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. 2—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” 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 this Act.”.

(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 re-inforced 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:

SEC. 1. Short title; table of contents.

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

Sec. 101. Definitions.

Sec. 102. Authorization to share cyber threat information.

Sec. 103. Information sharing by the Federal government.

Sec. 104. Construction.

Sec. 105. Report on implementation.

Sec. 106. Inspector General review.

Sec. 107. Technical amendments.

Sec. 108. Access to classified information.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

Sec. 201. Coordination of Federal information security policy.


Sec. 203. No new funding.

Sec. 204. Technical and conforming amendments.

Sec. 205. Clarification of authorities.

TITLE III—CRIMINAL PENALTIES

Sec. 301. Penalties for fraud and related activity in connection with computers.

Sec. 302. Tampering in passwords.

Sec. 303. Conspiracy and attempted computer fraud offenses.

Sec. 304. Criminal and civil forfeiture for fraud and related activity in connection with computers.

Sec. 305. Damage to critical infrastructure computers.

Sec. 306. Limitation on actions involving unauthorized use.

Sec. 307. No new funding.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

Sec. 401. National High-Performance Computing Program planning and coordination.

Sec. 402. Research in areas of national importance.

Sec. 403. Program improvements.

Sec. 404. Improving access to networking and information technology, including high performance computing.


Sec. 406. Federal cyber scholarship-for-service program.

Sec. 407. Study and analysis of certification and training of information infrastructure professionals.

Sec. 408. International cybersecurity technical standards.

Sec. 409. Identity management research and development.

Sec. 410. Federal cybersecurity research and development.

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(A) Agency.—The term ‘‘agency’’ means the meaning given in the term in section 3502 of title 44, United States Code.

(B) Antitrust laws.—The term ‘‘antitrust laws’’—

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

(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 to be unable to access the information system or information;

(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 compromised 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 Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, the National Protection and Computer Emergency Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term “cybersecurity system” means a system designed or employed to ensure the integrity, confidentiality, availability of, or control over, a system, a system's networks, or the system's constituent parts, including measures or practices that provide—

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

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

(7) ENTITY.—

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

(B) INCLUSIONS.—The term “entity” includes a government agency or department (including an officer, employee, or agent thereof) of any successor center, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, or 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 non-repudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access to and disclosure, including means for protecting private information 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 “information system” of a Federal department or agency under section 302 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 an incident or a linked series of incidents that has the potential to create a direct or indirect or cascading adverse impact or consequence to the Federal department or agency, a State, tribal, or local government or government agency, or any entity supporting critical information infrastructure, that is so severe or extensive that, if successful, would have resulted in—

(A) a failure or impairment of a Federal information system from which 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 in, or transmitted by, or transmitted through 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 (20 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, and to request anonymization of such information, notwithstanding any other provision of law, an entity may disclose 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.

(2) INFORMATION SECURITY PROVIDERS.—If the entity submitting such information is an information security provider, the disclosure described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract, then the entity shall be entitled to the use and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(b) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose 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 entity submitting such information is an information security provider, the disclosure described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract, then the entity shall be entitled to the use and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

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

(1) IN GENERAL.—The term “significant cyber incident” means an incident or a linked series of incidents that has the potential to create a direct or indirect or cascading adverse impact or consequence to the Federal department or agency, a State, tribal, or local government or government agency, or any entity supporting critical information infrastructure, that is so severe or extensive 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) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

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

(d) 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, or 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, and 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 disclosee outside the Federal government may only be used or disclosed 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) may 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 or administrative proceedings 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.

(8) shall not be used in any manner by the Federal government and any disclosee outside the Federal government may only be used or disclosed upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law.

(9) shall not be directly used by any Federal agency or department or any judicial or administrative proceedings with a decision-making official.

(10) shall not be directly used by any Federal, State, tribal, or local government or agency to regulate the lawful activities of an

advance with an entry described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type and extent of information 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 this section.

(5) 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, and 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;
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 section 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 an entity—

(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 manner that includes, but is not limited to, 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;

(D) except as provided in this section, shall not be considered cybersecurity centers, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this section shall not be considered regulations within the meaning of this subparagraph.

(2) SHARING WITH A CYBERSECURITY CENTER.—

(A) may, with the prior written consent of the owner or custodian of such information, except that the conduct of such procedures shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records; and

(B) shall be deemed voluntarily shared information and exempt from disclosure under 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 government 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 section shall not be considered regulations within the meaning of this subparagraph.

(3) ANTI-TRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this section shall not be considered a violation 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 cyber threat information to help prevent, investigate, or mitigate threats or the effects of a threat to information security.

(4) 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 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.

(g) 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 statute, tribal or local law requiring disclosure of information or records.

(h) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTION.—

(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; or

(ii) 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 to preclude any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to obtain any law or procedure governing the appropriate handling, disclosure, and use of classified information.

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

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preclude 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 in consultation with 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 shall comply with—

(A) the appropriate handling, disclosure, and use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.

