bill S. 754, supra; which was ordered to lie on the table.

SA 2629. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2630. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2631. Mr. GARDNER (for himself and Mr. CARDIN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2632. Mr. TESTER (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2633. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. Ayotte to the bill S. 754, supra; which was ordered to lie on the table.

SA 2634. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. Ayotte to the bill S. 754, supra; which was ordered to lie on the table.

SA 2635. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2636. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2637. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2638. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2639. Mr. WHITEHOUSE proposed an amendment to the bill S. 1523 , to amend the Federal Water Pollution Control Act to reauthorize the National Estuary Program, and for other purposes.

TEXT OF AMENDMENTS

SA 2616. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 11. EFFECTIVE PERIOD.

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall cease to have effect 4 years after the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

SA 2617. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 16, line 9, insert ''make reasonable efforts to'' before ''review''.

On page 16, line 11, strike ''knows'' and insert ''reasonably believes''.

On page 16, line 17, insert ''identify and'' before ''remove''.

On page 16, line 19, strike ''knows'' and insert ''reasonably believes''.

SA 2618. Mr. MENENDEZ submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—COMMERCIAL PRIVACY

SEC. 201. SHORT TITLE.

This title may be cited as the ''Commercial Privacy Bill of Rights Act of 2015''.

SEC. 202. FINDINGS.

Congress finds the following:

(1) Personal privacy is worthy of protection through appropriate legislation.

(2) Trust in the treatment of personally identifiable information collected on and off the Internet is essential for businesses to succeed.

(3) Persons interacting with others engaged in interstate commerce have a significant interest in their personal information, as well as a right to control how that information is collected, used, stored, or transferred.

(4) Persons engaged in interstate commerce and collecting personally identifiable information on individuals have a responsibility to treat that information with respect and in accordance with common standards.

(5) On the day before the date of the enactment of this Act, the laws of the Federal Government and State and local governments provided inadequate privacy protection for individuals engaging in and interacting with persons engaged in interstate commerce.

(6) As of the day before the date of the enactment of this Act, with the exception of Federal Trade Commission enforcement of laws against unfair and deceptive practices, the Federal Government has eschewed general commercial privacy laws in favor of industry self-regulation, which has led to several self-policing schemes, some of which are enforceable, and some of which provide insufficient privacy protection to individuals.

(7) As of the day before the date of the enactment of this Act, many collectors of personally identifiable information have yet to provide baseline fair information practice protections for individuals.

(8) The ease of gathering and compiling personal information on the Internet and off, both overtly and surreptitiously, is becoming increasingly efficient and effortless due to advances in technology which have provided information gatherers the ability to compile seamlessly highly detailed personal histories of individuals.

(9) Personal information requires greater privacy protection than is available on the day before the date of the enactment of this Act. Vast amounts of personal information, including sensitive information, about individuals are collected on and off the Internet, often combined and sold or otherwise transferred to third parties, for purposes unknown to an individual to whom the personally identifiable information pertains.

(10) Toward the close of the 20th Century, as individuals' personal information was increasingly collected, profiled, and shared for commercial purposes, and as technology advanced to facilitate these practices, Congress enacted numerous statutes to protect privacy.

(11) Those statutes apply to the government, telephones, cable television, e-mail, video tape rentals, and the Internet (but only with respect to children and law enforcement requests).

(12) As in those instances, the Federal Government has a substantial interest in creating a level playing field of protection across all collectors of personally identifiable information, both in the United States and abroad.

(13) Enhancing individual privacy protection in a balanced way that establishes clear, consistent rules, both domestically and internationally, will stimulate commerce by instilling greater consumer confidence at home and greater confidence abroad as more and more entities digitize personally identifiable information, whether collected, stored, or used online or offline.

SEC. 203. DEFINITIONS.

(a) IN GENERAL.—Subject to subsection (b), in this title:

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

(2) COVERED ENTITY.—The term ''covered entity'' means any person to whom this title applies under section 241.

