholarship programs carried out under subsection (b)(2) in recruiting individuals for scholarships; and

(B) hiring and retaining individuals who receive scholarships under a scholarship program carried out under subsection (b)(2) in the public sector workforce.

(d) BENCHMARKS.—

(1) PROPOSALS.—A proposal submitted to the Director of the National Science Foundation for assistance under subsection (b)(3) shall include—

(A) clearly stated goals translated into a set of expected measurable outcomes that can be monitored; and

(B) an evaluation plan that explains how the outcomes described in subparagraph (A) will be measured.

(2) USE OF GOALS.—The Director of the National Science Foundation shall use the goals included in a proposal submitted under paragraph (1)—

(A) to track the progress of a recipient of assistance under subsection (b)(3);

(B) to guide a project carried out using assistance under subsection (b)(3); and

(C) to evaluate the impact of a project carried out using assistance under subsection (b)(3).

SA 2725. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. TO CLASSIFY THE INDIVIDUAL MANDATE AS A NON-TAX.

(a) FINDING.—Congress finds that on June 28, 2012, the Supreme Court ruled that the individual mandate imposed by section 1501 of the Patient Protection and Affordable Care Act (Public Law 111–148) and amended by section 10106 of such Act and sections 1002 and 1004 of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), has certain functional characteristics of a tax and could be sustained as an exercise of Congress's power to tax under article I, section 8, clause 1 of the Constitution.

(b) CLASSIFICATION OF INDIVIDUAL MANDATE AS NON-TAX.—

(1) IN GENERAL.—Section 1501 of the Patient Protection and Affordable Care Act (Public Law 111–148) is amended by adding at the end the following new subsection:

''(e) RULE OF CONSTRUCTION.—Nothing in the amendments made by this section shall be construed as imposing any tax or as an exercise of any power of Congress enumerated in article I, section 8, clause 1 of, or the 16th amendment to, the Constitution.''.

(2) EFFECTIVE DATE.—The amendment made by this section shall apply as if included in the enactment of section 1501 of the Patient Protection and Affordable Care Act.

SA 2726. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 119, between lines 14 and 15, insert the following:

(b) GEOGRAPHIC DISPERSION.—In establishing academic and professional Centers of Excellence in cybersecurity under this section, the Secretary and the Secretary of Defense shall consider the need to avoid undue geographic concentration among any one category of States based on their predominant rural or urban character as indicated by population density.

SA 2727. Mr. BLUMENTHAL (for himself, Mr. SCHUMER, Ms. KLOBUCHAR, Mr. WYDEN, Mr. AKAKA, Mr. SANDERS, and Mrs. SHAHEEN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PROHIBITED ACTIVITY.

(a) IN GENERAL.—Section 1030(a) of title 18, United States Code, is amended—

(1) in paragraph (7)(C), by inserting ''or'' after the semicolon; and

(2) by inserting after paragraph (7)(C) the following:

''(8) acting as an employer, knowingly and intentionally—

''(A) for the purposes of employing, promoting, or terminating employment, compels or coerces any person to authorize access, such as by providing a password or similar information through which a computer may be accessed, to a protected computer that is not the employer's protected computer, and thereby obtains information from such protected computer; or

''(B) discharges, disciplines, discriminates against in any manner, or threatens to take any such action against, any person—

''(i) for failing to authorize access described in subparagraph (A) to a protected computer that is not the employer's protected computer; or

''(ii) who has filed any complaint or instituted or caused to be instituted any proceeding under or related to this paragraph, or has testified or is about to testify in any such proceeding;''.

(b) FINE.—Section 1030(c) of title 18, United States Code, is amended—

(1) in paragraph (4)(G)(ii), by striking the period at the end and inserting ''; and''; and

(2) by adding at the end the following:

''(5) a fine under this title, in the case of an offense under subsection (a)(8) or an attempt to commit an offense punishable under this paragraph.''.

