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

SA 2633. Mr. GRAHAM submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2634. Mr. CRAPO (for himself and Mr. JOHANNETT) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2635. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2636. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2637. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2638. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2639. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2640. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2641. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2642. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2643. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2644. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2621. Mr. DeMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. 205. 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—

(i) in subsection (A), by striking the period at the end and inserting “700-mile fence requirement”;

(ii) in subparagraph (B)—

(A) in clause (i), by striking “and” and inserting “;”;

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

(C) by adding at the end the following:

“(iii) funding not contingent on consultation.—Amounts appropriated to carry out this paragraph may not be impounded or otherwise withheld for failure to fully comply with the consultation requirement under clause (i).”;

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

(1) the progress made in completing the re-infused 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 all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Enhancing Cybersecurity Act of 2012”.

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

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Authorization to share cyber threat information.
Sec. 4. Information sharing by the Federal government.
Sec. 5. Construction.
Sec. 6. Report on implementation.
Sec. 7. Final report.
Sec. 8. Flexibility.
Sec. 9. Authorization of appropriations.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

Sec. 101. Coordination of Federal information security policy.
Sec. 102. Management of Federal information security programs.
Sec. 103. Information security by the Federal government.
Sec. 104. Cybersecurity interoperability.
Sec. 105. Report on implementation.

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 computing systems.
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. Improvements 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.
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 computing systems.
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. Improvements 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.
of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and the Threat Operations Center.

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

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

(B) theft or misappropriation of private or governmental 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 (including 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 a system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

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

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

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

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

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

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

(12) MALICIOUS RECONNAISSANCE.—The term “malicious reconnaissance” means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

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

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

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

(16) SIGNIFICANT CYBER INCIDENT.—The term “significant cyber incident” means a cybersecurity incident that, had it occurred, would have resulted in—

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

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

(17) TECHNICAL CONTROL.—The term “technical control” means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored in, transmitted through, or maintained on 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, on its own networks, or as authorized by another entity, on such entity’s networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

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

(A) a cybersecurity center; or

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

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

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (1), including clarification of the information provided to a cybersecurity center under this subsection to a cybersecurity center,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(24) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.
entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

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

(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; and

(B) shall 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 allows, after considering the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, and fully accommodating 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 threat information with the Federal government; and

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

(2) a Federal agency or department, under subsection (b) is provided immediately to a cybersecurity center, and that includes the ability to provide information to the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

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

(2) CYBER THREAT INFORMATION SHARED BY ANY ENTITY WITH ANOTHER ENTITY UNDER THIS TITLE—

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

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

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

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

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

(C) shall not be shared or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information to the Federal government, to a 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 title shall not be considered regulations within the meaning of this subparagraph.

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

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

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

(g) 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.

(h) 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 a cyber threat information shared, through the cybersecurity center, and that includes the ability to provide information to the Federal government.

(2) STATE LAWS.—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.

(i) PUBLIC DISCLOSURE.—No information shared with or provided to a cybersecurity center, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(j) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall be brought in any court against an 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.

(k) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this Act shall affect not any requirement under any provision of law of a State, tribal, or local government—

(1) to incorporate, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center.

(2) to facilitate and promote the sharing of cyber threat information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) to the appropriate handling, disclosure, or use of classified information.

(l) INFORMATION SHARED WITH THE FEDERAL GOVERNMENT.—

(A) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and the heads of the appropriate Federal departments and agencies, shall develop and promulgate procedures to facilitate and promote—

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

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

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section shall be able to limit or prohibit otherwise lawful disclosures of communications, records, or other information by the Federal government to any other governmental or private entity not under this section.

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

(n) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this Act shall not affect any requirement under any provision of law of a State, tribal, or local government.
threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102 of this Act, the center shall—

(1) facilitate information sharing, inter-

action, and collaboration among and be-

tween cybersecurity centers and—

(A) cybersecurity entities; (B) any entity; and

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

(2) facilitate timely and actionable cy-

bersecurity threat, vulnerability, mitiga-

tion, and warning information, including alert-

s, advisories, indicators, signatures, and mitigat-

ing response measures, to improve the security and protection of information systems; and

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

(e) SHARING WITHIN THE FEDERAL 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 relating 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 heads of the agencies of the Intelligence Community, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—

Nothing in this title shall be construed—

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

(2) to prohibit a new information sharing relationship;

(3) to limit the sharing of cyber threat information with an entity on such entity’s express consent; 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) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to require or compel the Federal government—

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

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

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

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

(e) NO NEW FUNDING.—An applicable Fed-

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

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties office of the appropriate Federal department or agency and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

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

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

(3) a review of the type of cyber threat informa-

tion shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberti-

es 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 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 such information, a review of inappropriate stovepiping within the Federal government 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 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of 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 a reasonable manner, including any failure by the Federal government that resulted in substantial 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 reasonably and, including consideration of the need to protect the privacy and civil liberties of individuals throughout, has made publicly available other appropriate methods, while fully accomplishing the objective of this title.

(c) REPORT TO CONGRESS.—Each review con-

cluded under this section shall be pre-

mitted to Congress not later than 30 days after the date of completion of the review.
(3) CYBERSECURITY CENTER.—The term ‘cybersecurity center’ means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

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

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

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

(C) malicious reconnaisance, 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) network activity or protocols known to be associated with a malicious cyber actor or that otherwise affect the cyber threat environment;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed, or transmitted by an information system to inadvertently enable the defeat of a technical or operational control; or

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

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

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

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

(6) ENVIRONMENT OF OPERATION.—The term ‘environment of operation’ means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technical controls, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

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

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

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

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

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

(10) INFORMATION SECURITY.—The term ‘information security’ means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide confidence in the information and information systems that the information is stored on, processed by, or transmitting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

§ 3553. Federal information security authority and coordination

(1) In general.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

(a) 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 guide information systems prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

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

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

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

(C) reporting requirements, consistent with laws, regulations, and policies regarding information security incidents and cyber threat information;

(D) requirements for agencywide information security programs; and

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

(b) review requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subsection;

(c) 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 subsection;

(d) coordinate the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 276g–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 subsection;

(c) Award.—The Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 1131 of title 40.