(1) IN GENERAL.—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—

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

(B) 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 procedures utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures incorporated in this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with the National Cybersecurity Center 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 of this Act, the Federal government—

(1) facilitate information sharing, inter-
ation, and collaboration among and be-
tween cybersecurity centers and—

(A) cybersecurity agencies;

(B) any entity; and

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

(2) facilitate timely and actionable cyber-
security threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation recommendations, 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 GOVERN-
MENT.—The heads of appropriate Federal de-
partments and agencies shall ensure that cyber threat information in the possession of such departments or agencies 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 Department of Homeland Security, 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) 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 of offici-"§ 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 information technology, management, 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 and implementation of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

(5) to provide for the development of mechanisms for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements to reduce overly prescriptive manual reporting.

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 of official 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, to the cybersecurity center;

(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 infor-

mation shared with a cybersecurity cen-
ter 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 impacts the privacy and civil lib-
erties of individuals, any appropriate metrics to determine any impact of the shar-
ing of such information with the Federal government, 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 where such was an inappropriate stoepping within the Federal gov-
ernment of any such information;

(5) a description of any violations of the re-
quirements of this title by the Federal gov-
ernment;

(6) a classified list of entities that received classified information from the Federal government under section 106 of this Act and a description of any indication that such infor-
mation may not have been appropriately handled;

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

(8) any recommendations 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 In-
spectors General on Integrity and Efficiency is authorized to review compliance by the cybersecurity centers and 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 appropriately or, including consideration of the need to pro-
tect the privacy and civil liberties of individ-
uals throughout the use of such information, has made publicly available any steps taken to reduce such impact;

(c) REPORT TO CONGRESS.—Each review con-
ducted under this section shall be presen-
ted 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 (B), by striking ‘‘or’’;

(2) in paragraph (2), by striking ‘‘wells.’’ and inserting ‘‘wells;’’; 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 informa-
tion (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 with-
out the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appro-
priate 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 the Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL
INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMA-
TION SECURITY POLICY.

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

‘‘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 environ-
ment and provide effective government-wide information technology, management, 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 main-
tenance of controls required to protect agen-
cy information and information systems and contribute to the overall improvement of agency information security posture;

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

(5) to provide for the development of mechanisms for improving agency information security programs through continuous monitoring of agency information system operations and streamlined reporting requirements to reduce overly prescriptive manual reporting.

§ 3552. Definitions

In this subchapter:

(1) ADEQUATE SECURITY.—The term ‘‘ade-
quate security’’ means security commensu-
rate 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 mean-
ing given the term in section 3502 of title 44.
changing threats, vulnerabilities, and Budget unless otherwise specified. The term ‘information resources’ has the meaning given the term in section 3502 of title 44.

(6) ENVIROMENT OF OPERATION. The term ‘information system’ means any information system (including any telecommunications systems) used or operated by an agency or by a contractor or other organization on behalf of an agency—

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

(A) involves intelligence activities; 

(B) involves cryptographic activities related to national security; 

(C) involves command and control of military forces; 

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

(E) is protected at all times by procedures established for that purpose 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 any safeguard or countermeasure prescribed for an information system to protect the confidentiality, integrity, or 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 systems 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 security or privacy is compromised or unavailable to an unauthorized individual. 

(20) TECHNICAL CONTROL. The term ‘technical control’ means software, firmware, hardware, or a software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transmitted an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

§ 3553. Federal information security authorizations 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 1131 of title 40 to identify and prioritize information systems and provide for common situational awareness across all agency information systems; 

(B) reporting requirements, consistent with the law, regarding information security incidents; and 

(C) requirements for agencywide information security programs; 

(2) requirements 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 1131 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 or any security policies, 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 security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each level of the chain of command and to other appropriate entities consistent with policies for national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3553(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—

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

‘‘(B) ensuring the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3555(a), and standards and guidelines promulgated under section 1331 of title 48 for information security classification standards and 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 3555(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 authorities 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 information 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 systems in a manner that is consistent with the policies and directives under section 3553;

‘‘(B) develops and maintains, and oversees an agencywide information security program; and

‘‘(C) ensures that information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 1331 of title 48; and

‘‘(4) train and oversee the agency personnel with a significant role in 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 other 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 security controls 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

‘‘(2) ensure that the agency has the capability to ensure the continuity of operations for information systems that support the operations and assets of the agency.

‘‘(d) 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 and cyber threats involving information systems 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) is 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 personnel training, including—

(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.

§ 3556. 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; and

(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) any 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) DISTRIBUTION OF REPORTS.—Each agency应当 perform an annual independent evaluation of the agency’s information security program and practices as directed by the President in accordance with the criteria under subsection (a).

(d) DISTRIBUTION OF REPORTS.—Not later than 90 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.

(e) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall prepare a report evaluating the performance of the evaluation and 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.

§ 3557. National security systems

(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, the Secretaries of Defense and Homeland Security, and other appropriate authorities, shall conduct an 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 the effectiveness of the agencywide information security program (and practices).

(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency head shall perform an annual independent evaluation of the agency’s information security program (and practices) in coordination 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, the Secretary of Defense, and the Director of National Intelligence.

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

§ 3558. 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 to protect information and information system and to minimize the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information that is contained in or processed by the information system;

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

(b) SAVINGS PROVISIONS.
SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities. The head of an applicable Federal agency may employ standards for the security of Federal information systems.