(3) COVERED INFORMATION.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''covered information'' means only the following:

(i) Personally identifiable information.

(ii) Unique identifier information.

(iii) Any information that is collected, used, or stored in connection with personally identifiable information or unique identifier information in a manner that may reasonably be used by the party collecting the information to identify a specific individual.

(B) EXCEPTION.—The term ''covered information'' does not include the following:

(i) Personally identifiable information obtained from public records that is not merged with covered information gathered elsewhere.

(ii) Personally identifiable information that is obtained from a forum—

(I) where the individual voluntarily shared the information or authorized the information to be shared; and

(II) that—

(aa) is widely and publicly available and was not made publicly available in bad faith; and

(bb) contains no restrictions on who can access and view such information.

(iii) Personally identifiable information reported in public media.

(iv) Personally identifiable information dedicated to contacting an individual at the individual's place of work.

(4) ESTABLISHED BUSINESS RELATIONSHIP.—The term ''established business relationship'' means, with respect to a covered entity and a person, a relationship formed with or without the exchange of consideration, involving the establishment of an account by the person with the covered entity for the receipt of products or services offered by the covered entity.

(5) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means only the following:

(A) Any of the following information about an individual:

(i) The first name (or initial) and last name of an individual, whether given at birth or time of adoption, or resulting from a lawful change of name.

(ii) The postal address of a physical place of residence of such individual.

(iii) An e-mail address.

(iv) A telephone number or mobile device number.

(v) A social security number or other government issued identification number issued to such individual.

(vi) The account number of a credit card issued to such individual.

(vii) Unique identifier information that alone can be used to identify a specific individual.

(viii) Biometric data about such individual, including fingerprints and retina scans.

(B) If used, transferred, or stored in connection with 1 or more of the items of information described in subparagraph (A), any of the following:

(i) A date of birth.

(ii) The number of a certificate of birth or adoption.

(iii) A place of birth.

(iv) Unique identifier information that alone cannot be used to identify a specific individual.

(v) Precise geographic location, at the same degree of specificity as a global positioning system or equivalent system, and not including any general geographic information that may be derived from an Internet Protocol address.

(vi) Information about an individual's quantity, technical configuration, type, destination, location, and amount of uses of voice services, regardless of technology used.

(vii) Any other information concerning an individual that may reasonably be used by the party using, collecting, or storing that information to identify that individual.

(6) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means—

(A) personally identifiable information which, if lost, compromised, or disclosed without authorization either alone or with other information, carries a significant risk of economic or physical harm; or

(B) information related to—

(i) a particular medical condition or a health record; or

(ii) the religious affiliation of an individual.

(7) THIRD PARTY.—

(A) IN GENERAL.—The term ''third party'' means, with respect to a covered entity, a person that—

(i) is—

(I) not related to the covered entity by common ownership or corporate control; or

(II) related to the covered entity by common ownership or corporate control and an ordinary consumer would not understand that the covered entity and the person were related by common ownership or corporate control;

(ii) is not a service provider used by the covered entity to receive personally identifiable information or sensitive personally identifiable information in performing services or functions on behalf of and under the instruction of the covered entity; and

(iii) with respect to the collection of covered information of an individual, does not have an established business relationship with the individual and does not identify itself to the individual at the time of such collection in a clear and conspicuous manner that is visible to the individual.

(B) COMMON BRANDS.—The term ''third party'' may include, with respect to a covered entity, a person who operates under a common brand with the covered entity.

(8) UNAUTHORIZED USE.—

(A) IN GENERAL.—The term ''unauthorized use'' means the use of covered information by a covered entity or its service provider for any purpose not authorized by the individual to whom such information relates.

(B) EXCEPTIONS.—Except as provided in subparagraph (C), the term ''unauthorized use'' does not include use of covered information relating to an individual by a covered entity or its service provider as follows:

(i) To process and enforce a transaction or deliver a service requested by that individual.