(11) NATIONAL SECURITY SYSTEM.—The term ‘National Security System’ means any system that is—

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

(B) information technology that is—

(i) information technology that is—

(1) information security; and

(ii) 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.

(II) involves command and control of military forces;

(III) involves cryptologic activities related to national security;

(iv) involves command and control of military forces;

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

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

(II) is protected at all times by procedures established for that equipment 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.

(12) INFORMATION TECHNOLOGY.—The term ‘information technology’ has the meaning given the term in section 11310 of title 40.

(13) MALICIOUS RECONNAISSANCE.—The term ‘malicious reconnaissance’ means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) NATIONAL SECURITY SYSTEM.—The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency—

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

(i) involves intelligence activities;

(ii) involves cryptologic activities related to national security; or

(iii) involves command and control of military forces;

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

(v) involves command and control of military forces; or

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

(vii) involves command and control of military forces; or

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

(ix) involves command and control of military forces; or

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

(xi) involves command and control of military forces; or

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

(xiii) involves command and control of military forces; or

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

(xv) involves command and control of military forces;

(B) involves the function, operation, or use of a computer system used or operated by an agency or by a contractor of an agency; or

(C) involves any combination of subparagraphs (A) through (B).

(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 a technical control, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

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

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

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

(20) TECHNICAL CONTROL.—The term ‘technical control’ includes software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transmitting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.
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 protection 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 applying to any system of the agency operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

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

“(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threats, information, and deterioration of security controls to the individual or entity designated at each level of authority and to other appropriate entities consistent with policies for non-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 3553;

“(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets of the agency, 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, by selecting the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and other requirements;

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

“(D) acting on the basis of implementing information security security controls and techniques; and

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

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

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

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

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

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

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

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

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

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

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

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

“(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency’s information or information systems in a cost-effective manner and in accordance with the policies and directives under section 3553; and

“(B) reports any information security incident under subsection (a)(5) to the entity designated under section 3555;

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

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

“(4) train and oversee the agency personnel 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 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 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, to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

“(B) ensuring that the agency information systems maintain the continuity of operations for information systems that support the operations and assets of the agency.

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

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

“(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;
§ 3556. Independent evaluations

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

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

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

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

§ 3557. National security systems

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

(1) provides information security protections to protect against the magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained therein;

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

(b) SAVINGS PROVISIONS.
"§ 11331. Responsibilities for Federal information systems standards

(a) STANDARDS AND GUIDELINES.—

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

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

(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

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

(b) MANDATORY STANDARDS AND GUIDELINES.—

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

(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

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

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

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

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

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

TITLE III—CRIMINAL PENALTIES

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

Section 1029(c) of title 18, United States Code, is amended to read as follows:

(c) The punishment for an offense under subsection (a), (b), or (b)(1) 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 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; or

(3) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B) of this section.

(b) A fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(B) of this section; or

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

CHAPTER 102—CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

Section 1083(b) of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

(i) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of any provision of State law, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of the Constitution or laws of the United States in furtherance of the act which constitutes or aids in the commission of such violation; and

(j) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of the Constitution or laws of the United States in furtherance of the act which constitutes or aids in the commission of such violation; and

SEC. 302. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1083(c) of title 18, United States Code, is amended to read as follows:

(c) 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—

(1) the property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

(2) the property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of this title; or

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

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

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

Section 1083 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—

(1) the property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

(2) the property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of this title; or

(j) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of, or in connection with, any violation of this title; or

SEC. 305. CIVIL FORFEITURE.—

Section 1083(c) of title 18, United States Code, is amended by inserting ‘‘as if for the completed offense’’ after ‘‘punished as provided’’.
or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

"(B) Any property, real or personal, constituting or used in, or intended to be used in, any fraud or deceit through any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

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

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

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

"(a)(2)(A) shall include—

"(1) of the operation of the critical infrastructure computer or

"(2) of the critical infrastructure associated with the computer;

"(c) Penalty.—Any person who violates subsection (b) shall—

"(1) be fined under this title;

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

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

"(d) Penitentiary Sentence.—Notwithstanding any other provision of law—

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

"(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for such crime as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

"(d) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

"(b) Technical and Conforming Amendment.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

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

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

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

SEC. 307. NO NEW FUNDING.

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

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

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

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

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

"(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology.

"(A) through collaborations across agencies;

"(B) through collaborations across Program Component Areas;

"(C) through collaborations with industry;

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

"(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1995 (15 U.S.C. 3700)); and

"(F) through collaborations with international organizations;

"(2) addressing national, multi-agency, multi-faced challenges of national importance;

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

"(b) Development of Strategic Plan.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

"(e) Strategic Plan.—

"(1) In General.—Not later than 1 year after the date of enactment of the Strengthening America’s Capability and Readiness Act of 1991 (15 U.S.C. 5511(a)(2))—

"(a) National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

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

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

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

"(3) the anticipated time frame for achieving the near-term objectives;

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

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

"(3) Implementation Roadmap.—

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

"(B) Requirements.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the strategic plan under section 101(a)(3). The implementation roadmap shall—

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

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

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

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

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

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

"(5) Report to Congress.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan for this subsection, including the implementation roadmap and any updates under paragraph (3), to—

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

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

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

"(c) Periodic Reviews.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

"(f) Periodic Reviews.—The agencies under subsection (a)(3)(B) shall—

"(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

"(2) ensure that the Program includes national priority multi-agency, multi-faced research and development activities, including activities described in section 101.