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’’ 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’’.

TITLE III—CRIMINAL PENALTIES

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

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) of this section;

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

‘‘(2) A fine under this subsection, including any seizure under this section, including any seizure under this subsection, shall be governed by the provisions of section 3553(a) of title 18, United States Code, except that—

(1) the term ‘‘seizure’’ has the meaning given in section 3552 of title 18, United States Code, except that—

(2) the term ‘‘seizure’’ has the meaning given in section 3552 of title 18, United States Code; and

(3) the term ‘‘seizure’’ has the meaning given in section 3552 of title 18, United States Code.

‘‘(g) DEFINITIONS.—In this section:

(1) FEDERAL INFORMATION SYSTEM.—The term ‘‘Federal information system’’ means anything provided under section 3552 of title 44.

(2) INFORMATION SECURITY.—The term ‘‘information security’’ means the information security required under paragraph (1) of this subsection.

(3) NATIONAL SECURITY SYSTEM.—The term ‘‘national security system’’ means the information security required under paragraph (1) of this subsection.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended by inserting ‘‘as if for the completed offense’’ after ‘‘punished as provided’’.

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

‘‘(i) 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 person interested 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 property traceable to such property, that such person obtained, directly or indirectly, as a result of an offense under this section; or

(J) any property traceable to such property, that such person obtained, directly or indirectly, as a result of an offense under this section; or

(K) recovery of any property, real or personal, that was used, or intended to be used, to commit

SEC. 305. QUALIFICATION 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.
or facilitate the commission of any violation of this section, or a conspiracy to violate this section; or

(2) 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, including the definition of 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) 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 priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include:

(a) the term 'computer' has the meaning given the term in section 1030;
(1) by redesigning 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 committees of the House of Representatives and the Senate, 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:

"federal agencies and departments;"

and
(B) by redesigning paragraphs (2) and (3), respectively;

(2) by redesigning paragraph (3) as paragraph (6); and
(3) by redesigning paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting after paragraph (2), as redesignated, the following:

"(i) '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”;

"(1) working with 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

"(ii) to ensure that 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 redesigning paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesigning paragraph (3) as paragraph (6);

and
(3) by redesigning paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

"(1) cybersecurity;

"(2) health care;

"(3) energy management and low-power systems and devices;

"(4) transportation, including surface and air transportation;

"(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating solutions to important problems in areas including—

"(i) cyber-security;

"(ii) health care;

"(iii) energy management and low-power systems and devices;

"(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 sections (a) and (c) of section 102 for the next fiscal year by category of activity;

(2) by inserting after section 102—

"(c) 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—

(1) by redesigning subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) 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 sections (a) and (c) of section 102 for the next fiscal year by category of activity;

(3) by redesigning subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively;

"(3) by redesigning subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively;

"(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 committees of the House of Representatives and the Senate, 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:

"federal agencies and departments;"

and
(B) by redesigning paragraphs (2) and (3), respectively;

(2) by redesigning paragraph (3) as paragraph (6); and
(3) by redesigning paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

"(i) '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”;

"(1) working with 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

"(ii) to ensure that 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 redesigning paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesigning paragraph (3) as paragraph (6);

and
(3) by redesigning 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”;

"(1) cybersecurity;

"(2) health care;

"(3) energy management and low-power systems and devices;

"(4) transportation, including surface and air transportation;

"(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating solutions to important problems in areas including—

"(i) cyber-security;

"(ii) health care;

"(iii) energy management and low-power systems and devices;

"(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 sections (a) and (c) of section 102 for the next fiscal year by category of activity;
managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

(2) to take appropriate steps for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant issues and requiring collaboration and to ensure the development of related scientific and technological milestones;

(3) to define the roles and responsibilities of the participants from institutions of higher education, Federal laboratories, and industry in such entity;

(4) to issue guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

(5) to 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) DURATION.—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. 5521) is amended to read as follows:

"SEC. 102. PROGRAM IMPROVEMENTS.

"(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall:

"(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, Federal laboratories, 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 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 industries;

"(6) to ensure accurate and detailed budget reports on 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.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program shall be adjusted as follows:

"(1) IN GENERAL.—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).

"(2) DATABASE.—

"(i) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop, in consultation with the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year for each Program Component Area.

"(ii) 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, 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. 5522(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.


(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" and 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 inserting "networking and information technology"; and

"(B) by striking "high-performance computing network" and inserting "networking and information technology network".

(b) TITLE READING.—The heading of title I of the High-Performance Computing Act of 1991 (U.S.C. 5501) 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 "NATIONAL HIGH-PERFORMANCE COMPUTING" and inserting "NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT"; and

(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 information technology" and inserting "high-end computing, distributed, and networking"; and

"(iii) in subparagraphs (B) and (G), 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 "high-end computing";

(4) in subsection (b)(2), by striking "high-performance computing" and inserting "networking and information technology"; and

(5) in paragraphs (c)(1)(A), by striking "high-performance computing" and inserting "networking and information technology".

