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

SA 2653. Mr. GRAHAM submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2654. Mr. CRAPO (for himself and Mr. JOHANNS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2655. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2656. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2657. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2658. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2659. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2660. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2661. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2662. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2663. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2664. Mr. MCCAIN 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 2621. 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. ___. BORDER FENCE COMPLETION.

(a) MINIMUM REQUIREMENTS.—Section 102(b)(1) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) is amended—

(1) in subparagraph (A), by adding at the end the following: ''Fencing that does not effectively restrain pedestrian traffic (such as vehicle barriers and virtual fencing) may not be used to meet the 700-mile fence requirement under this subparagraph.'';

(2) in subparagraph (B)—

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

(B) in clause (ii), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(iii) not later than 1 year after the date of the enactment of the Cybersecurity Act of 2012, complete the construction of all the reinforced fencing and the installation of the related equipment described in subparagraph (A).''; and

(3) in subparagraph (C), by adding at the end the following:

''(iii) FUNDING NOT CONTINGENT ON CONSULTATION.—Amounts appropriated to carry out this paragraph may not be impounded or otherwise withheld for failure to fully comply with the consultation requirement under clause (i).''.

(b) REPORT.—Not later than 6 months after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report that describes—

(1) the progress made in completing the reinforced fencing required under section 102(b)(1) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note), as amended by subsection (a); and

(2) the plans for completing such fencing not later than 1 year after the date of the enactment of this Act.

SA 2622. Mr. CHAMBLISS 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 I.

SA 2623. Mr. CHAMBLISS 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 all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(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, employeee, 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 subsection 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 2624. Mr. CHAMBLISS 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.

SA 2625. Mr. CHAMBLISS 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—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 701. 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, employeee, 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. 702. 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. 703. 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 702, 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. 704. 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 702(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 702(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 702 for any use other than a use permitted under subsection 702(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. 705. 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 703 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 702 of this Act, including whether such information meets the definition of cyber threat information under section 701, 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 702 of this Act, including the appropriateness of any subsequent use under section 702(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 703 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. 706. 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. 707. 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 702 of title I of the Cybersecurity Act of 2012.''.

SEC. 708. 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.

SA 2626. Mr. CHAMBLISS 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 30, strike line 10, and all that follows through page 31, line 21, and insert the following:

(1) LIABILITY.—

(A) IN GENERAL.—No cause of action shall lie or be maintained in any court against a certified owner for any cyber-related incident that has impacted, or may impact, the information security of an information system of such owner, if such owner has been found to be in compliance with applicable cybersecurity practices through an assessment under subsection (b).

(B) ONGOING ASSESSMENT.—No cause of action shall lie or be maintained in any court against an owner or operator for any cyber-related incident that has impacted, or may impact, the information security of an information system of such owner or operator, if such owner or operator is, in good faith, in the process of obtaining, disputing, or satisfying the findings of an assessment under subsection (b).

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

(D) REMOVAL.—Any civil action arising from a cyber-related incident that has impacted, or may impact, the information security of an information system of an owner or operator engaged in the voluntary activities authorized under this title that is brought in a State court against any owner or operator shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

SA 2627. Mr. CHAMBLISS 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 23, strike line 18, and all that follows through page 25, line 8.

SA 2628. Mr. CHAMBLISS 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—EFFECTIVE DATE

SEC. 801. EFFECTIVE DATE.

(a) IN GENERAL.—This Act and the amendments made by this Act shall be effective during the 3-year period beginning on the date of the enactment of this Act.

(b) TRANSITION PROCEDURES.—Notwithstanding subsection (a), the limitations of liability in section 104(c)(1) and section 706 shall continue to apply to any actions described in such sections.

SA 2629. Mr. CHAMBLISS 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 9, strike line 7, and all that follows through page 25, line 24, and insert the following:

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

(1) the Department of Commerce;

(2) the Department of Defense;

(3) the Department of Justice;

(4) the intelligence community;

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

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

(7) the Department.

SEC. 102. VOLUNTARY CYBERSECURITY PRACTICES.

Not later than 180 days after the date of enactment of this Act, each sector coordinating council shall establish and maintain voluntary cybersecurity practices sufficient to effectively remediate or mitigate cyber risks identified by such sector coordinating council.

SA 2630. Ms. SNOWE 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, add the following:

TITLE VIII—MISCELLANEOUS

SEC. 801. LIMITATIONS ON BILLS IMPLEMENTING TRADE AGREEMENTS.

(a) IN GENERAL.—Notwithstanding section 151 of the Trade Act of 1974 (19 U.S.C. 2191) or any other provision of law, any bill implementing a trade agreement between the United States and a country described in subsection (b) shall be subject to a point of order pursuant to subsection (c).

(b) COUNTRY DESCRIBED.—A country described in this subsection is a country the government of which is identified as perpetrating foreign economic collection or industrial espionage that threatens the economic security of the United States in a report to Congress of the Office of the National Counterintelligence Executive.

(c) POINT OF ORDER IN SENATE.—

(1) IN GENERAL.—The Senate shall cease consideration of a bill to implement a trade agreement if—

(A) a point of order is made by any Senator against the bill because the bill implements a trade agreement between the United States and a country described in subsection (b); and

(B) the point of order is sustained by the presiding officer.

(2) WAIVERS AND APPEALS.—

(A) WAIVERS.—Before the presiding officer rules on a point of order described in paragraph (1), any Senator may move to waive the point of order and the motion to waive shall not be subject to amendment. A point of order described in paragraph (1) is waived only by the affirmative vote of a majority of the Members of the Senate, duly chosen and sworn.

(B) APPEALS.—After the presiding officer rules on a point of order under this paragraph, any Senator may appeal the ruling of the presiding officer on the point of order as it applies to some or all of the provisions on which the presiding officer ruled. A ruling of the presiding officer on a point of order described in paragraph (1) is sustained unless a majority of the Members of the Senate, duly chosen and sworn, vote not to sustain the ruling.

(C) DEBATE.—Debate on a motion to waive under subparagraph (A) or on an appeal of the ruling of the presiding officer under subparagraph (B) shall be limited to 1 hour. The time shall be equally divided between, and controlled by, the majority leader and the minority leader of the Senate, or their designees.

SA 2631. Ms. SNOWE 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, add the following:

SEC. 416. STUDY AND REPORT ON CYBERWORK BY SMALL BUSINESS CONCERNS.

(a) DEFINITIONS.—In this section—

(1) the term ''covered Federal agency'' means—

(A) the Department of Homeland Security;

(B) the Department of Defense; and

(C) each element of the intelligence community;

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

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

(b) STUDY.—The heads of the covered Federal agencies, in consultation with the Administrator of the Small Business Administration, shall jointly conduct a study of cyberwork performed by small business concerns for the covered Federal agencies.

(c) REPORT.—Not later than 180 days after the date of enactment of this Act, the heads of the covered Federal agencies shall jointly submit to the Committee on Small Business and Entrepreneurship, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate and the Committee on Small Business, the Committee on Armed Services, the Committee on Homeland Security, and the Committee on Intelligence of the House of Representatives a report on the results of the study under subsection (b) that contains—

(1) the number of small business concerns with top secret or sensitive compartmented information site clearances and an evaluation of whether small business concerns are carrying out a proportional amount of cyberwork for covered Federal agencies;

(2) a description of challenges faced by small business concerns in—

(A) securing cyberwork with covered Federal agencies;

(B) securing classified information technology work with covered Federal agencies;

(C) securing sponsorship by covered Federal agencies for site security clearances;

(D) obtaining security clearances for employees; and

(E) matters relating to the matters described in subparagraphs (A), (B), (C), and (D);

(3) recommendations for overcoming the challenges described in paragraph (2);

(4) an evaluation of the feasibility of and benefits to the Federal Government, the private sector, and small business concerns of establishing a program that would use small business concerns as incubators for developing cyberworkers who have top secret or sensitive compartmented information security clearances while the small business concerns perform other cyberwork for covered Federal agencies; and

(5) recommendations, if any, for legislation that would enable covered Federal agencies to better use the talents of small business concerns for cleared cyberwork.

SA 2632. Ms. SNOWE 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 108, line 6, insert '', including through the use of quantum entanglement for secured satellite and other point-to-point wireless communications'' before the semicolon.

SA 2633. Ms. SNOWE 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 150, strike line 24 and all that follows through page 151, line 8, and insert the following:

Congress reports—

(1) on available technical options, consistent with constitutional and statutory privacy rights, for enhancing the security of the information networks of entities that own or manage critical infrastructure through—

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

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

(2) providing an evaluation of the effort to implement the Domain Name System Security Extensions by owners and operators of critical infrastructure and Internet service providers, which shall—

(A) identify challenges hampering implementation; and

(B) provide proposals—

(i) to resolve any challenges identified under subparagraph (A); and

(ii) regarding how owners and operators of critical infrastructure and Internet service providers can streamline implementation of Domain Name System Security Extensions.