(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 councils established under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;"

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following:

"in each Program Component Area and each research area supported in accordance with section 104;"

(B) by striking "high-performance" in subparagraph (D) and inserting "high-end"; and

(2) by amending paragraph (2) to read as follows:

"(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every three years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan."


(1) in subparagraph (C)—

(A) by striking "is submitted," and inserting "is submitted, the levels for the previous fiscal year;" and

(B) by striking each Program Component Area and inserting "each Program Component Area and each research area supported in accordance with section 104;"

(2) in subparagraph (D)—

(A) by striking "is submitted," and inserting "is submitted, the levels for the previous fiscal year;" and

(B) by striking "each Program Component Area and inserting "each Program Component Area and each research area supported in accordance with section 104;"

(3) by redesigning subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

"(E) include a description of how the objectives for activities that involve physical phenomena;"
managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;''

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

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

(4) to provide 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 cyberspace, 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.

(3) The task force shall terminate upon transmittal of the report required under subsection (d).

(4) 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(a)) is amended to read as follows:

"SEC. 102. PROGRAM IMPROVEMENTS.

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

(1) to provide technical and administrative support to—

(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

(B) the advisory committee under section 101(h); and

(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and program 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 reporting of networking and information technology research and development investment; and

(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

(b) SOURCE OF FUNDING.—

(1) In general.—The functions under this section shall be supported by funds from each agency participating in the Program.

(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency’s share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

(c) DATABASE.—

(1) In general.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

(A) a description of the project;

(B) each agency, industry, institution of higher education, laboratory, or international institution involved in the project;

(C) the source funding of the project (set forth by agency); and

(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’’ 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 (15 U.S.C. 5511) 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’’;

(2) in subsection (a), by striking—

(A) in the section 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’’;

(iii) in subparagraphs (B) and (G), by striking—

(A) ‘‘high-performance computing’’ each place it appears and inserting ‘‘high-end’’; and

(B) ‘‘high-performance computing and networking’’ each place it appears and inserting ‘‘networking and information technology’’;

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ‘‘high-performance computing’’ each place it appears and inserting ‘‘networking and information technology’’; and

(II) by striking ‘‘development, networking,’’ each place it appears and inserting ‘‘development,’’; and

(ii) in subparagraphs (G) and (H), by redesigning—

(A) by striking ‘‘high-performance computing network’’ each place it appears and inserting ‘‘high-end’’;

(B) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ‘‘high-performance computing network’’ each place it appears and inserting ‘‘networking and information technology network’’;

(C) in subsection (c)(1)(A), by striking ‘‘high-performance computing network’’ and inserting ‘‘networking and information technology network’’;

(d) SECTION 201.—Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)(1)) is amended by striking the term ‘‘high-performance computing’’ and inserting—

"high-end’’; and

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended—

(1) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’;

(2) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(3) by inserting after section 202(b) the following:

"SEC. 203. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY.


(1) by striking ‘‘high-performance computing’’ and inserting—

(A) ‘‘high-end’’; and

(B) ‘‘networking and information technology’’; and

(2) by inserting after section 203(b) the following:

"SEC. 204. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY.


(1) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(2) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’.

(f) SECTION 205.—Section 205 of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended—

(1) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(2) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting—

(A) ‘‘high-end’’; and

(B) ‘‘networking and information technology’’; and

(C) by striking—

(i) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(ii) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’.

(g) SECTION 206.—Section 206 of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended—

(1) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(2) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting—

(A) ‘‘high-end’’; and

(B) ‘‘networking and information technology’’; and

(C) by striking—

(i) in paragraph (1), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’; and

(ii) in paragraph (2), by striking ‘‘high-performance computing and networking’’ and inserting ‘‘networking and information technology’’.
SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) In General.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require scholarship recipients to first condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to any internship in the cybersecurity field, if applicable, following the completion of a service obligation under paragraph (4);

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation;

(5) provide opportunities for students to receive temporary appointments for meaningful employment on Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

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

(d) ELIGIBILITY REQUIREMENTS FOR A SCHOLARSHIP.—

(1) an evaluation of the body of knowledge and skills the students possess and the capabilities of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs 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 skills that students possess and the capabilities of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described at (a); 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 and the private sector, an examination of the current and future capacity of United States higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

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

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

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with appropriate Federal agencies, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.
(b) Consultation With the Private Sector.—In carrying out the activities under subsection (a)(1), the Director shall consult with appropriate private sector stakeholders, and shall continue to carry out the requirements of this section for fiscal years 2012 through 2013.

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, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) National Science Foundation Computer and Network Security Research Grant Areas.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(1)) is amended—

(1) in subparagraph (H), by striking “and” and inserting “and”;

(2) in subparagraph (E), by striking “property,” and inserting “property;”;

and

(3) by adding at the end the following:

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

“(K) system security that addresses the building of secure systems from trusted and untrusted components;

“(L) monitoring and detection; and

“(M) resiliency and rapid recovery methods.”.

(b) National Science Foundation Computer and Network Security Grants.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(3)) is amended—

(1) in subparagraph (D), by striking “2007.”;

(2) in subparagraph (E), by striking “2007.”;

and

(3) by adding at the end the following:

“(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.”.

(f) Graduate Traineeships in Computer and Network Security Research.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking “and”;

(2) in subparagraph (E), by striking “2007.”;

and

(3) by adding at the end the following:

“(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.”.