(d) SECTION 201.—Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesigning paragraphs (2) through (5) as paragraphs (3) through (6), 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. 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) 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" and each place it appears and inserting "networking and information technology"; and

(3) in paragraph (2)(A), by striking "high-performance computing network" and inserting "networking and information technology network".
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 to pursue undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) provide that scholarship recipients—

(A) are qualified for scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times that portion of years of service completed divided by the number of years of service required, shall be awarded annually to ensure that the program actually improves the Federal government;

(b) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a report on the results of the study. The report shall include—

(1) findings regarding the types of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(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, 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 types of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(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, State and local entities, and the private sector.

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 these skills that personnel of government, academic, and private-sector entities 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 knowledge and various skills described in paragraph (1); and

(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, 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 types of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(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, State and local entities, and the private sector.

SEC. 408. 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 these skills that personnel of government, academic, and private-sector entities 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 knowledge and various skills described in paragraph (1); and

(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, 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 types of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(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, State and local entities, and the private sector.

SEC. 409. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS. 

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal agencies, shall—

(1) ensure 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 report 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 stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall establish a program to support the development of technical standards, metrology, test beds, 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 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 (B), by striking ‘‘and’’; and

(2) in subparagraph (E), by striking ‘‘2007. ’’ and inserting ‘‘2007;’’.

(b) 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’’; and

(2) in subparagraph (E), by striking ‘‘2007. ’’ and inserting ‘‘2007;’’.

(c) 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’’; and

(2) in subparagraph (E), by striking ‘‘2007. ’’ and inserting ‘‘2007;’’.

(d) 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.’’.

(5) 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 misappropriation 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 local government agency or department (including an officer, employee, or agent thereof).

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

The term ‘‘Federal government 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 computer and network information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to preserve—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information non-repudiation and availability;

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

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

(10) INFORMATION SYSTEM.—The term ‘‘information system’’ means a system of components and facilities that (A) automatically processes, stores, or transmits information, and (B) is used to carry out the functions of a Federal department or agency.

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 in the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ‘‘antitrust laws’’—

(A) has the meaning given in the term in section 5 of the Federal Trade Commission Act (15 U.S.C. 41 (including section 3502 of title 44, United States Code), including an officer, employee, or agent thereof);

(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 any 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 signify malicious cyber intent; and

(D) a method of defending an operational control;

(E) 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.’’. 
(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 or network for the purpose of identifying 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 over an information system that is primarily 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) SEC. 702. AUTHORIZATION TO SHARE CYBER INCIDENT INFORMATION.—

(a) VOLUNTARY DISCLOSURE.—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 information that is likely to assist in identifying and subsequently documenting of such cybersecurity threat information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SEC. 702b. NOTIFICATION OF CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information services to a Federal department or agency shall notify the Federal department or agency if a significant cyber incident involving an operational control of that Federal department or agency that:

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

(B) is disclosed to the entity as a result of providing 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 subparagraph (A) or (B) of paragraph (1). The parameters of that type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—The 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 section 2516 of title 18, United States Code, and the Federal government may only be used, disclosed, or handled in accordance with otherwise applicable laws, 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 another entity.

(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 a criminal act, as 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 that may not use 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 submitting 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 its applicability 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(b)(4) 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 or 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 submitting such information, 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 government or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information or any cybersecurity 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 Federal 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 be handled by the entity containing a cybersecurity center, otherwise be disclosed or distributed to any entity submitting such information or records;

(C) is directly known to the entity as a result of providing such services by the entity, otherwise be disclosed or distributed to any other entity in order to assist with the purpose of preventing, investigating, or otherwise mitigating threats to information security across the Federal government;

(2) 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 another entity;

(3) 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 another entity; and

(4) is provided in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of the sharing of cyber threat information with another entity.

(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) 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; and

(3) the heads of each Federal agency or department containing a cybersecurity center shall provide written notice to Congress if the Federal government shares cyber threat information with another entity, including a description of the need to protect the privacy and civil liberties of the sharing of cyber threat information with another entity.

(f) REPORT.—Notwithstanding any other provision of law, the heads of each Federal 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 be handled by the entity containing a cybersecurity center, otherwise be disclosed or distributed to any entity submitting such information or records;