SA 2634. Ms. SNOWE 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, add the following:

TITLE VIII—FCC TECHNICAL EXPERTISE CAPACITY

SECTION 801. SHORT TITLE.

This title may be cited as the ''FCC Technical Expertise Capacity Heightening Act'' or the ''FCC TECH Act''.

SEC. 802. APPOINTMENT OF TECHNICAL STAFF.

Section 4(f)(2) of the Communications Act of 1934 (47 U.S.C. 154(f)(2)) is amended by inserting after the first sentence the following new sentence: ''Each commissioner may also appoint an electrical engineer or computer scientist to provide the commissioner technical consultation when appropriate and to interface with the Office of Engineering and Technology, Commission Bureaus, and other technical staff of the Commission for additional technical input and resources, provided that such engineer or scientist holds an undergraduate or graduate degree from an institution of higher education in their respective field of expertise.''.

SEC. 803. TECHNICAL POLICY AND PERSONNEL STUDY.

(a) STUDY.—

(1) REQUIREMENTS OF STUDY.—The Chairman of the Federal Communications Commission (referred to in this section as the ''Commission'') shall enter into an arrangement with the National Academy of Sciences to complete a study of the technical policy decision-making and the technical personnel at the Commission.

(2) CONTENTS.—The study required under paragraph (1) shall—

(A) review the technical policy decision making of the Commission, including if the Commission has the adequate resources and processes in place to properly evaluate and account for the technical aspects and impact of the Commission's regulatory rulemaking;

(B) review—

(i) the timeliness of the rulemaking process utilized by the Commission; and

(ii) the impact of regulatory delay on telecommunications innovation;

(C) based upon the review undertaken pursuant to subparagraph (B), make recommendations for the Commission to streamline its rulemaking process;

(D) evaluate the current staffing levels and skill sets of technical personnel at the Commission to determine if such staffing levels and skill sets are aligned with the current and future needs of the Commission, as well as with current and future issues that come or may come under the jurisdiction of the

Commission and shall include a recommendation on the appropriate number or percentage of technical personnel that should constitute the Commission workforce;

(E) examine the current technical staff and engineering recruiting procedures at the Commission and make recommendations on how the Commission can improve its efforts to hire and retain engineers and other technical staff members;

(F) examine—

(i) the reliance of the Commission on external contractors in the development of policy and in evaluating the technical aspects of services, devices, and issues that arise under the jurisdiction of the Commission; and

(ii) the potential costs and benefits of the development of ''in-house'' resources to perform the duties that are currently being outsourced to external contractors; and

(G) compare the decision-making process of the Commission with the decision-making process used by similar regulatory authorities in other industrialized countries, including the European Union, Japan, Canada, Australia, and the United Kingdom.

(b) REPORT.—The Commission shall transmit a report describing the results of the study and recommendations required by subsection (a) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

(c) OFFSET OF ADMINISTRATIVE COSTS.—Section 4(a) of Public Law 109–34 (47 U.S.C. 703(a)) is amended by striking ''annual'' and inserting ''biennial''.

SA 2635. Ms. SNOWE 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. ___. SMALL BUSINESS REGULATORY TRANSPARENCY.

Section 609(d) of title 5, United States Code, is amended—

(1) in paragraph (2), by striking ''and'' at the end;

(2) in paragraph (3), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(4) the Department of Homeland Security.''.

SA 2636. Ms. SNOWE 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 I, add the following:

SEC. 111. SMALL BUSINESS MEMBERSHIP ON THE CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL.

The Secretary shall ensure that the members of the Critical Infrastructure Partnership Advisory Council include—

(1) a representative of the Office of Advocacy of the Small Business Administration; and

(2) the owner of a small business concern or an advocate for small business concerns from the private sector.

SA 2637. Ms. SNOWE 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, add the following:

SEC. 416. REPORT BY SMALL BUSINESS INFORMATION SECURITY TASK FORCE.

Not later than 1 year after the date of enactment of this Act, the Small Business Information Security Task Force, in consultation with the Chief Counsel for Advocacy of the Small Business Administration, shall submit to Congress a report that—

(1) analyzes the impact of this Act, and the amendments made by this Act, on small business concerns; and

(2) describes methods for mitigating any costs or unnecessary burdens imposed on small business concerns by regulations issued under this Act or the amendments made by this Act.

SA 2638. 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:

At the appropriate place, insert the following:

SEC. ___. PROHIBITION ON TREASURY REGULATIONS WITH RESPECT TO INFORMATION REPORTING ON CERTAIN INTEREST PAID TO NONRESIDENT ALIENS.

Except to the extent provided in Treasury Regulations as in effect on February 21, 2011, the Secretary of the Treasury shall not require (by regulation or otherwise) that an information return be made by a payor of interest in the case of interest—

(1) which is described in section 871(i)(2)(A) of the Internal Revenue Code of 1986; and

(2) which is paid—

(A) to a nonresident alien; and

(B) on a deposit maintained at an office within the United States.

SA 2639. 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 RENEWABLE FUEL STANDARD.

Section 211 of the Clean Air Act (42 U.S.C. 7545) is amended by striking subsection (o).

SA 2640. Mr. LEAHY (for himself and Mr. HOEVEN) 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 109, strike line 4 and all that follows through page 110, line 20, and insert the following:

(d) CYBERSECURITY MODELING AND TEST BEDS.—

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

(2) ESTABLISHMENT OF PROGRAM.—

(A) IN GENERAL.—The Director of the National Science Foundation, the Secretary, and the Secretary of Commerce shall establish a program for the appropriate Federal agencies to award grants to institutions of higher education or research and development non-profit institutions and to provide funds to the military service academies and senior military colleges (as defined in section 2111a of title 10, United States Code) to establish cybersecurity test beds capable of realistic modeling of real-time cyber attacks and defenses. The test beds shall work to enhance the security of public systems and focus on enhancing the security of critical private sector systems such as those in the finance, energy, and other sectors.

(B) REQUIREMENTS.—

(i) SIZE OF TEST BEDS.—The test beds established under the program established under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real world networks and environments.

(ii) USE OF EXISTING TEST BEDS.—The test bed program established under subparagraph (A) shall build upon and expand test beds and cyber attack simulation, experiment, and distributed gaming tools developed by the Under Secretary of Homeland Security for Science and Technology prior to the date of enactment of this Act.

(3) PURPOSES.—The purposes of the program established under paragraph (2) shall be to—

(A) support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment; and

(B) to improve understanding among private sector partners of the risk, magnitude, and consequences of cyber attacks.

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

(1) the National Institute of Standards and Technology;

(2) the Department;

(3) other Federal agencies;

(4) other Federal and private research laboratories, research entities, the military service academies, senior military colleges (as defined in section 2111a of title 10, United States Code), and universities and institutions of higher education, and relevant nonprofit organizations; and

---

SA 2641. Mr. CARPER (for himself and Mr. BLUNT) 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—ACCOUNT DATA SECURITY

SEC. 801. SHORT TITLE.

This title may be cited as the ''Data Security Act of 2012''.

SEC. 802. DEFINITIONS.

For purposes of this title, the following definitions shall apply:

(1) AFFILIATE.—The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

(2) AGENCY.—The term ''agency'' has the same meaning as in section 551(1) of title 5, United States Code.

(3) BREACH OF DATA SECURITY.—

(A) IN GENERAL.—The term ''breach of data security'' means the unauthorized acquisition of sensitive account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM.—

(i) IN GENERAL.—The term ''breach of data security'' does not include the unauthorized acquisition of sensitive account information or sensitive personal information that is maintained or communicated in a manner that is not usable—

(I) to commit identity theft; or

(II) to make fraudulent transactions on financial accounts.

(ii) RULE OF CONSTRUCTION.—For purposes of this subparagraph, information that is maintained or communicated in a manner that is not usable includes any information that is maintained or communicated in an encrypted, redacted, altered, edited, or coded form.

(4) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(5) CONSUMER.—The term ''consumer'' means an individual.

(6) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(7) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any—

(i) entity, the business of which is engaging in financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k));

(ii) financial institution, including any institution described in section 313.3(k) of title 16, Code of Federal Regulations, as in effect on the date of enactment of this Act;

(iii) entity that maintains or otherwise possesses information that is subject to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w); or

(iv) other individual, partnership, corporation, trust, estate, cooperative, association, or entity that maintains or communicates sensitive account information or sensitive personal information.