(c) DEFINITIONS.—Section 1030(e) of title 18, United States Code, is amended—

(1) in paragraph (11), by striking ''and'' after the semicolon;

(2) in paragraph (12), by striking the period and inserting a semicolon; and

(3) by adding at the end the following:

''(13) the term 'employee' means an employee, as such term is defined in section 201(2) of the Genetic Information Nondiscrimination Act of 2008 (42 U.S.C. 2000ff(2));

''(14) the term 'employer' means an employer, as such term is defined in such section 201(2); and

''(15) the term 'employer's protected computer' means a protected computer of the employer, including any protected computer owned, operated, or otherwise controlled by, for, or on behalf of that employer.''.

(d) EXCEPTIONS.—Section 1030(f) of title 18, United States Code, is amended—

(1) by striking ''(f) This'' and inserting ''(f)(1) This''; and

(2) by adding at the end the following:

''(2)(A) Nothing in subsection (a)(8) shall be construed to limit the authority of a court of competent jurisdiction to grant equitable relief in a civil action, if the court determines that there are specific and articulable facts showing that there are reasonable grounds to believe that the information sought to be obtained is relevant and material to protecting the intellectual property, a trade secret, or confidential business information of the party seeking the relief.

''(B) Notwithstanding subsection (a)(8), the prohibition in such subsection shall not apply to an employer's actions if—

''(i) the employer discharges or otherwise disciplines an individual for good cause and an activity protected under subsection (a)(8) is not a motivating factor for the discharge or discipline of the individual;

''(ii) a State enacts a law that specifically waives subsection (a)(8) with respect to a particular class of State government employees or employees who work with individuals under 13 years of age, and the employer's action relates to an employee in such class; or

''(iii) an Executive agency (as defined in section 105 of title 5), a military department (as defined in section 102 of such title), or any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and National Reconnaissance Office, specifically waives subsection (a)(8) with respect to a particular class of employees requiring eligibility for access to classified information under Executive Order 12968 (60 Fed. Reg. 40245), or any successor thereto, and the employer's action relates to an employee in such class.''.

SA 2728. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 192, strike line 19, and all that follows through page 193, line 22, and insert the following:

(i) the actual damages sustained by the person as a result of the violation or $50,000, 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.

(h) CRIMINAL PENALTIES.—A person who knowingly violates a provision of this title shall be—

(1) for each such violation, fined not more than $50,000, imprisoned for not more than 1 year, or both;

(2) for each such violation committed under false pretenses, fined not more than $100,000, imprisoned for not more than 5 years, or both; and

(3) for each such violation committed for commercial advantage, personal gain, or malicious harm, fined not more than $250,000, imprisoned for not more than 10 years, or both.

SA 2729. Mr. WARNER (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 138, line 2, after ''subsection (a)'' insert '', including guidelines that provide for interoperable, non-proprietary technologies wherever possible''.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 134, line 4, insert ''and in consultation with Centers of Academic Excellence in Information Assurance Education designated by the National Security Agency and the Department,'' after ''United States Code,''.

SA 2731. Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

On page 20, strike line 3 and all that follows through page 42, line 10, and insert the following:

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 organizations, 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 consequences 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) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to increase, decrease, or otherwise alter the existing authority of any Federal agency to regulate the security of critical cyber infrastructure.

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

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

(B) require an owner (including a certified owner) or operator to implement cybersecurity measures that prevent the owner or operator from complying with any law or regulation.

(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 established 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) 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;

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

(3) 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; and

(C) 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.

SA 2732. Mr. REID (for Mr. FRANKEN) proposed an amendment to amendment SA 2731 proposed by Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

At the end, add the following new section:

SEC. ____.

Notwithstanding any other provision of this Act, section 701 and section 706(a)(1) shall have no effect.

SA 2733. Mr. REID proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

On page 20, line 5, strike ''180 days'' and insert ''170 days''.

SA 2734. Mr. REID proposed an amendment to amendment SA 2733 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment strike ''170'' and insert ''160''.

SA 2735. Mr. REID proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

At the end, add the following new section:

SEC. ____.

This Act shall become effective 3 days after enactment.