(C) is directly known to the entity as a result of providing such services by the entity, otherwise be disclosed or distributed to any other entity in order to assist with the purpose of preventing, investigating, or otherwise mitigating threats to information security across 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 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 another 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 an interdepartmental or interagency sharing agreement or other provision of law for an entity to provide such entity with—
(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 private entity.
(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing such sharing, such as appropriate anonymization of such information; and
(C) may not be shared in a manner that prohibits the lawful activities of an entity, including activities relating to obtaining, using, or sharing threat information to help prevent, investigate, or mitigate threats to information security; or
(D) shall not be directly used by any State, tribal, or local government or 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 consent that may be provided orally with subsequent documentation of the consent;
(B) shall be deemed voluntarily shared information exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;
(C) shall not be disclosure as attributed to any entity by the State, tribal, or local government or 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 government 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 developed and implemented under this title shall not be considered subparagrapghs within the meaning of this subsection.
(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 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 ON 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.
(1) FEDERAL PREEMPTION.—
(1) 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 except as controlled under any State or local law requiring disclosure of information or records.
(4) CIVIL AND CRIMINAL LIABILITY.—
(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—
(i) the use of cybersecurity centers and cybersecurity systems as authorized by this title;
(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title;
(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.
(B) COMPLIANCE WITH CONDUCT.—Any entity from 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.
(C) SUBMISSION OF 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, classified, and 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.
(1) COMPLIANCE WITH CONDUCT.—
(A) PROVISION OF CYBER THREAT INFORMATION.—The procedures developed under this section shall incorporate, to the 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.
(3) PUBLIC DISCLOSURE.—
(A) REQUIREMENT.—The procedures developed under this section shall incorporate, to the 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.
(4) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 702, a cybersecurity center shall—
(A) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—
(I) other Federal entities;
(II) any entity; and
(III) international partners, in consultation with the Secretary of State;
(B) disseminate timely and actionable cyber threat information to Federal entities to enhance the security posture of the United States;
(C) provide situational awareness of the cybersecurity posture of the United States;
(D) 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.
(2) 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.
(3) 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 to—
(1) to limit or modify an existing information sharing relationship;
(2) to prohibit the exchange of nonpublic information between entities;
(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 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 under Title 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 an 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(e)(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 means such 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 issued 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 affect 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 the 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 to provide cyber threat 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 or by 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 Inspector General on Integrity and Efficiency are authorized to review compliance by the cybersecurity center, Federal government, or any department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 702 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government shared 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 of title 5, United States Code, is amended—

(1) in paragraph (8), by striking “or”;

(2) in paragraph (9), by striking “and” and inserting “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 1 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 under this title unless—

(1) the Department of Commerce;

(2) the Department of Defense;

(3) the Department of Justice;

(4) the intelligence community;

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

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

(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 Executive Order 13526) to access such cyber threat information.

SEC. 709. ATTACHMENT.

This title is subject to the enactment of this Act, and any amendments made by this Act shall be effective during the 3-year period beginning on the date of the enactment of this Act.

SEC. 801. EFFECTIVE DATE.

(a) IN GENERAL.—This Act and the amendments made by this Act shall be effective on the date of the enactment of this Act.

(b) TRANSITION PROVISIONS.—Notwithstanding sections 704 and 706 of this Act, any cause of action arising under the Constitution and laws of the United States shall continue to apply to any actions described in such sections.

SEC. 2627. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the cybersecurity 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 23, line 8.

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

SEC. 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) any other sector-specific Federal agencies, as appropriate; or

(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 any cybersecurity risk identified by such sector coordinating council.

SEC. 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 AMENDMENTS.

(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 an agreement between the United States and a country described in subsection (b) shall be subject to a point of order under section (c) and

(b) Country Described.—A country described in this subsection is a country the government of which is identified as perpetrating or engaging in 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.

(d) 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 continued 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 CYBERWORKER SENDING CAPACITIES.

(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 ‘‘intelligence community’’ has the meaning given that term under section 3(6) 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 cybersecurity personnel and cybersecurity 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 Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate and the Committee on Small Business, the Select 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 covered with Federal agencies;

(C) securing sponsorship by covered Federal agencies; and

(D) obtaining security clearances for employees; and

(3) recommendations, if any, for legislation that would best 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 communications infrastructure 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 defend against cyber security threats, such as quantum technologies used in a secure domain; and

(2) providing an evaluation of the effort to implement the Domain Name System Security Extensions by 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 interact, as with current and future issues that come before the Commission, 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 conduct a study on 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; and

(B) review—

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

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

(b) Authorization of Appropriations.—Congress may authorize the use of appropriations to carry out the study undertaken pursuant to paragraph (1), and may require recommendations to the Commission for the Commission to streamline its rulemaking process.

(c) Recommendations.—Congress may require the Federal Communications Commission to—

(1) make recommendations to the Commission forthwith and as 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; and

(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 for performing 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) 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 49(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. 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. 2. 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:

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) by tampering with a security system of a consumer; or

(II) to make fraudulent transactions on financial accounts.

(ii) RULE OF CONSTRUCTION.—For purposes of this Act, 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 680(p) of the Fair Credit Reporting Act (15 U.S.C. 1681).

(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 638 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 the Federal Government or any subdivision of such unit.

(8) FINANCIAL INSTITUTION.—The term ‘‘financial institution’’ has the same meaning as in section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801).

(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 personally identifying 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 number that is an 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) 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; or

(ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, initiated by a covered entity, such as 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.—

(i) 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, such 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 the information relates.

(ii) RULE OF CONSTRUCTION.—For purposes of clause (i), any policy or procedure implemented or maintained under paragraph (1) shall be adequate if the covered entity—

(A) size and scope of the covered entity; and

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

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

(b) INVESTIGATION REQUIRED.—

(i) IN GENERAL.—If a covered entity determines that a breach of data security has occurred, it 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.

(ii) NOTICE REQUIRED.—If a covered entity determines under subparagraph (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—

(I) notify, in the following order—

(aa) the appropriate agency or authority identified in subsection (a)(1)(A) of this section;

(bb) the entity identified in subsection (a)(1)(B) of this section;

(cc) 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 relating to that account;

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

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

(III) any entity that owns, or is obligated on, a financial account to which the sensitive account information involved in the breach relates.