(B) EXCEPTION.—The term ''covered entity'' does not include any agency or any other unit of Federal, State, or local government or any subdivision of such unit.

(8) FINANCIAL INSTITUTION.—The term ''financial institution'' has the same meaning as in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(9) SENSITIVE ACCOUNT INFORMATION.—The term ''sensitive account information'' means a financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account.

(10) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''sensitive personal information'' means the first and last name, address, or telephone number of a consumer, in combination with any of the following relating to such consumer:

(i) Social security account number.

(ii) Driver's license number or equivalent State identification number.

(iii) Taxpayer identification number.

(B) EXCEPTION.—The term ''sensitive personal information'' does not include publicly available information that is lawfully made available to the general public from—

(i) Federal, State, or local government records; or

(ii) widely distributed media.

(11) SUBSTANTIAL HARM OR INCONVENIENCE.—

(A) IN GENERAL.—The term ''substantial harm or inconvenience'' means—

(i) material financial loss to, or civil or criminal penalties imposed on, a consumer, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer; or

(ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by a consumer reporting agency, financial institution, or government entity, in order to avoid material financial loss, increased costs, or civil or criminal penalties, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer.

(B) EXCEPTION.—The term ''substantial harm or inconvenience'' does not include—

(i) changing a financial account number or closing a financial account; or

(ii) harm or inconvenience that does not result from identity theft or account fraud.

SEC. 803. PROTECTION OF INFORMATION AND SECURITY BREACH NOTIFICATION.

(a) SECURITY PROCEDURES REQUIRED.—

(1) IN GENERAL.—Each covered entity shall implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information which is maintained or is being communicated by or on behalf of a covered entity, from the unauthorized use of such information that is reasonably likely to result in substantial harm or inconvenience to the consumer to whom such information relates.

(2) LIMITATION.—Any policy or procedure implemented or maintained under paragraph (1) shall be appropriate to the—

(A) size and complexity of a covered entity;

(B) nature and scope of the activities of such entity; and

(C) sensitivity of the consumer information to be protected.

(b) INVESTIGATION REQUIRED.—

(1) IN GENERAL.—If a covered entity determines that a breach of data security has or may have occurred in relation to sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, such covered entity, the covered entity shall conduct an investigation—

(A) to assess the nature and scope of the breach;

(B) to identify any sensitive account information or sensitive personal information that may have been involved in the breach; and

(C) to determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

(2) NEURAL NETWORKS AND INFORMATION SECURITY PROGRAMS.—In determining the likelihood of misuse of sensitive account information under paragraph (1)(C), a covered entity shall consider whether any neural network or security program has detected, or is likely to detect or prevent, fraudulent transactions resulting from the breach of security.

(c) NOTICE REQUIRED.—If a covered entity determines under subsection (b)(1)(C) that sensitive account information or sensitive personal information involved in a breach of data security is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates, such covered entity, or a third party acting on behalf of such covered entity, shall—

(1) notify, in the following order—

(A) the appropriate agency or authority identified in section 805;

(B) an appropriate law enforcement agency;

(C) any entity that owns, or is obligated on, a financial account to which the sensitive account information relates, if the breach involves a breach of sensitive account information;

(D) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves sensitive personal information relating to 5,000 or more consumers; and

(E) all consumers to whom the sensitive account information or sensitive personal information relates; and

(2) take reasonable measures to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach.

(d) PRESUMED COMPLIANCE BY CERTAIN ENTITIES.—

(1) IN GENERAL.—An entity shall be deemed to be in compliance with—

(A) in the case of a financial institution—

(i) subsection (a), and any regulations prescribed under such subsection, if such institution maintains policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information that are consistent with the policies and procedures of such institution that are designed to comply with the requirements of section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and any regulations or guidance prescribed under that section that are applicable to such institution; and

(ii) subsections (b) and (c), and any regulations prescribed under such subsections, if such financial institution—

(I)(aa) maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of such institution that are designed to comply with the investigation and notice requirements established by regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to such institution; or

(bb) is an affiliate of a bank holding company that maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of a bank that is an affiliate of such institution, and that bank's policies and procedures are designed to comply with the investigation and notice requirements established by any regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to that bank; and

(II) provides for notice to the entities described under subparagraphs (B), (C), and (D) of subsection (c)(1), if notice is provided to consumers pursuant to the policies and procedures of such institution described in subclause (I); and

(B) subsections (a), (b), and (c), if the entity is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note), to the extent that such entity is in compliance with such regulations.

(2) DEFINITIONS.—For purposes of this subsection, the terms ''bank holding company'' and ''bank'' have the same meanings as in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841).

SEC. 804. IMPLEMENTING REGULATIONS.

(a) IN GENERAL.—Notwithstanding any other provision of law, and except as provided under section 806, the agencies and authorities identified in section 805, with respect to the covered entities that are subject to the respective enforcement authority of such agencies and authorities, shall prescribe regulations to implement this title.

(b) COORDINATION.—Each agency and authority required to prescribe regulations under subsection (a) shall consult and coordinate with each other agency and authority identified in section 805 so that, to the extent possible, the regulations prescribed by each agency and authority are consistent and comparable.

(c) METHOD OF PROVIDING NOTICE TO CONSUMERS.—The regulations required under subsection (a) shall—

(1) prescribe the methods by which a covered entity shall notify a consumer of a breach of data security under section 803; and

(2) allow a covered entity to provide such notice by—

(A) written, telephonic, or e-mail notification; or

(B) substitute notification, if providing written, telephonic, or e-mail notification is not feasible due to—

(i) lack of sufficient contact information for the consumers that must be notified; or

(ii) excessive cost to the covered entity.

(d) CONTENT OF CONSUMER NOTICE.—The regulations required under subsection (a) shall—

(1) prescribe the content that shall be included in a notice of a breach of data security that is required to be provided to consumers under section 803; and

(2) require such notice to include—

(A) a description of the type of sensitive account information or sensitive personal information involved in the breach of data security;

(B) a general description of the actions taken by the covered entity to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach of data security; and

(C) the summary of rights of victims of identity theft prepared by the Commission under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g), if the breach of data security involves sensitive personal information.

(e) TIMING OF NOTICE.—The regulations required under subsection (a) shall establish standards for when a covered entity shall provide any notice required under section 803.

(f) LAW ENFORCEMENT DELAY.—The regulations required under subsection (a) shall allow a covered entity to delay providing notice of a breach of data security to consumers under section 803 if a law enforcement agency requests such a delay in writing.

(g) SERVICE PROVIDERS.—The regulations required under subsection (a) shall—

(1) require any party that maintains or communicates sensitive account information or sensitive personal information on behalf of a covered entity to provide notice to that covered entity if such party determines that a breach of data security has, or may have, occurred with respect to such information; and

(2) ensure that there is only 1 notification responsibility with respect to a breach of data security.

(h) TIMING OF REGULATIONS.—The regulations required under subsection (a) shall—

(1) be issued in final form not later than 6 months after the date of enactment of this Act; and

(2) take effect not later than 6 months after the date on which they are issued in final form.

SEC. 805. ADMINISTRATIVE ENFORCEMENT.

(a) IN GENERAL.—Notwithstanding any other provision of law, section 803, and the regulations required under section 804, shall be enforced exclusively under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) a national bank, a Federal branch or Federal agency of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), or a savings association, the deposits of which are insured by the Federal Deposit Insurance Corporation, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Office of the Comptroller of the Currency;

(B) a member bank of the Federal Reserve System (other than a national bank), a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), a commercial lending company owned or controlled by a foreign bank, an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601, 604), or a bank holding company and its nonbank subsidiary or affiliate (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Governors of the Federal Reserve System; and

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (other than a member of the Federal Reserve System), an insured State branch of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the National Credit Union Administration Board with respect to any federally insured credit union;

(3) the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer;

(4) the Investment Company Act of 1940 (15 U.S.C. 80a–1 et seq.), by the Securities and Exchange Commission with respect to any investment company;

(5) the Investment Advisers Act of 1940 (15 U.S.C. 80b–1 et seq.), by the Securities and Exchange Commission with respect to any investment adviser registered with the Securities and Exchange Commission under that Act;

(6) the Commodity Exchange Act (7 U.S.C. 1 et seq.), by the Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(7) the provisions of title XIII of the Housing and Community Development Act of 1992 (12 U.S.C. 4501 et seq.), by the Director of Federal Housing Enterprise Oversight (and any successor to such functional regulatory agency) with respect to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and any other entity or enterprise (as defined in that title) subject to the jurisdiction of such functional regulatory agency under that title, including any affiliate of any such enterprise;

(8) State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled; and

(9) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8).