SEC. 4264. 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:

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 3092 of title 44, United States Code.

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

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

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

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

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

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

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

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

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

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

(E) a method of defeating an operational control;

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

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transmitted an information system to inadvertently enable the defeat of a technical or operational control;

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

(I) the actual or potential harm caused by a cyber threat; and

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

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

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

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

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

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

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

(9) INFORMATION SECURITY.—The term ‘information security’ means an automated or manual 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 authentication of originators; and

(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 an automated or manual 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 authentication of originators; and

(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.
(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 discovering 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 of an information system that, primarily, is implemented and executed by people.

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

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

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

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

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

(17) TECHNICAL CONTROL.—The term "technical control" means a hardware or software restriction or access control that is an information system or information that is stored on, processed by, or transmitted as an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

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

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

SEC. 702. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—Notwithstanding any other provision of law, any 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 necessary to otherwise possess cyber threat information.

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

(1) a cybersecurity center; or

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

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

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

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or data centering services to a Federal department or agency shall report the Federal department or agency of a significant cyber incident involving any Federal department or agency of significant cyber incident involving any Federal department or agency that—

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

(B) is directly known 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 this paragraph that shall include—

(A) an operational or technical control that information system or information that is stored on, processed by, or transmitted as an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(3) 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 any other law.

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

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department containing a cybersecurity center, or any State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each 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;

(2) an entity submitting such information, or an entity that is in possession of such information;

(3) a cybersecurity center containing a cybersecurity center, or any State, tribal, or local government or government agency, 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; and

(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 section (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) 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.

(3) 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 another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(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 any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(9) 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 any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(10) 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.

(11) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(12) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(13) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(14) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(15) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(16) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;

(17) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to another entity by the entity, including activities relating to obtaining, identifying, or otherwise possessing any information that is in, or originates from, technology that is covered by the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph;
(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 or pursuant to the written consent of the entity authorizing such sharing, such as appropriate anonymization of such information; and
(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing such sharing.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—
(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining 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; and
(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and
(D) shall not be directly used by any State, tribal, or local 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.

(4) ANTI-TRUST 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 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.

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

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

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available by any governmental or private entity not covered under this section.

(1) IN GENERAL.—The procedures developed under paragraph (3) shall ensure that each entity receiving classified cyber threat information pursuant to this section, shall be made aware of the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of such classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, non-protected controlled unclassified information, and cyber threat information in the possession of the Federal government—
(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and
(2) if appropriate, is made publicly available.

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

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

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 702, a cybersecurity center shall—
(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—
(A) other Federal entities; and
(B) international partners, in consultation with the Secretary of State;
(2) disseminate timely and actionable cyber threat threat information, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and
(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

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

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit to Congress 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; or
(2) to prohibit a new information sharing relationship; or
(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—
(1) require an entity to share information with the Federal government, except as expressly provided under section 702(b); or
(2) to limit or modify an existing information sharing relationship; or
(3) to prohibit a new information sharing relationship; or
(4) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 702(b); or
(5) 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.
(2) to condition the sharing of cyber threat information with an entity on such entity’s provision of cyber threat information to the Federal government;

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

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of a department or agency of the Federal government to retain or use any information shared under section 702 for any use other than a use permitted under subsection 702(c)(1).

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

SEC. 705. REPORT ON IMPLEMENTATION.

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

(1) an assessment of the sufficiency of the procedures developed under section 703 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances 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 be used to protect 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 such cybersecurity center with 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 stoviping 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 that has been appropriately classified in such section 703 of this Act and the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(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 Inspector General of the United States shall review, as part of the Inspector General’s semiannual report to Congress, the implementation of this title.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall be conducted within 180 days after the date of enactment of this Act, and shall be submitted to Congress not later than 30 days after the date of completion of the review.

SEC. 707. TECHNICAL AMENDMENTS.

Section 552a(c)(1) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ‘‘wells.’’

(2) in paragraph (9), by striking ‘‘wells,’’

(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 Act in a manner that is not authorized under subsection (b), unless the President, acting through the Executive (as defined in section 8.1 of Executive Order 13335 (50 U.S.C. 435 note; relating to classified national security information)) has determined that the sharing or disclosure of such information will not result in significant national security risk.

(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 obtaining an appropriate security clearance, in order to ensure that cyber threat information under this title is appropriately handled.

SEC. 709. SECURITY CLEARANCES FOR STATE AND LOCAL GOVERNMENTS.

(a) IN GENERAL.—Any individual who is an employee of a State or local government shall be considered to be an employee of the Federal government as provided in section 702 of this Act.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall make available, upon request, classified information to members of the National Guard of a State, including an individual or unit which is directly supporting a Department of Defense mission.

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

(d) REMOVAL.—Any civil action arising from a cyber-related incident that has impacted, or may impact, the information security of an information system of such entity, or any action for breach of contract, liability, or other appropriate relief, shall be dismissed without prejudice.

SEC. 710. VOLTARY CYBERSECURITY PRACTICES.

(a) IN GENERAL.—Nothing in this title shall be construed to subject any owner or operator for choosing not to engage in the voluntary activities authorized under this title.

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

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

(d) REMOVAL.—Any civil action arising from a cyber-related incident that has impacted, or may impact, the information security of an information system of such owner or operator, or any action for breach of contract, liability, or other appropriate relief, shall be dismissed without prejudice.
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 IMPELLING 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 any amendment 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 the illicit 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.

**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 commission may appoint an electrical engineer or computer scientist to provide the commissioner technical consultation when appropriate and to interface with the Office of Engineering and Technology, Commission Bureaus, and other technical staff of the Commission for additional technical input and resources, provided that such engineer or scientist holds an undergraduate or graduate degree from an institution of higher education in their respective field of expertise.”.