(c) PRESCRIBED COMPLIANCE BY CERTAIN ENTITIES.

(i) 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 in compliance with the policies and procedures of such institution that are consistent with the policies and procedures of such institution that are designed to comply with the requirements 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—

(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

(c) any entity that owns, or is obligated on, a financial account to which the sensitive account information involved in the breach relates.

(ii) NOTICE REQUIRED.—If a covered entity determines under paragraph (1)(C), if notice is provided to consumers pursuant to the policies and procedures of such institution described in subparagraph (I), and

(iii) 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 subparagraph (I), and

(II) 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 subparagraph (I), and

(III) with respect to the covered entities that are subject to 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, 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 requirements of such agencies and authorities, shall prescribe regulations to implement this title.
S5680

CONGRESSIONAL RECORD — SENATE

July 30, 2012

(b) COORDINATION.—Each agency and authority required to prescribe regulations under subsection (a) shall consult and coordinate with each other agency and authority that may, to the extent possible, prescribe regulations that are consistent and comparable.

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

(1) prescribe the methods by which a covered entity shall provide notice 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 each 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 for any person engaged in providing insurance, by the Secretary of the Treasury relating to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, or any other financial institution owning or controlling a financial institution (other than a bank), an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 461, 464), or a bank holding company and its nonbank subsidiary or affiliate (other than a bank, 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, 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 lender (other than a bank) owned or controlled by a foreign bank, an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 461, 464), or a bank holding company and its nonbank subsidiary or affiliate (other than a bank, broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Reserve System; and

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation, an insured branch or agency 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 Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(6) 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, or any other financial institution owning or controlling a financial institution (other than a bank, a bank holding company, a branch, or agency of a foreign bank, or any subsidiary thereof); or

(7) the provisions of section 803, and the regulations required under section 803, and the regulations required under section 804, shall be enforced exclusively under—

(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. 184 et seq.), include the authority to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

SEC. 809. PROTECTION OF INFORMATION AT FEDERAL AGENCIES.

(a) DATA SECURITY STANDARDS.—Each agency shall implement appropriate standards describing 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 the consumers to whom the information relates.

(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. 810. 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 date 1 year after the date of enactment of this Act.

(b) ADMINISTRATIVE ENFORCEMENT.—(a) IN GENERAL.—Notwithstanding any other provision of law, section 804, 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, 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 lender (other than a bank) owned or controlled by a foreign bank, an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 461, 464), or a bank holding company and its nonbank subsidiary or affiliate (other than a bank, broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Reserve System; and

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation, an insured branch or agency 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 Reserve System;

(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 Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(6) 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, or any other financial institution owning or controlling a financial institution (other than a bank, a bank holding company, a branch, or agency of a foreign bank, or any subsidiary thereof); or

(7) the provisions of section 803, and the regulations required under section 803, and the regulations required under section 804, shall be enforced exclusively under—

(a) 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

(b) notwithstanding the Packers and Stockyards Act (7 U.S.C. 184 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 enforced by any consumer by a class 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 pend-
SA 2642. Mr. Levin submitted an amendment intended to be proposed by him to the bill S. 3414, to authorize the extension of nondiscriminatory treatment (normal trade relations treatment) to products of the Russian Federation and Moldova, to require reports on the compatibility 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), this amendment makes 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) CB0 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. Rusho, 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) 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 acquired or will cause, identify 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 NOTICE.—

(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 the system 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 service provider 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.—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 contracts to operate a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transitory storage of 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 law enforcement agency determines that the notification required under subsection (a) would impede a criminal 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. 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. This subparagraph by a subsequent 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 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;

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

and

(III) 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 other print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was accessed or will cause identity theft or other financial harm.


(iv) Notification to the Internal Revenue Service.

(v) Notification to the Social Security Administration.

(vi) Notification to the Office of the United States Attorney for the district in which the individual resides.

(vii) Notification to the Governor of the state in which the individual resides.

(viii) Notification to the Attorney General of the state in which the individual resides.

(vi) Notification to the state legislature in the state in which the individual resides.

(vii) Notification to the office of the chief of police or sheriff of the county in which the individual resides.

(viii) Notification to the office of the chief of police or sheriff of the city or town in which the individual resides.

(vii) Notification to the emergency management agency in the county in which the individual resides.

(vii) Notification to the emergency management agency in the city or town in which the individual resides.


(vii) Notification to the Internal Revenue Service.

(vii) Notification to the Social Security Administration.

(viii) Notification to the Office of the United States Attorney for the district in which the individual resides.

(ix) Notification to the Governor of the state in which the individual resides.

(x) Notification to the State legislature in the state in which the individual resides.

(xi) Notification to the office of the chief of police or sheriff of the county in which the individual resides.

(xii) Notification to the office of the chief of police or sheriff of the city or town in which the individual resides.

(xiii) Notification to the emergency management agency in the county in which the individual resides.

(xiv) Notification to the emergency management agency in the city or town in which the individual resides.


(xv) Notification to the Internal Revenue Service.

(xvi) Notification to the Social Security Administration.

(xvii) Notification to the Office of the United States Attorney for the district in which the individual resides.

(xviii) Notification to the Governor of the state in which the individual resides.