SA 2736. Mr. REID proposed an amendment to amendment SA 2735 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment, strike ''3 days'' and insert ''2 days''.

SA 2737. Mr. REID proposed an amendment to amendment SA 2736 proposed by Mr. REID to the amendment SA 2735 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment, strike ''2 days'' and insert ''1 day''.

SA 2738. Ms. SNOWE (for herself and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 23, strike line 19 and all that follows through page 24, line 18, and insert the following:

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to increase, decrease, or otherwise alter the existing authority of any Federal agency to regulate the security of critical cyber infrastructure.

SA 2739. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

In section 402, strike subsection (a) and insert the following:

(a) ASSESSMENT OF CYBERSECURITY EDUCATION IN COLLEGES, UNIVERSITIES, UNIVERSITY SYSTEMS, NONPROFIT ORGANIZATIONS, AND THE PRIVATE SECTOR.—

(1) REPORT BY THE NATIONAL SCIENCE FOUNDATION.—

(A) REPORT REQUIRED.—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.

(B) CONTENTS OF REPORT.—The report required under subparagraph (A) shall include baseline data on—

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

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

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

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

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

(2) REPORT BY SECRETARY.—

(A) REPORT REQUIRED.—Not later than 1 year after the date of enactment of this Act, the Secretary 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 support provided by the Department to education and training programs, including—

(i) the use of resources by the Department;

(ii) how the Secretary plans to use the resources of the Department in the future; and

(iii) the overall strategy of the Department to expand the cybersecurity human capital capacity of the United States.

(B) CONTENTS OF REPORTS.—The report required under subparagraph (A) shall include information on past, planned, or potential support by the Department for education and training programs that—

(i) emphasize experiential learning and the opportunity to take on significant real-world casework as integral parts of training and development programs for cybersecurity professions;

(ii) demonstrate a current and projected caseload of sufficient, important system and network defense activity to provide real-world training opportunities for trainees, with a heavy emphasis on real-life, hands-on, high-level cybersecurity work;

(iii) demonstrate practical computer network defense skills and up-to-date cybersecurity experience of the senior staff proposing to lead the education and training programs;

(iv) demonstrate access to hands-on training programs in the most up-to-date computer network defense technologies and techniques; and

(v) collaborate or plan to collaborate with the Federal Government, including laboratories of the Department of Defense and the Department of Energy, State or local governments, or private sector companies in the United States.

SA 2740. Mr. LIEBERMAN (for Mr. NELSON of Florida) proposed an amendment to the resolution S. Res. 525, honoring the life and legacy of Oswaldo Paya Sardinas; as follows:

On page 4, line 13, strike ''; and'' and insert a semicolon.

On page 4, line 17, strike the period and insert ''; and''.

On page 4, after line 17, insert the following:

(7) condemns the Government of Cuba for the detention of nearly 50 pro-democracy activists following the memorial service for Oswaldo Payá Sardiñas.

SA 2741. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 27, strike line 13 and all that follows through page 30, line 19, and insert the following:

(ii) submit to the Council an application for an assessment described in subsection (b)(1)(B) by a qualified third-party private entity 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.—

(A) SELF-CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i), the Council shall certify an owner.

(B) ASSESSMENT APPLICATION.—

(i) IN GENERAL.—Upon receipt of an application by an owner for an assessment under paragraph (3)(B)(ii), the Council shall direct a qualified third-party private entity to conduct an assessment of the owner in accordance with an agreement described in subsection (b)(1).