**SEC. 803. TECHNICAL POLICY AND PERSONNEL STUDY.**

(a) Study.—

(1) Requirements of study.—The Chairman, 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 of technical policy decision-making and the technical personnel at the Commission.

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

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

(B) review—

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

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

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

(D) evaluate the current staffing levels and skill sets of technical personnel at the Commission to determine if such staffing levels and skill sets are aligned with the current and future needs of the Commission; and

(E) make recommendations for the Commission to streamline its rulemaking process.

(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 related security concerns for the covered 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, the Committee on Homeland Security, and the Committee on Intelligence of the House of Representatives a report on the results of the study under subsection (b) that contains—

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

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

(A) cybersecurity for covered Federal agencies;

(B) securing classified information technology systems for covered Federal agencies;

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

(D) obtaining security clearances for employees;

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

(4) recommendations for overcoming the challenges described in paragraph (2) including the feasibility of and benefits to the Federal Government, the private sector, and small business concerns of establishing a program that would use small business concerns as incubators for developing cyberworkers who have top secret or sensitive compartmented information security clearances while the small business concerns perform other cybersecurity for covered Federal agencies; and

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

**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:

**TITLE VIII—FCC TECHNICAL EXPERTISE CAPACITY**

**SECTION 801. SHORT TITLE AND CONGRESSIONAL FINDING**

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 commission may appoint an electrical engineer or computer scientist to provide the commissioner technical consultation when appropriate and to interface with the Office of Engineering and Technology, Commission Bureaus, and other technical staff of the Commission for additional technical input and resources, provided that such engineer or scientist holds an undergraduate or graduate degree from an institution of higher education in their respective field of expertise.”.
Commission and shall include a recommendation on the appropriate number or percentage of technical personnel that should constitute the Commission workforce;

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

(F) examine—

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

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

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

(b) the National 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.

Offset of Administrative Costs.—Section 4(a) of Public Law 109-34 (47 U.S.C. 703(a)) is amended by striking “annual” and inserting “biennial.”

SA 2635. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. 1. SMALL BUSINESS REGULATORY TRANS- PARENCY.

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

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

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

(3) by adding at the end the following:

“(4) the Department of Homeland Security.”

SA 2636. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title I, add the following:

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

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

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

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

SA 2637. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

SEC. 416. REPORT BY SMALL BUSINESS INFOR- MATION ASSISTANCE FORCE.

Not later than 1 year after the date of enactment of this Act, the Small Business Information Security Task Force, in consulta- tion 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 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. 1. PROHIBITION OF TREASURY REGULA- TIONS WITH RESPECT TO INFORMATION REPORTING ON CERTAIN INFORMATION TELD TO NONRESIDENT ALIENS.

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

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

(2) which is paid—

(A) to a nonresident alien; and

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

SA 2639. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. 1. REPEAL OF RENEWABLE FUEL STAND- ARD.

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

Beginning on page 109, strike line 4 and all that follows through page 110, line 20, and insert the following:

(d) CYBERSECURITY MODELING AND TEST BEDS.—

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

(2) ESTABLISHMENT OF PROGRAM.—

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

(B) REQUIREMENTS.—

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

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

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

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

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

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

(1) the National Institute of Standards and Technology;

(2) the Department;

(3) other Federal agencies;

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

SA 2641. Mr. CARPER (for himself and Mr. BLUNT) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—ACCOUNT DATA SECURITY

SEC. 801. SHORT TITLE.

This title may be cited as the “Data Secu- rity 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.
SEC. 803. PROTECTION OF INFORMATION AND SECURITY BREACH NOTIFICATION.

(a) Security Procedures Required.—

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

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

(A) size and nature of a covered entity; (B) nature and scope of the activities of such entity; and (C) sensitivity of the consumer information to be protected.

(b) Investigation Required.—

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

(A) to assess the nature and scope of the breach; (B) to identify any sensitive account information or sensitive personal information that may have been involved in the breach; and (C) to determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

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

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

(1) notify, in the following order—

(A) the appropriate agency or authority identified in section 804(b)(1); (B) an appropriate law enforcement agency; (C) any entity that owns, or is obligated on, a financial account to which the sensitive account information relates, if the breach involves a breach of sensitive account information; or (D) 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

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

(d) Presumed Compliance by Certain Entities.—

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

(A) in the case of a financial institution—

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

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

(I) 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

(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

(B) subsections (a), (b), and (c), if the entity is a covered entity for purposes of the regulations promulgated under section 206(c) of the Portability and Accountability Act of 1996 (42 U.S.C. 13204-2 note), to the extent that such entity is in compliance with such regulations.

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

SEC. 804. IMPLEMENTING REGULATIONS.

(a) IN GENERAL.—Notwithstanding any other provision of law, 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 this section, shall prescribe regulations to implement this title.
(b) COORDINATION.—Each agency and authority required to prescribe regulations under subsection (a) shall consult and coordinate with each other agency and authority identified in section 905 so that, to the extent possible, the regulations prescribed by each agency and authority are consistent and comparable.

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

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

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

(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 under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g), if the breach of data security involves sensitive personal information.

e. TIMING OF NOTICE.—The regulations required under subsection (a) shall—

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

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

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

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

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

SEC. 805. ADMINISTRATIVE ENFORCEMENT.

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

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

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

(B) a member bank of the Federal Reserve System (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), a commercial lender (other than a bank holding company or nonbank subsidiary or affiliate (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Governors of the Federal Reserve System; and

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

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

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

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

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

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

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

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

(9) the Federal Trade Commission Act (15 U.S.C. 45 et seq.) and section 4 for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8).