(b) EXTENSION OF FEDERAL TRADE COMMISSION ENFORCEMENT AUTHORITY.—The authority of the Commission to enforce compliance with section 803, and the regulations required under section 804, under subsection (a)(8) shall—

(1) notwithstanding the Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.), include the authority to enforce compliance by air carriers and foreign air carriers; and

(2) notwithstanding the Packers and Stockyards Act (7 U.S.C. 181 et seq.), include the authority to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

(c) NO PRIVATE RIGHT OF ACTION.—

(1) IN GENERAL.—This title, and the regulations prescribed under this title, may not be construed to provide a private right of action, including a class action with respect to any act or practice regulated under this title.

(2) CIVIL AND CRIMINAL ACTIONS.—No civil or criminal action relating to any act or practice governed under this title, or the regulations prescribed under this title, shall be commenced or maintained in any State court or under State law, including a pendent State claim to an action under Federal law.

SEC. 806. PROTECTION OF INFORMATION AT FEDERAL AGENCIES.

(a) DATA SECURITY STANDARDS.—Each agency shall implement appropriate standards relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of the sensitive account information and sensitive personal information that is maintained or is being communicated by, or on behalf of, that agency;

(2) to protect against any anticipated threats or hazards to the security of such information; and

(3) to protect against misuse of such information, which could result in substantial harm or inconvenience to a consumer.

(b) SECURITY BREACH NOTIFICATION STANDARDS.—Each agency shall implement appropriate standards providing for notification of consumers when such agency determines that sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, such agency—

(1) has been acquired without authorization; and

(2) is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

SEC. 807. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to—

(1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, such person;

(2) safeguard information relating to consumers from potential misuse;

(3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of such information for fraudulent, illegal, or other purposes; or

(4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers.

SEC. 808. DELAYED EFFECTIVE DATE FOR CERTAIN PROVISIONS.

(a) COVERED ENTITIES.—Sections 803 and 807 shall take effect on the later of—

(1) 1 year after the date of enactment of this Act; or

(2) the effective date of the final regulations required under section 804.

(b) AGENCIES.—Section 806 shall take effect 1 year after the date of enactment of this Act.

SA 2642. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3406, to authorize the extension of nondiscriminatory treatment (normal trade relations treatment) to products of the Russian Federation and Moldova, to require reports on the compliance of the Russian Federation with its obligations as a member of the World Trade Organization, and to impose sanctions on persons responsible for gross violations of human rights, and for other purposes; which was ordered to lie on the table; as follows:

On page 25, line 14, insert ''or any other foreign government'' before the semicolon.

SA 2643. 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 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.

SA 2644. Mr. TOOMEY (for himself, Ms. SNOWE, Mr. DEMINT, Mr. BLUNT, Mr. RUBIO, and Mr. HELLER) 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—DATA SECURITY AND BREACH NOTIFICATION

SEC. 801. REQUIREMENTS FOR INFORMATION SECURITY.

Each covered entity shall take reasonable measures to protect and secure data in electronic form containing personal information.

SEC. 802. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NOTIFICATION.—

(1) IN GENERAL.—A covered entity that owns or licenses data in electronic form containing personal information shall give notice of any breach of the security of the system following discovery by the covered entity of the breach of the security of the system to each individual who is a citizen or resident of the United States whose personal information was or that the covered entity reasonably believes to have been accessed and acquired by an unauthorized person and that the covered entity reasonably believes has caused or will cause, identity theft or other financial harm.

(2) LAW ENFORCEMENT.—A covered entity shall notify the Secret Service or the Federal Bureau of Investigation of the fact that a breach of security has occurred if the number of individuals whose personal information the covered entity reasonably believes to have been accessed and acquired by an unauthorized person exceeds 10,000.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY AGENTS.—

(A) IN GENERAL.—In the event of a breach of security of a system maintained by a third-party entity that has been contracted to maintain, store, or process data in electronic form containing personal information on behalf of a covered entity who owns or possesses such data, such third-party entity shall notify such covered entity of the breach of security.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM THIRD PARTIES.—Upon receiving notification from a third party under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(C) EXCEPTION FOR SERVICE PROVIDERS.—A service provider shall not be considered a third-party agent for purposes of this paragraph.

(2) SERVICE PROVIDERS.—

(A) IN GENERAL.—If a service provider becomes aware of a breach of security involving data in electronic form containing personal information that is owned or possessed by a 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, such service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM SERVICE PROVIDERS.—Upon receiving notification from a service provider under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) with respect to a security breach shall be made as expeditiously as practicable and without unreasonable delay, consistent with any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the data system that was breached.

(2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) LAW ENFORCEMENT.—If a Federal law enforcement agency determines that the notification required under subsection (a) would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if further delay is necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be delayed upon the written request of the national security agency or homeland security agency for any period which the national security agency or homeland security agency determines is reasonably necessary. A Federal national security agency or homeland security agency may revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods:

(i) Written notification, sent to the postal address of the individual in the records of the covered entity.

(ii) Telephone.

(iii) Email or other electronic means.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a security breach, such notification, to the extent practicable, 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 accessed and acquired, or reasonably believed to have been accessed and acquired, by an unauthorized person as a part of the security breach; and

(iii) information that the individual can use to contact the covered entity to inquire about—

(I) the breach of security; or

(II) the information the covered entity maintained about that individual.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) may provide substitute notification in lieu of the direct notification required by paragraph (1) if such direct notification is not feasible due to—

(i) excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity; or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include at least one of the following:

(i) A conspicuous notice on the Internet Web site of the covered entity (if such covered entity maintains such a Web site).

(ii) Notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(e) TREATMENT OF PERSONS GOVERNED BY OTHER FEDERAL LAW.—Except as provided in section 4(b), a covered entity who is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a breach of security shall be deemed to be in compliance with this section.

SEC. 803. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 801 and 802 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 section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—Sections 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 222, 338, and 551), and any regulations promulgated thereunder, shall not apply with respect to the information security practices,

including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections.

(c) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 801 or 802 shall be treated as an unfair or 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.—

(A) IN GENERAL.—Except as provided in subsection (a), 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.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates section 801 or 802 shall be subject to the penalties and entitled to the privileges and immunities provided in such Act.

(3) 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 for all actions shall not exceed—

(A) $500,000 for all violations of section 801 resulting from the same related act or omission; and

(B) $500,000 for all violations of section 802 resulting from a single breach of security.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title shall be construed to establish a private cause of action against a person for a violation of this title.

SEC. 804. DEFINITIONS.

In this title:

(1) BREACH OF SECURITY.—The term ''breach of security'' means unauthorized access and acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or utilizes personal information.

(B) EXEMPTIONS.—The term ''covered entity'' does not include the following:

(i) Financial institutions subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(ii) An entity covered by the regulations issued under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191) to the extent that such entity is subject to the requirements of such regulations with respect to protected health 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 and includes recordable tapes and other mass storage devices.

(5) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) EXCLUSIONS.—

(i) PUBLIC RECORD INFORMATION.—Personal information does not include information obtained about an individual which has been lawfully made publicly available by a Federal, State, or local government entity or widely distributed by media.

(ii) ENCRYPTED, REDACTED, OR SECURED DATA.—Personal information does not include information that is encrypted, redacted, or secured by any other method or technology that renders the data elements unusable.

(6) SERVICE PROVIDER.—The term ''service provider'' means an entity that provides electronic data transmission, routing, intermediate, and transient storage, or connections to its system or network, where such entity 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 entity transmits, routes, stores, or for which such entity provides connections. Any such entity 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. 805. EFFECT ON OTHER LAWS.

This title preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security.

SEC. 806. EFFECTIVE DATE.

This title shall take effect on the date that is 1 year after the date of enactment of this Act.

SA 2645. Mr. BINGAMAN 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 the bill, add the following:

TITLE VIII—GRID CYBER SECURITY

SEC. 801. SHORT TITLE.

This title may be cited as the ''Grid Cyber Security Act''.

SEC. 802. CRITICAL ELECTRIC INFRASTRUCTURE.

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. CRITICAL ELECTRIC INFRASTRUCTURE.

''(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) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information relating to critical electric infrastructure.

''(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given the term in section 212 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131).

''(4) 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.

''(5) CYBER SECURITY VULNERABILITY.—The term 'cyber security vulnerability' means a weakness or flaw in the design or operation of any programmable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat.

''(6) ELECTRIC RELIABILITY ORGANIZATION.—The term 'Electric Reliability Organization' has the meaning given the term in section 215(a).

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

''(b) AUTHORITY OF COMMISSION.—

''(1) INITIAL DETERMINATION.—Not later than 120 days after the date of enactment of this section, the Commission shall determine whether reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities.