(ii) IN COMPLIANCE.—If a qualified third-party private entity determines an owner is in compliance with all applicable cybersecurity practices, the Council shall certify the 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 shall—

(A) develop qualifications for third-party private entities that ensure that the entity has—

(i) substantial expertise in cybersecurity;

(ii) the expertise necessary to perform third-party audits of the cybersecurity of critical cyber infrastructure systems and assets;

(iii) adopted appropriate policies and procedures to ensure that the entity provides independent analysis that is not affected by any conflict of interest or colored by any business interest that the entity may hold; and

(iv) any other qualifications determined relevant by the Council; and

(B) 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 submitting an application 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) DEFINITION.—

(i) IN GENERAL.—In this paragraph, the term ''cyber attack'' means an incident determined by the Attorney General to be an unauthorized intrusion or attack on or through a computer system or asset that causes damage or disruption to the operation or integrity of critical infrastructure that results in—

(I) loss of life, serious physical injury, or the substantial interruption of life-sustaining services;

(II) catastrophic economic damage to the United States, including—

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

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

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

(III) severe degradation of national security or national security capabilities, including intelligence and defense functions.

(ii) NO JUDICIAL REVIEW.—A determination by the Attorney General under clause (i) shall not be subject to judicial review.

(B) LIMITATION.—In any civil action for damages directly caused by a cyber attack, a certified owner shall not be liable for any punitive damages intended to punish or deter if the certified owner is in compliance with the appropriate cybersecurity practices at the time of the incident related to that cyber risk.

SA 2742. Mr. TESTER submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 186, beginning on line 14, strike ''for the timely destruction of cybersecurity threat indicators that'' and insert ''to destroy cybersecurity threat indicators not later than 1 year after such indicators''.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on July 31, 2012, at 2:30 p.m. in room SR–253 of the Russell Senate Office Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Energy and Natural Resources be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m. in room SD–366 of the Dirksen Senate Office Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON FOREIGN RELATIONS

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

SELECT COMMITTEE ON INTELLIGENCE

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on July 31, 2012, at 2:30 p.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs' Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m. to conduct a hearing entitled, ''State of Federal Privacy and Data Security Law: Lagging Behind the Times?''

The PRESIDING OFFICER. Without objection, it is so ordered.

SUBCOMMITTEE ON WESTERN HEMISPHERE, PEACE CORPS, AND GLOBAL NARCOTICS AFFAIRS

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on July 30, 2012, at 2 p.m., to hold a Western Hemisphere, Peace Corps, and Global Narcotics Affairs subcommittee hearing entitled, ''Doing Business in Latin America: Positive Trends but Serious Challenges.''

The PRESIDING OFFICER. Without objection, it is so ordered.

PRIVILEGES OF THE FLOOR

Mr. HARKIN. Mr. President, I ask unanimous consent that Oliver O'Connor and Kevin Burgess of my staff be granted floor privileges for the duration of today's session.

The PRESIDING OFFICER. Without objection, it is so ordered.

FOREIGN TRAVEL FINANCIAL REPORTS

In accordance with the appropriate provisions of law, the Secretary of the Senate herewith submits the following reports for standing committees of the Senate, certain joint committees of the Congress, delegations and groups, and select and special committees of the Senate, relating to expenses incurred in the performance of authorized foreign travel:

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON APPROPRIATIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Paul Grove:									
Bahrain	Dinar		364.24						364.24
Pakistan	Rupee		40.00						40.00
Afghanistan	Afghani		112.00						112.00
Iraq	Dinar		276.00						276.00
United States	Dollar				12,435.60				12,435.60
Adrienne Hallett:									
Côte d'Ivoire	Franc		436.00						436.00
Namibia	Rand		457.00						457.00
South Africa	Rand		994.09						994.09
Morocco	Dirahm		300.48						300.48
Zambia	Dollar		278.43						278.43
Erik Fatemi:									
Côte d'Ivoire	Franc		436.00						436.00
Namibia	Rand		457.00						457.00
South Africa	Rand		994.09						994.09
Morocco	Dirahm		300.48						300.48
Zambia	Dollar		278.43						278.43
Senator Thad Cochran:									
Turkey	Lira		589.03						589.03
Thailand	Baht		974.28						974.28
China	Yuan		736.18						736.18
Korea	Won		683.02						683.02
Stewart Holmes:									
Turkey	Lira		589.03						589.03
Thailand	Baht		608.85						608.85
China	Yuan		736.18						736.18
Korea	Won		683.02						683.02
Kay Webber:									
Turkey	Lira		589.03						589.03