(xix) Notification to the State legislature in the state in which the individual resides.

(xx) Notification to the office of the chief of police or sheriff of the county in which the individual resides.

(xx) Notification to the office of the chief of police or sheriff of the city or town in which the individual resides.

(xxx) Notification to the emergency management agency in the county in which the individual resides.

(xxxx) Notification to the emergency management agency in the city or town in which the individual resides.


(xxxx) Notification to the Internal Revenue Service.

(xxxx) Notification to the Social Security Administration.

(xxxx) Notification to the Office of the United States Attorney for the district in which the individual resides.

(xxxx) Notification to the Governor of the state in which the individual resides.

(xxxx) Notification to the State legislature in the state in which the individual resides.

(xxxx) Notification to the office of the chief of police or sheriff of the county in which the individual resides.

(xxxx) Notification to the office of the chief of police or sheriff of the city or town in which the individual resides.

(xxxx) Notification to the emergency management agency in the county in which the individual resides.

(xxxx) Notification to the emergency management agency in the city or town in which the individual resides.


(ix) Notification to the Internal Revenue Service.

(x) Notification to the Social Security Administration.

(xi) Notification to the Office of the United States Attorney for the district in which the individual resides.

(xii) Notification to the Governor of the state in which the individual resides.

(xiii) Notification to the State legislature in the state in which the individual resides.

(xiv) Notification to the office of the chief of police or sheriff of the county in which the individual resides.

(xv) Notification to the office of the chief of police or sheriff of the city or town in which the individual resides.

(xvi) Notification to the emergency management agency in the county in which the individual resides.

(xvii) Notification to the emergency management agency in the city or town in which the individual resides.


(xix) Notification to the Internal Revenue Service.

(xx) Notification to the Social Security Administration.

(2) SUBSTITUTE NOTIFICATION.—If the date, estimated date, or estimated date range of the breach of security is not known, the covered entity shall 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.

(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.
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.—Section 801 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. 41 et seq.) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (b), 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) $300,000 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 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.


(iii) An entity covered by the regulations issued under section 240(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.

(iv) 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.

(v) 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.

(2) EXCLUSIONS.—

(1) 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.

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

(3) 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 services are capable of handling, 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 such transmission, routing, intermediate and transient storage, or connections.

SEC. 805. EFFECT ON OTHER LAWS. This title does not preempt 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 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.

(1) DEFINITIONS.—In this section:

(a) 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 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.

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

(c) 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.

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

(3) 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.

(4) 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.

(8) ELECTRIC RELIABILITY ORGANIZATION.—

(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 inadequate 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 cyber security vulnerabilities, 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 cyber security vulnerabilities.

(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).

(6) EMERGENCY AUTHORITY OF SECRETARY.—

(1) IN GENERAL.—If the Secretary determines that immediate action is necessary to prevent or mitigate a cyber security threat, the Secretary may, by order, with or without notice, persons subject to the jurisdiction of the Commission to take such actions as the Secretary determines will best avert or mitigate the cyber security threat.
SEC. 804. LIMITATION.
Section 215(i) of the Federal Power Act (16 U.S.C. 824j(i)) is amended by adding at the end the following:

"(6) LIMITATION.—The ERO shall have authority to develop and enforce compliance with interim reliability standards and emergency orders with respect to a facility used in the local distribution of electric energy only to the extent the Commission determines that the incapacity 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. 824d(d)) is amended by adding at the end the following:

"(7) TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.—Notwithstanding the limitations described in section 804, 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 vulnerabilities; and

"(B) 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 Laborator- ies, 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 and geomagnetic disturbances.

(b) CONTESTS.—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 uncertain- tities 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 de- fined in section 215(a) of the Federal Power Act (16 U.S.C. 824(a)), shall submit to Congress an assessment of whether and to what extent infrastructure affecting the trans- mission of electric power in interstate com- merce should be hardened against electromagnetic events and geomagnetic disturbances, including estimates of the costs and benefits of options to harden the infrastructure.
The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined in accordance with the most recent budgetary estimate for the purpose of this Act, submitted for printing in the Congressional Record by the Chairman of the Committee, provided that such statement has been submitted prior to the vote on passage.

SEC. 864. 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 technology.

(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; and

(3) 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 and industry in such entity; and

(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).

SEC. 807. BUDGETARY EFFECTS.
The budgetary effects of this Act, for the budgetary effects of this Act, submitted for printing in the Congressional Record, shall be determined in accordance with the most recent budgetary estimate for the purpose of this Act, submitted for printing in the Congressional Record by the Chairman of the Committee, provided that such statement has been submitted prior to the vote on passage.

SEC. 842. 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.

(b) Activities.—In developing the strategy established under subsection (a), the Director shall give consideration to activities that—

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

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

(3) 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 ensure security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

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

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

(C) to develop security standards as required under section 607 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:

```
(1) conduct a research program to develop a unified 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 security of industrial control systems;

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

(5) make recommendations for how such system could be funded from Federal, State, and nongovernmental sources;

(6) 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 ensure security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

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

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

(C) to develop security standards as required under section 607 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:

```

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. 2. SPECTRUM EFFICIENCY AND SECURITY FUND.