(ii) To operate the covered entity that is providing a transaction or delivering a service requested by that individual, such as inventory management, financial reporting and accounting, planning, and product or service improvement or forecasting.

(iii) To prevent or detect fraud or to provide for a physically or virtually secure environment.

(iv) To investigate a possible crime.

(v) That is required by a provision of law or legal process.

(vi) To market or advertise to an individual from a covered entity within the context of a covered entity's own Internet website, services, or products if the covered information used for such marketing or advertising was—

(I) collected directly by the covered entity; or

(II) shared with the covered entity—

(aa) at the affirmative request of the individual; or

(bb) by an entity with which the individual has an established business relationship.

(vii) Use that is necessary for the improvement of transaction or service delivery through research, testing, analysis, and development.

(viii) Use that is necessary for internal operations, including the following:

(I) Collecting customer satisfaction surveys and conducting customer research to improve customer service information.

(II) Information collected by an Internet website about the visits to such website and the click-through rates at such website—

(aa) to improve website navigation and performance; or

(bb) to understand and improve the interaction of an individual with the advertising of a covered entity.

(ix) Use—

(I) by a covered entity with which an individual has an established business relationship;

(II) which the individual could have reasonably expected, at the time such relationship was established, was related to a service provided pursuant to such relationship; and

(III) which does not constitute a material change in use or practice from what could have reasonably been expected.

(C) SAVINGS.—A use of covered information regarding an individual by a covered entity or its service provider may only be excluded under subparagraph (B) from the definition of ''unauthorized use'' under subparagraph (A) if the use is reasonable and consistent with the practices and purposes described in the notice given the individual in accordance with section 121(a)(1).

(9) UNIQUE IDENTIFIER INFORMATION.—The term ''unique identifier information'' means a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number.

(b) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that a term defined in any of paragraphs (3) through (8) is not reasonably sufficient to protect an individual from unfair or deceptive acts or practices, the Commission may by rule modify such definition as the Commission considers appropriate to protect such individual from an unfair or deceptive act or practice to the extent that the Commission determines will not unreasonably impede interstate commerce.

Subtitle A—Right to Security and Accountability

SEC. 211. SECURITY.

(a) RULEMAKING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity to carry out security measures to protect the covered information it collects and maintains.

(b) PROPORTION.—The requirements prescribed under subsection (a) shall provide for security measures that are proportional to the size, type, nature, and sensitivity of the covered information a covered entity collects.

(c) CONSISTENCY.—The requirements prescribed under subsection (a) shall be consistent with guidance provided by the Commission and recognized industry practices for safety and security on the day before the date of the enactment of this Act.

(d) TECHNOLOGICAL MEANS.—In a rule prescribed under subsection (a), the Commission may not require a specific technological means of meeting a requirement.

SEC. 212. ACCOUNTABILITY.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information it collects—

(1) have managerial accountability, proportional to the size and structure of the covered entity, for the adoption and implementation of policies consistent with this title;

(2) have a process to respond to non-frivolous inquiries from individuals regarding the collection, use, transfer, or storage of covered information relating to such individuals; and

(3) describe the means of compliance of the covered entity with the requirements of this Act upon request from—

(A) the Commission; or

(B) an appropriate safe harbor program established under section 241.

SEC. 213. PRIVACY BY DESIGN.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by—

(1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on—

(A) the reasonable expectations of such individuals regarding privacy; and

(B) the relevant threats that need to be guarded against in meeting those expectations; and

(2) maintaining appropriate management processes and practices throughout the data life cycle that are designed to ensure that information systems comply with—

(A) the provisions of this title;

(B) the privacy policies of a covered entity; and

(C) the privacy preferences of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 222.

Subtitle B—Right to Notice and Individual Participation

SEC. 221. TRANSPARENT NOTICE OF PRACTICES AND PURPOSES.

(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity—

(1) to provide accurate, clear, concise, and timely notice to individuals of—

(A) the practices of the covered entity regarding the collection, use, transfer, and storage of covered information; and

(B) the specific purposes of those practices;

(2) to provide accurate, clear, concise, and timely notice to individuals before implementing a material change in such practices; and

(3) to maintain the notice required by paragraph (1) in a form that individuals can readily access.