''(2) INITIAL ORDER.—Unless the Commission determines that the reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities within 120 days after the date of enactment of this section, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of issuance of the order, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from cyber security vulnerabilities.

''(3) SUBSEQUENT DETERMINATIONS AND ORDERS.—If at any time following the issuance of the initial order under paragraph (2) the Commission determines that the reliability standards established pursuant to section 215 are inadequate to protect critical electric infrastructure from a cyber security vulnerability, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of the determination, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from the cyber security vulnerability.

''(4) RELIABILITY STANDARDS.—Any proposed reliability standard or modification to a reliability standard submitted pursuant to paragraph (2) or (3) shall be developed and approved in accordance with section 215(d).

''(5) ADDITIONAL TIME.—The Commission may, by order, grant the Electric Reliability Organization reasonable additional time to submit a proposed reliability standard or a modification to a reliability standard under paragraph (2) or (3).

''(c) 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 under this section 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 the entities described in subsection (e)(1) 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.

''(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any order issued by the Secretary under subsection (c) 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.

''(e) JURISDICTION.—

''(1) IN GENERAL.—Notwithstanding section 201, this section shall apply to any entity that owns, controls, or operates critical electric infrastructure.

''(2) COVERED ENTITIES.—

''(A) IN GENERAL.—An entity described in paragraph (1) shall be subject to the jurisdiction of the Commission for purposes of—

''(i) carrying out this section; and

''(ii) applying the enforcement authorities of this Act with respect to this section.

''(B) JURISDICTION.—This subsection shall not make an electric utility or any other entity subject to the jurisdiction of the Commission for any other purpose.

''(3) ALASKA AND HAWAII EXCLUDED.—Except as provided in subsection (f), nothing in this section shall apply in the State of Alaska or Hawaii.

''(f) DEFENSE FACILITIES.—Not later than 1 year after the date of enactment of this section, the Secretary of Defense shall prepare, in consultation with the Secretary, the States of Alaska and Hawaii, the Territory of Guam, and the electric utilities that serve national defense facilities in those States and Territory, a comprehensive plan that identifies the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those States and Territory in the event of an imminent cybersecurity threat.

''(g) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(1) IN GENERAL.—Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to the Commission or the Secretary under this section, or developed by a Federal power marketing administration or the Tennessee Valley Authority under this section or section 215, to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.).

''(2) RULES PROHIBITING DISCLOSURE.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring cyber security under this section if the Secretary or Commission, as appropriate, decides disclosing the information would be detrimental to the security of critical electric infrastructure.

''(3) PROCEDURES FOR SHARING INFORMATION.—

''(A) IN GENERAL.—The Secretary and the Commission shall establish procedures on the release of critical infrastructure information to entities subject to this section, to the extent necessary to enable the entities to implement rules or orders of the Commission or the Secretary.

''(B) REQUIREMENTS.—The procedures shall—

''(i) limit the redissemination of information described in subparagraph (A) to ensure that the information is not used for an unauthorized purpose;

''(ii) ensure the security and confidentiality of the information;

''(iii) protect the constitutional and statutory rights of any individuals who are subjects of the information; and

''(iv) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

''(h) ACCESS TO CLASSIFIED INFORMATION.—

''(1) 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 section without the appropriate security clearances.

''(2) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall cooperate with the Secretary or the Commission, to the maximum extent practicable consistent with applicable procedures and requirements, in expeditiously providing appropriate security clearances to individuals that have a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this section.

''(i) NUCLEAR SAFETY.—No order issued by the Secretary or the Commission under this section, no reliability standard issued or modified by the Electric Reliability Organization pursuant to this section, and no temporary emergency order issued by the Electric Reliability Organization under section 215(d)(7) shall require or authorize a licensee of the Nuclear Regulatory Commission to operate a facility licensed by the Nuclear Regulatory Commission in a manner inconsistent with the terms of the license of the facility.''.

SEC. 803. LIMITED ADDITION OF ERO AUTHORITY FOR CRITICAL ELECTRIC INFRASTRUCTURE.

Section 215(a)(1) of the Federal Power Act (16 U.S.C. 824o(a)(1)) is amended—

(1) in the first sentence—

(A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and indenting appropriately;

(B) by striking ''(1) The term'' and inserting the following:

''(1) BULK-POWER SYSTEM.—

''(A) IN GENERAL.—The term'';

(C) in clause (i) (as so redesignated), by striking ''and'' after the semicolon at the end;

(D) in clause (ii) (as so redesignated), by striking the period at the end and inserting ''; and'';

(E) by adding at the end the following:

''(iii) for purposes of section 224, facilities used for the local distribution of electric energy that the Commission determines to be critical electric infrastructure pursuant to section 224.''; and

(2) in the second sentence, by striking ''The term'' and inserting the following:

''(B) EXCLUSION.—Except as provided in subparagraph (A), the term''.

SEC. 804. LIMITATION.

Section 215(i) of the Federal Power Act (16 U.S.C. 824o(i)) is amended by adding at the end the following:

''(6) LIMITATION.—The ERO shall have authority to develop and enforce compliance with reliability standards and temporary emergency orders with respect to a facility used in the local distribution of electric energy only to the extent the Commission determines the facility is so vital to the United States that the incapacity or destruction of the facility would have a debilitating impact on national security, national economic security, or national public health or safety.''.

SEC. 805. TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.

Section 215(d) of the Federal Power Act (16 U.S.C. 824o(d)) is amended by adding at the end the following:

''(7) TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.—Notwithstanding paragraphs (1) through (6), if the Commission determines that immediate action is necessary to protect critical electric infrastructure for a cyber security vulnerability, the Commission may, without prior notice or hearing, after consulting the ERO, require the ERO—

''(A) to develop and issue a temporary emergency order to address the cyber security vulnerability;

''(B) to make the temporary emergency order immediately effective; and

''(C) to keep the temporary emergency order in effect until—

''(i) the ERO develops, and the Commission approves, a final reliability standard under this section; or

''(ii) the Commission authorizes the ERO to withdraw the temporary emergency order.''.

SEC. 806. EMP STUDY.

(a) DOE REPORT.—Not later than 3 years after the date of enactment of this Act, the Secretary of Energy, in consultation with appropriate experts at the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), shall prepare and publish a report that assesses the susceptibility of critical electric infrastructure to electromagnetic pulse events and geomagnetic disturbances.

(b) CONTENTS.—The report under subsection (a) shall—

(1) examine the risk of electromagnetic pulse events and geomagnetic disturbances, using both computer-based simulations and experimental testing;

(2) assess the full spectrum of possible events and disturbances and the likelihood that the events and disturbances would cause significant disruption to the transmission and distribution of electric power; and

(3) seek to quantify and reduce uncertainties associated with estimates for electromagnetic pulse events and geomagnetic disturbances.

(c) FERC ASSESSMENT.—Not later than 1 year after publication of the report under subsection (a), the Federal Energy Regulatory Commission, in coordination with the Secretary of Energy and in consultation with electric utilities and the ERO (as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)), shall submit to Congress an assessment of whether and to what extent infrastructure affecting the transmission of electric power in interstate commerce should be hardened against electromagnetic events and geomagnetic disturbances, including an estimate of the costs and benefits of options to harden the infrastructure.

SEC. 807. BUDGETARY EFFECTS.

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 2646. Mr. MENENDEZ (for himself and Mr. KERRY) 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 III, add the following:

SEC. 305. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research, development, education, and training activities for cybersecurity through a consortium, or other appropriate entity, with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force established under subsection (a) 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 the consortium;

(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;

(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(4) propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental 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, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force established under subsection (a).

(e) TERMINATION.—The task force established under subsection (a) shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force established under subsection (a) shall serve without compensation.

SEC. 306. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH AND DEVELOPMENT.

(a) NIST CYBERSECURITY CHECKLISTS, CONFIGURATION PROFILES, AND DEPLOYMENT RECOMMENDATIONS.—Subsection (c) of section 8 of the Cyber Security Research and Development Act (15 U.S.C. 7406) is amended to read as follows:

''(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

''(2) PRIORITIES FOR DEVELOPMENT, IDENTIFICATION, REVISION, AND ADAPTATION.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

''(A) the security risks associated with the use of each system;

''(B) the number of agencies that use a particular system or security tool;

''(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

''(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

''(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

''(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

''(4) DISSEMINATION OF CHECKLISTS, CONFIGURATION PROFILES, AND DEPLOYMENT RECOMMENDATIONS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

''(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

''(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

''(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

''(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

''(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed, or identified under paragraph (1).''.

(b) NIST CYBERSECURITY RESEARCH AND DEVELOPMENT.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

''(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

''(2) carry out research associated with improving the security of information systems and networks;

''(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

''(4) carry out research associated with improving security of industrial control systems.''.