(b) AUTHORITY OF COMMISSION FOR ADMINISTRATIVE ENFORCEMENT.—The authority of the Commission to enforce compliance with section 803, and the regulations required under section 804, shall—

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

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

(c) NO PRIVATE RIGHT OF ACTION.—

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

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

SEC. 806. PROTECTION OF INFORMATION AT FEDERAL AGENCIES.

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

(1) to ensure 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. 807. RELATION TO STATE LAWS.

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

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

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

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

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

SEC. 808. DELAYED EFFECTIVE DATE FOR CERTAIN PROVISIONS.

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

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

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

(b) ADMINISTRATIVE ENFORCEMENT.—Section 805 shall take effect 1 year after the date of enactment of this Act.
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:

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

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), amendments made by this Act shall not take effect until the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act.

(b) CBQ 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.

Mr. TOOMEY (for himself, Ms. SNOWE, Mr. DEMINT, Mr. BLUNT, Mr. RUHIO, 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 is compromised as a result of the breach.

(2) LAW ENFORCEMENT.—A covered entity shall notify the Secret Service or the Federal Bureau of Investigation 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 ENTITY.—

(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 manage a covered entity’s data, such third party shall notify the covered entity of the breach of security.

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

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

(2) SERVICE PROVIDERS.—A 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 contains or relates to a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transit storage to such data, such service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified.

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

(c) TIMELINESS OF NOTIFICATION.—

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

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

(A) LAW ENFORCEMENT.—If a law enforcement agency determines that the notification required under subsection (a) would impede a criminal investigation, such notification shall be delayed upon written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency determines that the notification required under subsection (a) would impede a criminal investigation, such notification shall be delayed upon 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.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

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

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

(ii) Telephone.

(iii) Email or other electronic means.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a security breach, such notification, to the extent practicable, shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the personal information that was accessed and acquired, or reasonably believed to have been accessed and acquired, by an unauthorized person as a part of the security breach; and

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

(I) the breach of security;

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

(III) steps taken to prevent further unauthorized access to such personal information;

(2) SUBSTITUTE NOTIFICATION.—

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

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

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

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

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

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

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

SEC. 803. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 801 and 802 apply to—

(1) those persons, partnerships, and corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and


(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARriers.—Sections 222, 338, and 611 of the Communications Act of 1934 (47 U.S.C. 222, 338, and 611), as amended, and to any telecommunication carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).
including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections.

(c) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 801 or 802 shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (a), this section shall confer upon the Federal Trade Commission the power to obtain such information as it may determine to be necessary in order to enforce the provisions of this section, to require such reports as it may determine to be necessary, and to institute proceedings in its own name to enjoin violations of any provision of this section.

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

(3) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection for all actions shall not exceed—

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

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

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title shall be construed to establish a private cause of action against a person for any 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 person, including a cooperative, corporation, trust, estate, partnership, association, or any other commercial entity that acquires, maintains, stores, or utilizes personal information.

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

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

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

(iii) 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.

(iv) 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 of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport 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, maintained, or released by the National Credit Information Bureau established pursuant to section 801 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 that 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 intended recipient of the data, and does not differentiate personal information from other information that such entity provides connections for in such a manner consistent with the content 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 has possession of such data, which is transmitted, routing, intermediate, and transient storage, or connections.

SEC. 805. EFFECT ON OTHER LAWS.

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 critical infrastructure of the United States; which was ordered to lie on the table; as follows:

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—

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

(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical information relating to critical electric infrastructure."
“(2) COORDINATION WITH CANADA AND MEXICO.—In exercising the authority granted under this subsection, the Secretary is encouraged to consult and coordinate with the appropriate officials of Canada and Mexico and other nations responsible for the protection of cyber security of the interconnected North American electricity grid.

“(3) COOPERATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with the appropriate officials of Canada and Mexico and other nations responsible for the protection of cyber security of the interconnected North American electricity grid.

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

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

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

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

“(e) JURISDICTION.—

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

“(2) COVERED ENTITIES.—

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

“(i) carrying out this section; and

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

“(B) R EQUIREMENTS.—The procedures and regulations prescribed under this section shall apply to entities described in subparagraph (A) to ensure the security and confidentiality of the information; and

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

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

“(f) ACCESS TO CLASSIFIED INFORMATION.—

“(1) AUTHORIZATION REQUIRED.—No person shall be authorized to access classified information (as defined in section 6.1 of Executive Order 13326 (50 U.S.C. 435 note; relating to classified national security information)) unless such person is determined to have a need-to-know (as defined in section 215(a) of the Federal Power Act (6 U.S.C. 824o(i))) and a statutory or relevant Implementing regulations authorizing access to such information.

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

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

“SEC. 804. LIMITATION.

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

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

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

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

“(d) LIMITATION.—The ERO shall have authority to develop and enforce compliance procedures and temporary emergency orders with respect to a facility used in the local distribution of electric energy only to the extent the Commission determines that the facility is so important to national security, national economic security, national public health or safety.”
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 and for cybersecurity through a consortium, or other appropriate entity, with participants from institutions of higher education and industry.

(b) Purposes.—The task force established under subsection (a) shall—

(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in the consortium;

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;

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

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

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

(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity.

d) REPORT.—Not later than 12 months after the convening of the task force established under section (a) of the report required under subsection (d).

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

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

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

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

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

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and standards and associated reference materials for the selection of options that minimize the security risks associated with each information technology hardware or software system and security tool that is widely used within the Federal Government in order to enable the development and interoperability of technologies, architectures, and frameworks for continuous information security within the Federal Government.