(b) COMPLIANCE AND OTHER CONSIDERATIONS.—In the rulemaking required by subsection (a), the Commission—

(1) shall consider the types of devices and methods individuals will use to access the required notice;

(2) may provide that a covered entity unable to provide the required notice when information is collected may comply with the requirement of subsection (a)(1) by providing an alternative time and means for an individual to receive the required notice promptly;

(3) may draft guidance for covered entities to use in designing their own notice and may include a draft model template for covered entities to use in designing their own notice; and

(4) may provide guidance on how to construct computer-readable notices or how to use other technology to deliver the required notice.

SEC. 222. INDIVIDUAL PARTICIPATION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity—

(1) to offer individuals a clear and conspicuous mechanism for opt-in consent for any use of their covered information that would otherwise be unauthorized use;

(2) to offer individuals a robust, clear, and conspicuous mechanism for opt-in consent for the use by third parties of the individuals' covered information for behavioral advertising or marketing;

(3) to provide any individual to whom the personally identifiable information that is covered information pertains, and which the covered entity or its service provider stores, appropriate and reasonable—

(A) access to such information; and

(B) mechanisms to correct such information to improve the accuracy of such information; and

(4) in the case that a covered entity enters bankruptcy or an individual requests the termination of a service provided by the covered entity to the individual or termination of some other relationship with the covered entity, to permit the individual to easily request that—

(A) all of the personally identifiable information that is covered information that the covered entity maintains relating to the individual, except for information the individual authorized the sharing of or which the individual shared with the covered entity in a forum that is widely and publicly available, be rendered not personally identifiable; or

(B) if rendering such information not personally identifiable is not possible, to cease the unauthorized use or transfer to a third party for an unauthorized use of such information or to cease use of such information for marketing, unless such unauthorized use or transfer is otherwise required by a provision of law.

(b) UNAUTHORIZED USE TRANSFERS.—In the rulemaking required by subsection (a), the Commission shall provide that with respect to transfers of covered information to a third party for which an individual provides opt-in consent, the third party to which the information is transferred may not use such information for any unauthorized use other than a use—

(1) specified pursuant to the purposes stated in the required notice under section 221(a); and

(2) authorized by the individual when the individual granted consent for the transfer of the information to the third party.

(c) ALTERNATIVE MEANS TO TERMINATE USE OF COVERED INFORMATION.—In the rulemaking required by subsection (a), the Commission shall allow a covered entity to provide individuals an alternative means, in lieu of the access, consent, and correction requirements, of prohibiting a covered entity from use or transfer of that individual's covered information.

(d) SERVICE PROVIDERS.—

(1) IN GENERAL.—The use of a service provider by a covered entity to receive covered information in performing services or functions on behalf of and under the instruction of the covered entity does not constitute an unauthorized use of such information by the covered entity if the covered entity and the service provider execute a contract that requires the service provider to collect, use, and store the information on behalf of the covered entity in a manner consistent with—

(A) the requirements of this title; and

(B) the policies and practices related to such information of the covered entity.

(2) TRANSFERS BETWEEN SERVICE PROVIDERS FOR A COVERED ENTITY.—The disclosure by a service provider of covered information pursuant to a contract with a covered entity to another service provider in order to perform the same service or functions for that covered entity does not constitute an unauthorized use.

(3) LIABILITY REMAINS WITH COVERED ENTITY.—A covered entity remains responsible and liable for the protection of covered information that has been transferred to a service provider for processing, notwithstanding any agreement to the contrary between a covered entity and the service provider.

Subtitle C—Rights Relating to Data Minimization, Constraints on Distribution, and Data Integrity

SEC. 231. DATA MINIMIZATION.