(c) NIST IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.—The Director 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.

(d) FEDERAL GOVERNMENT CLOUD COMPUTING STRATEGY.—

(1) IN GENERAL.—The Director, in collaboration with the Federal Chief Information Officers Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(2) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(A) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(B) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(C) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(i) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(ii) to ensure secure access to the data stored in cloud computing data centers;

(iii) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3); and

(iv) to support the development of the automation of continuous monitoring systems.

SA 2647. Ms. SNOWE 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. ___. SPECTRUM EFFICIENCY AND SECURITY FUND.

(a) RETENTION OF UNUSED FUNDS.—Section 118(d)(4) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(4)) is amended by striking ''8 years'' and inserting ''20 years''.

(b) USE OF FUND FOR PLANNING AND RESEARCH.—

(1) IN GENERAL.—Section 118(c) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(c)) is amended to read as follows:

''(c) USES OF FUNDS.—The amounts in the Fund are authorized to be used—

''(1) to pay relocation costs;

''(2) to fund planning and research with the goal of improving the efficiency of Federal use of spectrum and security of Federal wireless networks and systems; and

''(3) to cover the costs of eligible Federal entities to upgrade their equipment and facilities as long as such upgrades include spectrum sharing, reuse, and layering, and result in more efficient use of spectrum and more secure networks and systems by such entities.''.

(2) CONFORMING AMENDMENT.—Section 118(d)(2) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(2)) is amended, in the matter preceding subparagraph (A), by inserting ''to pay relocation costs'' after ''subsection''.

(c) NATIONAL SCIENCE FOUNDATION.—Section 118(e) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(e)) is amended by adding at the end the following:

''(3) ELIGIBLE FEDERAL ENTITY; NATIONAL SCIENCE FOUNDATION.—In this section, the term 'eligible Federal entity' shall include the National Science Foundation. As an eligible Federal entity, the National Science Foundation may submit to the Director of OMB requests for funds under this section to support spectrum research and experimental facilities by the Foundation, provided that such requests have, in the determination of the Director of OMB, in consultation with the NTIA, clear benefits to existing and future Federal users of spectrum. The Director of OMB shall give priority to research that improves spectral efficiency or security of wireless network or systems.''.

(d) SPECTRUM EFFICIENCY AND SECURITY FUND.—

(1) IN GENERAL.—Section 118 of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928) is amended—

(A) in the section heading, by striking ''**SPECTRUM RELOCATION FUND**'' and inserting ''**SPECTRUM EFFICIENCY AND SECURITY FUND**''; and

(B) in subsection (a), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) COMMUNICATIONS ACT OF 1934.—Section 309(j)(8)(D) of the Communications Act of 1934 (47 U.S.C. 309(j)(8)(D)) is amended—

(i) in clause (i), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''; and

(ii) in clause (ii), in the first sentence, by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

(B) NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ORGANIZATION ACT.—Section 113 of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 923) is amended—

(i) in subsection (g)(3), in the first sentence, by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''; and

(ii) in subsection (h)(2)(G)(i), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

SA 2648. Mr. LEVIN 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—MISCELLANEOUS

SEC. 801. ACTIONS TO ADDRESS FOREIGN ECONOMIC OR INDUSTRIAL ESPIONAGE IN CYBERSPACE.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Director of National Intelligence shall submit to the appropriate congressional committees a report on foreign economic and industrial espionage in cyberspace during the 12-month period preceding the submission of the report that—

(A) identifies—

(i) foreign countries that engage in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons;

(ii) foreign countries identified under clause (i) that the Director determines engage in the most egregious economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons (in this section referred to as ''priority foreign countries'');

(iii) technologies developed by United States persons that—

(I) are targeted for economic or industrial espionage in cyberspace; and

(II) to the extent practicable, have been appropriated through such espionage; and

(iv) articles manufactured or otherwise produced using technologies described in clause (iii);

(B) describes the economic or industrial espionage engaged in by the foreign countries identified under subparagraph (A); and

(C) describes—

(i) actions taken by the Director and other Federal agencies to decrease the prevalence of economic or industrial espionage in cyberspace; and

(ii) the progress made in decreasing the prevalence of economic or industrial espionage in cyberspace.

(2) DETERMINATION OF FOREIGN COUNTRIES ENGAGING IN ECONOMIC OR INDUSTRIAL ESPIONAGE IN CYBERSPACE.—For purposes of paragraph (1)(A), the Director shall identify a foreign country as a foreign country that engages in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons if the government of the foreign country—

(A) engages in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons; or

(B) facilitates, supports, fails to prosecute, or otherwise tolerates such espionage by—

(i) individuals who are citizens or residents of the foreign country; or

(ii) entities that are organized under the laws of the foreign country or are otherwise subject to the jurisdiction of the government of the foreign country.

(3) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form but may contain a classified annex.

(b) REFERRAL TO UNITED STATES INTERNATIONAL TRADE COMMISSION.—The Director of National Intelligence shall refer the report required by subsection (a) to the United States International Trade Commission for appropriate action under section 337 of the Tariff Act of 1930 (19 U.S.C. 1337).

(c) DEFINITIONS.—In this section:

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

(A) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Finance, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on Ways and Means, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) CYBERSPACE.—The term ''cyberspace''—

(A) means the interdependent network of information technology infrastructures; and

(B) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

(3) ECONOMIC OR INDUSTRIAL ESPIONAGE.—The term ''economic or industrial espionage'' means—

(A) stealing a trade secret or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret without the authorization of the owner of the trade secret;

(B) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret without the authorization of the owner of the trade secret; or

(C) knowingly receiving, buying, or possessing a trade secret that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret.

(4) OWN.—The term ''own'', with respect to a trade secret, means to hold rightful legal or equitable title to, or license in, the trade secret.

(5) PERSON.—The term ''person'' means an individual or entity.

(6) TECHNOLOGY.—The term ''technology'' has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. App. 2415) (as in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)).

(7) TRADE SECRET.—The term ''trade secret'' has the meaning given that term in section 1839 of title 18, United States Code.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) an individual who is a citizen of the United States or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or any jurisdiction within the United States.

SA 2649. Mr. LEVIN 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 VII, add the following:

SEC. 709. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCESS FOR REPORTING PENETRATIONS.—The Under Secretary of Defense for

Intelligence shall, in coordination with the officials specified in subsection (c), establish a process by which cleared defense contractors shall report to elements of the Department of Defense designated by the Under Secretary for purposes of the process when a network or information system of such contractors designated pursuant to subsection (b) is successfully penetrated.

(b) DESIGNATION OF NETWORKS AND INFORMATION SYSTEMS.—The Under Secretary of Defense for Intelligence shall, in coordination with the officials specified in subsection (c), establish criteria for designating the cleared defense contractors' networks or information systems that contain or process information created by or for the Department of Defense to be subject to the reporting process established pursuant to subsection (a).

(c) OFFICIALS.—The officials specified in this subsection are the following:

(1) The Under Secretary of Defense for Policy.

(2) The Under Secretary of Defense for Acquisition, Technology, and Logistics.

(3) The Chief Information Officer of the Department of Defense.

(4) The Commander of the United States Cyber Command.

(d) PROCESS REQUIREMENTS.—

(1) RAPID REPORTING.—The process required by subsection (a) shall provide for rapid reporting by contractors of successful penetrations of designated network or information systems.

(2) REPORT ELEMENTS.—The report by a contractor on a successful penetration of a designated network or information system under the process shall include the following:

(A) A description of the technique or method used in the penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor.

(3) ACCESS.—The process shall include mechanisms by which Department of Defense personnel may, upon request, obtain access to equipment or information of a contractor necessary to conduct a forensic analysis to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of the contractor and, if so, what information was exfiltrated.

(e) CLEARED DEFENSE CONTRACTOR DEFINED.—In this section, the term ''cleared defense contractor'' means a private entity granted clearance by the Defense Security Service to receive and store classified information for the purpose of bidding for a contract or conducting activities under a contract with the Department of Defense.

SA 2650. Mr. UDALL of Colorado 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. CYBER TRAINING AND RESEARCH AT THE UNITED STATES AIR FORCE ACADEMY, COLORADO.

(a) FINDINGS.—Congress makes the following findings:

(1) The training of cyber security leaders is a critical function of the United States Air Force Academy.

(2) The Center for Cyberspace Research at the United States Air Force Academy has been instrumental in educating and developing highly skilled cyber innovators for the Department of Defense.

(3) The Center for Cyberspace Research benefits greatly from interagency funding, information-sharing, and other collaboration, and it is in the national interest that such funding, information-sharing and collaboration continue.