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

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

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

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

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

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

(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraphs (1) and (2) the development of standards, reference materials, and checklists under this subsection for an information technology system or tool if such Director determines that—

(A) the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the impracticality of developing a standard, reference material, or checklist for the system;

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

(6) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(7) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(8) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(9) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(10) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(11) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(12) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(13) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(14) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

(15) AGENCY USE REQUIREMENTS.—The Director, in collaboration with other relevant Federal agencies and stakeholders, shall require the use of standards, reference materials, and checklists under this subsection for Federal agency procurement or deployment of any such system.

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

"(f) INTRAMURAL CYBERSECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d), the Institute shall—

(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 information security and privacy policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

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

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

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

(c) NIST IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.—The Director shall continue a program to support the development of technical standards, protocols, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen and improve methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

(d) FEDERAL GOVERNMENT CLOUD COMPUTING STRATEGY.—

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

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

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

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

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

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

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

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

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

SA 2647. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the...
security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. 2. SPECTRUM EFFICIENCY AND SECURITY FUND.

(a) RETENTION OF UNSED FUNDS.—Section 118(d)(3) of the Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(3)) is amended by striking “8 years” and inserting “20 years”.

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

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

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

“(1) to pay relocation costs;

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

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

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

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

“(3) ELIGIBLE FEDERAL ENTITY; NATIONAL SCIENCE FOUNDATION.—In this section, the term ‘eligible Federal entity’ shall include the National Science Foundation. As an eligible Federal entity, the National Science Foundation may submit to the Director of OMB requests for funds under this section to support spectrum research and experimental facilities by the Foundation, provided that such requests are consistent with the determination of the Director of OMB, in consultation with the NTIA, the National Science Foundation shall be entitled to the first 5 years of the 15-year period designated in subsection (a) for the National Science Foundation to use such funds for the purposes of clause (1) and if the Director certifies that the National Science Foundation has used such funds to support spectrum research and experimental facilities.

(d) SPECTRUM EFFICIENCY AND SECURITY FUND.

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

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

(B) in subsection (a), by striking “Spectrum Re却ation Fund” and inserting “Spectrum Efficiency and Security Fund”;

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) COMMUNICATIONS ACT OF 1934.—Section 309(j)(b)(6) of the Communications Act of 1934 (47 U.S.C. 309(j)(b)(6)) is amended—

(i) in clause (1), by striking “Spectrum Re却ation Fund” and inserting “Spectrum Efficiency and Security Fund”;

(ii) in clause (2), by striking “Spectrum Efficiency and Security Fund” and inserting “Spectrum Efficiency and Security Fund”;

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

(1) in subsection (g)(3), in the first sentence, by striking “Spectrum Relocation Fund” and inserting “Spectrum Efficiency and Security Fund” and “Spectrum Relocation Fund” and inserting “Spectrum Efficiency and Security Fund”

SA 2648. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VII—MISCELLANEOUS

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

(a) REPORT REQUIRED.—

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

(A) identifies—

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

(ii) countries identified under clause (1) 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 as in this section referred to as ‘priority foreign countries’;

(iii) technologies developed by United States persons that—

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

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

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

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

(C) describes—

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

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

(2) DETERMINATION OF FOREIGN COUNTRIES ENGAGING IN ECONOMIC OR INDUSTRIAL ESPIONAGE IN CYBERSPACE.—For purposes of paragraphs (1) and (4), the term “economic or industrial espionage” means—

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

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

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

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

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

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

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appropriate congressional committee” means—

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

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

(2) CYBERSPACE.—The term “cyberspace” means—

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

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

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

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

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

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

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

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


(7) TRADE SECRET.—The term “trade secret” has the meaning given that term in section 3901 of title 18, United States Code.

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

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

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

SA 2649. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VII, add the following:

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

(a) PROCESS FOR REPORTING PENETRATIONS.—The Under Secretary of Defense for
Intelligence shall, in coordination with the officials specified in subsection (c), establish a process by which cleared defense contractors shall report to elements of the Department of Defense successful penetration by contractors of information systems that contain or process cleared defense contractors' networks or information systems.

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

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

(1) The Under Secretary of Defense for Policy.

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

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

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

(d) PROCEDURE REQUIREMENTS.—(1) RAPID REPORTING.—The process required by subsection (a) shall provide for rapid reporting by cleared defense contractors of a designated network or information system under the process shall include the following:

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

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

(2) ACCESS.—The process shall include mechanisms by which cleared defense contractors 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 under the process or stolen and, if so, what information was exfiltrated.

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

SA 2650. Mr. UDALL of Colorado submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

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

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

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

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

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

(b) THE CYBER TRAINING RANGE OPERATED BY THE UNITED STATES AIR FORCE ACADEMY PROVIDES REALISTIC CYBER TRAINING FOR CALIFORNIA’S ARMED FORCES THAT WILL BENEFIT THE ENTIRE UNITED STATES.

(c) THE CYBER TRAINING RANGE OPERATED BY THE UNITED STATES AIR FORCE ACADEMY PROVIDES REALISTIC CYBER TRAINING FOR CALIFORNIA’S ARMED FORCES THAT WILL BENEFIT THE ENTIRE UNITED STATES.

(d) THE CYBER TRAINING RANGE OPERATED BY THE UNITED STATES AIR FORCE ACADEMY PROVIDES REALISTIC CYBER TRAINING FOR CALIFORNIA’S ARMED FORCES THAT WILL BENEFIT THE ENTIRE UNITED STATES.

(e) THE CYBER TRAINING RANGE OPERATED BY THE UNITED STATES AIR FORCE ACADEMY PROVIDES REALISTIC CYBER TRAINING FOR CALIFORNIA’S ARMED FORCES THAT WILL BENEFIT THE ENTIRE UNITED STATES.