Each covered entity shall—

(1) collect only as much covered information relating to an individual as is reasonably necessary—

(A) to process or enforce a transaction or deliver a service requested by such individual;

(B) for the covered entity to provide a transaction or delivering a service requested by such individual, such as inventory management, financial reporting and accounting, planning, product or service improvement or forecasting, and customer support and service;

(C) to prevent or detect fraud or to provide for a secure environment;

(D) to investigate a possible crime;

(E) to comply with a provision of law;

(F) for the covered entity to market or advertise to such individual if the covered information used for such marketing or advertising was collected directly by the covered entity; or

(G) for internal operations, including—

(i) collecting customer satisfaction surveys and conducting customer research to improve customer service; and

(ii) collection from an Internet website of information about visits and click-through rates relating to such website to improve—

(I) website navigation and performance; and

(II) the customer's experience;

(2) retain covered information for only such duration as—

(A) with respect to the provision of a transaction or delivery of a service to an individual—

(i) is necessary to provide such transaction or deliver such service to such individual; or

(ii) if such service is ongoing, is reasonable for the ongoing nature of the service; or

(B) is required by a provision of law;

(3) retain covered information only for the purpose it was collected, or reasonably-related purposes; and

(4) exercise reasonable data retention procedures with respect to both the initial collection and subsequent retention.

SEC. 232. CONSTRAINTS ON DISTRIBUTION OF INFORMATION.

(a) IN GENERAL.—Each covered entity shall—

(1) require by contract that any third party to which it transfers covered information use the information only for purposes that are consistent with—

(A) the provisions of this title; and

(B) as specified in the contract;

(2) require by contract that such third party may not combine information that the covered entity has transferred to it, that relates to an individual, and that is not personally identifiable information with other information in order to identify such individual, unless the covered entity has obtained the opt-in consent of such individual for such combination and identification; and

(3) before executing a contract with a third party—

(A) assure through due diligence that the third party is a legitimate organization; and

(B) in the case of a material violation of the contract, at a minimum notify the Commission of such violation.

(b) TRANSFERS TO UNRELIABLE THIRD PARTIES PROHIBITED.—A covered entity may not transfer covered information to a third party that the covered entity knows—

(1) has intentionally or willfully violated a contract required by subsection (a); and

(2) is reasonably likely to violate such contract.

(c) APPLICATION OF RULES TO THIRD PARTIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), a third party that receives covered information from a covered entity shall be subject to the provisions of this Act as if it were a covered entity.

(2) EXEMPTION.—The Commission may, as it determines appropriate, exempt classes of third parties from liability under any provision of subtitle B if the Commission finds that—

(A) such class of third parties cannot reasonably comply with such provision; or

(B) with respect to covered information relating to individuals that is transferred to such class, compliance by such class with such provision would not sufficiently benefit such individuals.

SEC. 233. DATA INTEGRITY.

(a) IN GENERAL.—Each covered entity shall attempt to establish and maintain reasonable procedures to ensure that personally identifiable information that is covered information and maintained by the covered entity is accurate in those instances where the covered information could be used to deny consumers benefits or cause significant harm.

(b) EXCEPTION.—Subsection (a) shall not apply to covered information of an individual maintained by a covered entity that is provided—

(1) directly to the covered entity by the individual;

(2) to the covered entity by another entity at the request of the individual;

(3) to prevent or detect fraud; or

(4) to provide for a secure environment.

Subtitle D—Enforcement

SEC. 241. GENERAL APPLICATION.

The requirements of this title shall apply to any person who—

(1) collects, uses, transfers, or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period; and

(2) is—

(A) a person 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));

(B) a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.), notwithstanding the definition of the term ''Acts to regulate commerce'' in section 4 of the Federal Trade Commission Act (15 U.S.C. 44) and the exception provided by section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)) for such carriers; or

(C) a nonprofit organization, including any organization described in section 501(c) of the Internal Revenue code of 1986 that is exempt from taxation under section 501(a) of such Code, notwithstanding the definition of the term ''Acts to regulate commerce'' in section 4 of the Federal Trade Commission Act (15 U.S.C. 44) and the exception provided by section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)) for such organizations.