(a) RETENTION OF UNUSED FUNDS.—Section 118(d)(4) of the Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(4)) is amended by inserting “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:

(2) 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) SPECTRUM EFFICIENCY AND SECURITY FUND.

(4) 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, in consultation with the Director of the National Intelligence, a report on the table; as follows:

TITIE VIII—MISCELLANEOUS

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

(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 the 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; or

(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 ‘primary foreign countries’); and

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

(c) DEFINITIONS.—In this section:

(1) TECHNOLOGY.—The term ‘technology’ means—

(2) TRADE SECRET.—The term ‘trade secret’ has the meaning given that term in subsection (g)(3), in the first sentence, by striking ‘priority foreign countries’; and

SEC. 802. 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 the table; as follows:

At the end, add the following:

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:

SEC. 803. 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 the table; as follows:

At the end, add the following:

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. 799. 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 of Defense for purposes of the process when a network or information system of such contractor shall be penetrated pursuant to subsection (b) is successfully penetrated.

(b) DESIGNATION OF NETWORKS AND INFORMATION SYSTEMS.—The Under Secretary of Defense shall, in coordination with the officials specified in subsection (c), establish criteria for designating the cleared defense contractors’ networks and 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: (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; (5) The Director of the National Reconnaissance Office; (6) The Director of Defense Information Analysis and Processing; (7) The Director of the Defense Advanced Research Projects Agency; (8) The Director of Operational Test and Evaluation; (9) The Director of the Defense Security Service; and (10) The Deputy Under Secretary of Defense for Intelligence.

(d) PROCESS REQUIREMENTS.—

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

(2) REPORT ELEMENTS.—The report required by subsection (a) 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 subject to control or, 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.

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.

(b) THE CYBER TRAINING RANGE OPERATED BY THE CYBERSPACE RESEARCH CENTER.—The Cyber Training Range operated by the Cyber Space Research Center provides realistic cyber training for cadets that will benefit the entire Air Force.

(c) THE CYBER TRAINING RANGE.—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.

(d) THE CYBER TRAINING RANGE.—The Cyber Training Range, including the Cyber Space Research and the Cyber Training Range, is subject to the reporting process established pursuant to subsection (a).

(e) CIVILIAN 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.

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

(c) OFFICIALS.—The officials specified in subsection (a) shall provide for rapid reporting of a successful penetration of designated network or information systems.

(b) REPORT ELEMENTS.—The report required by subsection (a) 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 subject to control or, 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.

SEC. 416. CYBER TRAINING AND RESEARCH AT THE UNITED STATES AIR FORCE ACADEMY, COLORADO.

(a) FINDINGS.—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.

(b) FINDINGS.—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.

(b) FINDINGS.—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.

(b) FINDINGS.—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.

(b) FINDINGS.—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.
(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 identifies 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 communications infrastructure of the 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”.

(21) Secretary of Defense Leon Panetta 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 capabilities and they are floating 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.”

(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:

TITLExVIII—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 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 various concerns regarding possible military dimensions to Iran’s nuclear programme; and
(B) states that “Iran has carried out activities related to the development of a nuclear device”; and
(C) states that the efforts described in paragraphs (1) and (2) may be ongoing.
(4) On November 8, 2011, Iran had produced, according to the IAEA—
(A) approximately 630 kilograms of uranium hexafluoride enriched up to 3.5 percent uranium-235; and
(B) no uranium hexafluoride enriched up to 20 percent uranium-235.
(5) As of November 8, 2011, Iran had produced, according to the IAEA—
(A) nearly 5,000 kilograms of uranium hexafluoride enriched up to 3.5 percent uranium-235; and
(B) 79.7 kilograms of uranium hexafluoride 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 hexafluoride up to 20 percent uranium-235.
(7) Section 2(2) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (Public Law 111–196) 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; and
(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 matter of self-defense, look into all the 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 United States has designated 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, representatives of Iran’s Islamic Revolutionary Guard Corps (IRGC) Quads 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, and ill-treatment 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 United Kingdom, China, and Russia), and representatives of the Islamic Republic of Iran held negotiations on Iran’s nuclear program in Istanbul, Turkey, 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 “Iran is a dangerous and nuclear-armed Iran is 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, and said that all options were on the table to thwart Iran’s nuclear weapons efforts, and vowed that if the United States gets “intel-
SEC. 1. BUSINESS RISK MITIGATION AND PRICE STABILIZATION.

(a) Margin Requirements.—

(1) Commodity Exchange Act Amendment.—Section 4(e)(5) of the Commodity Exchange Act (7 U.S.C. 6a(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)(i) and (2)(B)(ii) shall not apply to a swap in which a counterparty qualifies for an exception under section 2(b)(7)(A) or satisfies the criteria in section 2(b)(7)(D)."

(2) Securities Exchange Act Amendments.—Section 15F(e) of the Securities Exchange Act of 1934 (15 U.S.C. 78o–10(e)), as added by section 756(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)(i) and (2)(B)(ii) shall not apply to a 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 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 by the Commission, which public comment will be sought before a final rule is issued; and

(3) such that paragraph (1) shall apply solely 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 23, strike line 18 and all that follows through page 25, line 8.

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

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 13 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 Jarché.

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 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

...