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

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

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

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

(A) An assessment whether the number of Extra High Voltage transformers currently held in reserve by utilities and public and private manufacturers is sufficient, and is secured in a manner adequate, to maintain national security operations in the event of a physical or network-based attack on the electric power infrastructure of the United States, Canada, or Mexico.

(B) An assessment that the risk associated with the lack of stockpiles of Extra High Voltage transformers stockpiled and securely stored for national security purposes.

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

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

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

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

(4) APPROPRIATE COMMITTEE OF CONGRESS DEFINED.—In this subsection, the term "appropriate committee of Congress" means the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and the Committee on Armed Services, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives.

SA 2652. Mr. UDALL of Colorado submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 132, strike lines 16 through 21 and insert the following:

(2) CONTENTS.—The strategy developed under paragraph (1) shall include—
(A) a 5-year plan on recruitment of personnel for the Federal workforce that includes—
   (i) a description of Federal programs for identifying, retaining, 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 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 cybersecurity and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—IRANIAN NUCLEAR PROGRAM

SEC. 801. IRANIAN NUCLEAR PROGRAM.

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

(1) At the end, add the following:

 TITLE VIII—IRANIAN NUCLEAR PROGRAM

SEC. 801. IRANIAN NUCLEAR PROGRAM.

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

(1) Since at least the late 1980s, the Government of the Islamic Republic of Iran has engaged in a sustained and well-documented pattern of 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’’;
   (B) states that “Iran has carried out activities relevant to the development of a nuclear device’’
   (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 111–195) states, “The United States and other responsible countries have a vital interest in working together to prevent the Government of Iran from acquiring a nuclear weapons capability.”

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

(9) On December 6, 2011, Prince Turki al-Faisal of Saudi Arabia stated that if international efforts to prevent Iran from obtaining nuclear weapons fail, “we must, as a matter of national security, look into all our options provided that we can be assured that these options will work and will work well’’.

(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 Government of Iran has designated as a state sponsor of terrorism since 1984 and characterized Iran as the “most active state sponsor of terrorism’’.

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

(13) On July 28, 2011, the Department of the Treasury stated 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, leaders of Iran’s Islamic Revolutionary Guard Corps (IRGC) Quds Force were implicated in a terrorist plot to assassinate Saudi Arabia’s Ambassador to the United States on United States soil.

(15) On December 26, 2011, the United Nations General Assembly passed a resolution denouncing the serious human rights abuses occurring in the Islamic Republic of Iran, including torture, cruel and degrading treatment,lynching 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, Japan, and Russia; the People’s Republic of China; and the United Kingdom) and representatives of the Islamic Republic of Iran held negotiations on Iran’s nuclear program in Isfahan, Iran on April 14, 2012, and these discussions are set to resume in Baghdad, Iraq on May 23, 2012.

(18) On March 31, 2010, President Obama stated that “Iran’s leaders should understand that I do not have a policy of containment; I have a policy of preventing Iran from obtaining a nuclear weapon, and I will take no options off the table to achieve that goal’’.

(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 of preventing Iran from obtaining a nuclear weapon, and I will take no options off the table to achieve that goal’’.

(21) Secretary of Defense Leon Panetta stated, in December 2011, that it was unacceptable for Iran to acquire nuclear weapons, and stated that all options were on the table to thwart Iran’s nuclear weapons efforts, and vowed that if the United States gets “intel-

ligence that they are proceeding with developing a nuclear weapon then we will take whatever steps necessary to stop it’’.

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

(23) On April 2, 2010, President Obama stated, “All the evidence indicates that the Iranians are trying to develop the capacity to develop nuclear weapons. They might decide that, once they have that capacity that they’d hold off right at the edge in order not to incur more sanctions. But, if they’ve got nuclear weapons-developed weapons, that 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’’.

(b) SENSE OF CONGRESS.—Congress—

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

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

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

   (A) the full and sustained suspension of all uranium enrichment-related and reprocessing activities by the Islamic Republic of Iran and its full cooperation with the IAEA on all outstanding issues related to its nuclear activities, particularly those concerning the possible military dimensions of its nuclear program;
   (B) a permanent agreement that verifiably assures that Iran’s nuclear program is entirely peaceful;
   (C) a permanent agreement that verifiably assures that Iran’s nuclear program is entirely peaceful;
   (D) a 5-year plan on recruitment of personnel for the Federal workforce that includes—
   (E) a description of Federal programs for identifying, retaining, and retaining individuals with outstanding computer skills for service in the Federal Government; and
   (F) 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;

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

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

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

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

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

(9) joins the President in ruling out any policy that would rely on efforts to contain a nuclear weapons-capable Iran as an option in response to the Iranian nuclear threat.

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

SA 2654. Mr. CRAPO (for himself and Mr. JOHANNS) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

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

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

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

(1) without regard to—

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

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

(2) through the promulgation of an interim final rule, where 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 145, strike lines 5 through 11 and insert the following:

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

SA 2657. Mr. McCaIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

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

SA 2658. Mr. McCaIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 121, strike lines 13 through 24.

SA 2659. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

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

SA 2660. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

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

SA 2661. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

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

SA 2662. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title I, add the following:

SEC. 111. SUNSET.

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

SA 2663. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title I, add the following:

SEC. 111. SUNSET.

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

SA 2664. Mr. McCain submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 122, strike lines 18 through 23, 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 Jarcha.

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 the way of

The legislative clerk read as follows:

A resolution (S. Res. 533) designating October 2012 as ‘‘National Work and Family Month’’ was agreed to.

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

The resolution was agreed to without further objection.