(4) The Cyber Training Range operated by the Computer Science Department at the United States Air Force Academy provides realistic cyber training for cadets that will benefit the entire Air Force.

(5) The establishment of a civilian director for the Cyberspace Research Center and the Cyber Training Range as permanent faculty positions at the United States Air Force Academy will help assure that the Center and Range are both maintained and staffed with highly-experienced cyber experts.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the partner organizations for the Center for Cyberspace Research and the Cyber Training Range, including the Air Force Office of Scientific Research (AFOSR), the Defense Advanced Projects Research Agency (DARPA), the Defense Information Assurance Program (DIAP) of the Department of Defense, the National Security Agency, and the National Reconnaissance Office, maintain their funding, information-sharing, and other collaborative commitments to the Center for Cyberspace Research and the Cyber Training Range.

(c) CIVILIAN DIRECTOR FOR CENTER FOR CYBERSPACE RESEARCH.—

(1) IN GENERAL.—The head of the Center for Cyberspace Research at the United States Air Force Academy, Colorado, shall be the Director of the Center for Cyberspace Research, who shall be a civilian employee of the Air Force.

(2) PERMANENT BILLET IN EXCEPTED SERVICE.—The position of Director of the Center for Cyberspace Research shall be a permanent civilian billet in the excepted service (as that term is defined in section 2103(a) of title 5, United States Code).

(3) PAY GRADE.—The level of pay of the person serving in the position of Director of the Center for Cyberspace Research shall be a level of pay not below that payable for paygrade GS–14 of the General Schedule.

(d) CIVILIAN DIRECTOR FOR CYBER TRAINING RANGE.—

(1) IN GENERAL.—The head of the Cyber Training Range in the Computer Science Department of the United States Air Force Academy, Colorado, shall be the Director of the Cyber Training Range, who shall be a civilian employee of Air Force.

(2) PERMANENT BILLET IN EXCEPTED SERVICE.—The position of Director of the Cyber Training Range shall be a permanent civilian billet in the excepted service (as so defined).

(3) PAY GRADE.—The level of pay of the person serving in the position of Director of the Cyber Training Range shall be a level of pay not below that payable for paygrade GS–12 of the General Schedule.

(e) AMOUNTS AVAILABLE FOR PAY.—Amounts for the pay and allowances of the directors covered by subsections (c) and (d) shall be derived from amounts available to the Air Force for the pay and allowances of civilian employees of the Air Force.

SA 2651. Mr. UDALL of Colorado 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 DOMESTIC PRODUCTION, SECURITY, AND AVAILABILITY OF EXTRA HIGH VOLTAGE TRANSFORMERS.

(a) FINDING.—Based on reports provided by the Department of Defense and the Department of Homeland Security, Congress finds that the lack of a secured stockpile of domestically-produced Extra High Voltage (EHV) transformers, and the current manufacturing backlog for Extra High Voltage transformers in the United States, are likely to contribute to extended blackouts and power shortages in the event of a physical or network-based attack on the electric power infrastructure of the United States.

(b) REPORT.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall, in collaboration with the Secretary of Defense, submit to the appropriate committees of Congress a report on the domestic production, security, and availability of Extra High Voltage transformers.

(2) ELEMENTS.—The report required by paragraph (1) shall include the following:

(A) An assessment whether the number of Extra High Voltage transformers currently held in reserve by utilities and public and private manufacturers in the United States is sufficient, and is secured in a manner adequate, to maintain national security operations in the event of loss or damage to multiple Extra High Voltage transformers in the United States, Canada, or Mexico.

(B) An identification and assessment of the risks associated with having no spare Extra High Voltage transformers stockpiled and securely stored for national security purposes.

(C) An estimate of the time that national security operations would be negatively impacted if two or more Extra High Voltage transformers in the United States were destroyed by cyber attack, physical attack, or a natural disaster.

(D) An estimate of the feasability and cost of establishing a stockpile of not fewer than 30, and as many 60, Extra High Voltage transformers at disbursed Department of Defense installations or other national security locations in the continental United States.

(E) Recommendation as to the best locations to store Extra High Voltage transformers stockpiled as described in subparagraph (D) in order to ensure security and the rapid distribution of such transformers in emergency circumstances.

(3) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, and shall include a classified annex containing a detailed description of the relationship between national security functions and locations of Extra High Voltage Transformers.

(4) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives.

SA 2652. Mr. UDALL of Colorado 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 132, strike lines 16 through 21 and insert the following:

(2) CONTENTS.—The strategy developed under paragraph (1) shall include—

(A) a 5-year plan on recruitment of personnel for the Federal workforce that includes—

(i) a description of Federal programs for identifying, recruiting, training, and retaining individuals with outstanding computer skills for service in the Federal Government; and

(ii) a description of any bonuses or any non-traditional or non-standard recruiting practices that are employed by the Federal Government to locate and recruit individuals for career fields related to cybersecurity; and

(B) a 10-year projection of Federal workforce needs that includes an identification of any staffing or specialty shortfalls in career fields related to cybersecurity.

SA 2653. Mr. GRAHAM 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—IRANIAN NUCLEAR PROGRAM

SEC. 801. IRANIAN NUCLEAR PROGRAM.

(a) FINDINGS.—Congress makes the following findings:

(1) Since at least the late 1980s, the Government of the Islamic Republic of Iran has engaged in a sustained and well-documented pattern of illicit and deceptive activities to acquire nuclear capability.

(2) The United Nations Security Council has adopted multiple resolutions since 2006 demanding the full and sustained suspension of all uranium enrichment-related and reprocessing activities by the Government of the Islamic Republic of Iran and its full cooperation with the International Atomic Energy Agency (IAEA) on all outstanding issues related to its nuclear activities, particularly those concerning the possible military dimensions of its nuclear program.

(3) On November 8, 2011, the IAEA issued an extensive report that—

(A) documents ''serious concerns regarding possible military dimensions to Iran's nuclear programme'';

(B) states that ''Iran has carried out activities relevant to the development of a nuclear device''; and

(C) states that the efforts described in paragraphs (1) and (2) may be ongoing.

(4) As of November 2008, Iran had produced, according to the IAEA—

(A) approximately 630 kilograms of uranium hexaflouride enriched up to 3.5 percent uranium-235; and

(B) no uranium hexaflouride enriched up to 20 percent uranium-235.

(5) As of November 2011, Iran had produced, according to the IAEA—

(A) nearly 5,000 kilograms of uranium hexaflouride enriched up to 3.5 percent uranium-235; and

(B) 79.7 kilograms of uranium hexaflouride enriched up to 20 percent uranium-235.

(6) On January 9, 2012, IAEA inspectors confirmed that the Government of the Islamic Republic of Iran had begun enrichment activities at the Fordow site, including possibly enrichment of uranium hexaflouride up to 20 percent uranium-235.

(7) Section 2(2) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (Public Law 111–195) states, ''The United States and other responsible countries have a vital interest in working together to prevent the Government of Iran from acquiring a nuclear weapons capability.''.

(8) If the Government of the Islamic Republic of Iran were successful in acquiring a nuclear weapon capability, it would likely spur other countries in the region to consider developing their own nuclear weapons capabilities.

(9) On December 6, 2011, Prince Turki al-Faisal of Saudi Arabia stated that if international efforts to prevent Iran from obtaining nuclear weapons fail, ''we must, as a duty to our country and people, look into all options we are given, including obtaining these weapons ourselves''.

(10) Top leaders of the Government of the Islamic Republic of Iran have repeatedly threatened the existence of the State of Israel, pledging to ''wipe Israel off the map''.

(11) The Department of State has designated Iran as a state sponsor of terrorism since 1984 and characterized Iran as the ''most active state sponsor of terrorism''.

(12) The Government of the Islamic Republic of Iran has provided weapons, training, funding, and direction to terrorist groups, including Hamas, Hezbollah, and Shiite militias in Iraq that are responsible for the murders of hundreds of United States forces and innocent civilians.

(13) On July 28, 2011, the Department of the Treasury charged that the Government of Iran had forged a ''secret deal'' with al Qaeda to facilitate the movement of al Qaeda fighters and funding through Iranian territory.

(14) In October 2011, senior leaders of Iran's Islamic Revolutionary Guard Corps (IRGC) Quds Force were implicated in a terrorist plot to assassinate Saudi Arabia's Ambassador to the United States on United States soil.

(15) On December 26, 2011, the United Nations General Assembly passed a resolution denouncing the serious human rights abuses occurring in the Islamic Republic of Iran, including torture, cruel and degrading treatment in detention, the targeting of human rights defenders, violence against women, and ''the systematic and serious restrictions on freedom of peaceful assembly'' as well as severe restrictions on the rights to ''freedom of thought, conscience, religion or belief''.

(16) President Barack Obama, through the P5+1 process, has made repeated efforts to engage the Government of the Islamic Republic of Iran in dialogue about Iran's nuclear program and its international commitments under the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow July 1, 1968, and entered into force March 5, 1970 (commonly known as the ''Nuclear Non-Proliferation Treaty'').

(17) Representatives of the P5+1 countries (the United States, France, Germany, the People's Republic of China, the Russian Federation, and the United Kingdom) and representatives of the Islamic Republic of Iran held negotiations on Iran's nuclear program in Istanbul, Turkey on April 14, 2012, and these discussions are set to resume in Baghdad, Iraq on May 23, 2012.

(18) On March 31, 2010, President Obama stated that the ''consequences of a nuclear-armed Iran are unacceptable''.

(19) In his State of the Union Address on January 24, 2012, President Obama stated, ''Let there be no doubt: America is determined to prevent Iran from getting a nuclear weapon, and I will take no options off the table to achieve that goal.''.

(20) On March 4, 2012, President Obama stated ''Iran's leaders should understand that I do not have a policy of containment; I have a policy to prevent Iran from obtaining a nuclear weapon''.

(21) Secretary of Defense Leon Panetta stated, in December 2011, that it was unacceptable for Iran to acquire nuclear weapons, reaffirmed that all options were on the table to thwart Iran's nuclear weapons efforts, and vowed that if the United States gets ''intelligence that they are proceeding with developing a nuclear weapon then we will take whatever steps necessary to stop it''.

(22) The Department of Defense's January 2012 Strategic Guidance stated that United States defense efforts in the Middle East would be aimed ''to prevent Iran's development of a nuclear weapons capability and counter its destabilizing policies''.

(23) On April 2, 2010, President Obama stated, ''All the evidence indicates that the Iranians are trying to develop the capacity to develop nuclear weapons. They might decide that, once they have that capacity that they'd hold off right at the edge in order not to incur more sanctions. But, if they've got nuclear weapons-building capacity and they are flouting international resolutions, that creates huge destabilizing effects in the region and will trigger an arms race in the Middle East that is bad for U.S. national security but is also bad for the entire world.''.

(b) SENSE OF CONGRESS.—Congress—

(1) reaffirms that the United States Government and the governments of other responsible countries have a vital interest in working together to prevent the Government of Iran from acquiring a nuclear weapons capability;

(2) warns that time is limited to prevent the Government of the Islamic Republic of Iran from acquiring a nuclear weapons capability;

(3) urges continued and increasing economic and diplomatic pressure on the Islamic Republic of Iran until the Government of the Islamic Republic of Iran agrees to and implements—

(A) the full and sustained suspension of all uranium enrichment-related and reprocessing activities and compliance with United Nations Security Council resolutions;

(B) complete cooperation with the IAEA on all outstanding questions related to the nuclear activities of the Government of the Islamic Republic of Iran, including the implementation of the additional protocol to Iran's Safeguards Agreement with the IAEA; and

(C) a permanent agreement that verifiably assures that Iran's nuclear program is entirely peaceful;

(4) expresses the desire that the P5+1 process successfully and swiftly leads to the objectives identified in paragraph (3);

(5) warns that, as President Obama has said, the window for diplomacy is closing;

(6) expresses support for the universal rights and democratic aspirations of the people of Iran;

(7) strongly supports United States policy to prevent the Government of the Islamic Republic of Iran from acquiring a nuclear weapons capability;

(8) rejects any United States policy that would rely on efforts to contain a nuclear weapons-capable Iran; and

(9) joins the President in ruling out any policy that would rely on containment as an option in response to the Iranian nuclear threat.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as an authorization for the use of force or a declaration of war.

SA 2654. Mr. CRAPO (for himself and Mr. JOHANNS) 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:

SEC. ___. BUSINESS RISK MITIGATION AND PRICE STABILIZATION.

(a) MARGIN REQUIREMENTS.—

(1) COMMODITY EXCHANGE ACT AMENDMENT.—Section 4s(e) of the Commodity Exchange Act (7 U.S.C. 6s(e)), as added by section 731 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, is amended by adding at the end the following new paragraph:

''(4) APPLICABILITY WITH RESPECT TO COUNTERPARTIES.—The requirements of paragraphs (2)(A)(ii) and (2)(B)(ii) shall not apply to a swap in which a counterparty qualifies for an exception under section 2(h)(7)(A) or satisfies the criteria in section 2(h)(7)(D).''.

(2) SECURITIES EXCHANGE ACT AMENDMENT.—Section 15F(e) of the Securities Exchange Act of 1934 (15 U.S.C. 78o–10(e)), as added by section 764(a) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, is amended by adding at the end the following new paragraph:

''(4) APPLICABILITY WITH RESPECT TO COUNTERPARTIES.—The requirements of paragraphs (2)(A)(ii) and (2)(B)(ii) shall not apply to a security-based swap in which a counterparty qualifies for an exception under section 3C(g)(1) or satisfies the criteria in section 3C(g)(4).''.

(b) IMPLEMENTATION.—The amendments made by this section to the Commodity Exchange Act shall be implemented—

(1) without regard to—

(A) chapter 35 of title 44, United States Code; and

(B) the notice and comment provisions of section 553 of title 5, United States Code;

(2) through the promulgation of an interim final rule, pursuant to which public comment will be sought before a final rule is issued; and

(3) such that paragraph (1) shall apply solely to changes to rules and regulations, or proposed rules and regulations, that are limited to and directly a consequence of such amendments.

SA 2655. 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:

On page 23, strike line 18 and all that follows through page 25, line 8.

SA 2656. 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:

On page 145, strike lines 5 through 11 and insert the following:

''(f) ANNUAL REPORT.—Not later than 1 year after

SA 2657. 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:

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

SA 2658. 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:

On page 121, strike lines 13 through 24.

SA 2659. 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:

On page 142, strike line 3 and all that follows through page 145, line 4.

SA 2660. 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:

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

SA 2661. 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:

On page 122, strike line 1 and all that follows through page 124, line 6.

SA 2662. 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 end of title I, add the following:

SEC. 111. SUNSET.

This title is repealed effective on the date that is 3 years after the date of enactment of this Act.

SA 2663. 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 end of title I, add the following:

SEC. 111. SUNSET.

This title is repealed effective on the date that is 5 years after the date of enactment of this Act.

SA 2664. 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:

On page 122, strike lines 18 through 25, and insert the following:

vulnerabilities; and

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

---

PRIVILEGES OF THE FLOOR

Mr. HARKIN. Mr. President, I ask unanimous consent that the following fellow and interns be granted floor privileges for the remainder of the day: Bryan Boroughs, Lucy Stein, Shauna Agan, Douglas Dorando, Keagan Buchanan, and Andrea Jarcho.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

Mr. BROWN of Ohio. Mr. President, I ask unanimous consent that the privilege of the floor be granted to Ben Cohen, a fellow on my staff.

The PRESIDING OFFICER. Without objection, it is so ordered.

NATIONAL WORK AND FAMILY MONTH

Mr. BROWN of Ohio. Madam President, I ask unanimous consent that the Senate proceed to S. Res. 533 submitted earlier today.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 533) designating October 2012 as ''National Work and Family Month.''

There being no objection, the Senate proceeded to consider the resolution.

Mr. BROWN of Ohio. I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, the motion, to reconsider be laid upon the table, with no intervening action or debate, and any statements be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolution (S. Res. 533) was agreed to.

The preamble was agreed to.

The resolution, with its preamble, reads as follows:

S. RES. 533

Whereas, according to a report by WorldatWork, a nonprofit professional association with expertise in attracting, motivating, and retaining employees, the quality of workers' jobs and the supportiveness of the workplace of the workers are key predictors of the job productivity, job satisfaction, and commitment to the employer of those workers, as well as of the ability of the employer to retain those workers;

Whereas ''work-life balance'' refers to specific organizational practices, policies, and programs that are guided by a philosophy of active support for the efforts of employees to achieve success within and outside the workplace, such as caring for dependents, health and wellness, paid and unpaid time off, financial support, community involvement, and workplace culture;

Whereas numerous studies show that employers that offer effective work-life balance programs are better able to recruit more talented employees, maintain a happier, healthier, and less stressed workforce, and retain experienced employees, which produces a more productive and stable workforce with less voluntary turnover;

Whereas job flexibility often allows parents to be more involved in the lives of their children, and research demonstrates that parental involvement is associated with higher achievement in language and mathematics, improved behavior, greater academic persistence, and lower dropout rates in children;

Whereas military families have special work-family needs that often require robust