SEC. 242. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A reckless or repetitive violation of a provision of this title shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(b) POWERS OF COMMISSION.—

(1) IN GENERAL.—Except as provided in paragraph (3), the Commission shall enforce this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title.

(2) PRIVILEGES AND IMMUNITIES.—Except as provided in paragraph (3), any person who violates a provision of this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(3) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—The Commission shall enforce this title with respect to common carriers and nonprofit organizations described in section 241 to the extent necessary to effectuate the purposes of this title as if such carriers and nonprofit organizations were persons 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)).

(c) RULEMAKING AUTHORITY.—

(1) LIMITATION.—In promulgating rules under this title, the Commission may not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(2) ADMINISTRATIVE PROCEDURE.—The Commission shall promulgate regulations under this title in accordance with section 553 of title 5, United States Code.

(d) RULE OF CONSTRUCTION.—Nothing in this title shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 243. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by a covered entity who violates any part of this title in a manner that results in economic or physical harm to an individual or engages in a pattern or practice that violates any part of this title, the attorney general may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States—

(1) to enjoin further violation of this title or a regulation promulgated under this title by the defendant;

(2) to compel compliance with this title or a regulation promulgated under this title; or

(3) for violations of this title or a regulation promulgated under this title to obtain civil penalties in the amount determined under section title.

(b) RIGHTS OF FEDERAL TRADE COMMISSION.—

(1) NOTICE TO FEDERAL TRADE COMMISSION.—

(A) IN GENERAL.—Except as provided in subparagraph (C), the attorney general of a State shall notify the Commission in writing of any civil action under subsection (b), prior to initiating such civil action.

(B) CONTENTS.—The notice required by subparagraph (A) shall include a copy of the complaint to be filed to initiate such civil action.

(C) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notice required by subparagraph (A), the State shall provide notice immediately upon instituting a civil action under subsection (b).

(2) INTERVENTION BY FEDERAL TRADE COMMISSION.—Upon receiving notice required by paragraph (1) with respect to a civil action, the Commission may—

(A) intervene in such action; and

(B) upon intervening—

(i) be heard on all matters arising in such civil action; and

(ii) file petitions for appeal of a decision in such action.

(c) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION.—If the Commission institutes a civil action for violation of this title or a regulation promulgated under this title, no attorney general of a State may bring a civil action under subsection (a) against any defendant named in the complaint of the Commission for violation of this title or a regulation promulgated under this title that is alleged in such complaint.

(d) INVESTIGATORY POWERS.—Nothing in this section may be construed to prevent the attorney general of a State from exercising the powers conferred on such attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) ACTIONS BY OTHER STATE OFFICIALS.—

(1) IN GENERAL.—In addition to civil actions brought by attorneys general under subsection (a), any other officer of a State who is authorized by the State to do so may bring a civil action under subsection (a), subject to the same requirements and limitations that apply under this section to civil actions brought by attorneys general.

(2) SAVINGS PROVISION.—Nothing in this section may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

SEC. 244. CIVIL PENALTIES.

(a) IN GENERAL.—In an action brought under section 243, in addition to any other penalty otherwise applicable to a violation of this title or any regulation promulgated under this title, the following civil penalties shall apply:

(1) SUBTITLE A VIOLATIONS.—A covered entity that recklessly or repeatedly violates subtitle A is liable for a civil penalty equal to the amount calculated by multiplying the number of days that the entity is not in compliance with such subtitle by an amount not to exceed $33,000.

(2) SUBTITLE B VIOLATIONS.—A covered entity that recklessly or repeatedly violates subtitle B is liable for a civil penalty equal to the amount calculated by multiplying the number of days that such an entity is not in compliance with such subtitle, or the number of individuals for whom the entity failed to obtain consent as required by such subtitle, whichever is greater, by an amount not to exceed $33,000.

(b) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index for All Urban Consumers is first published by the Bureau of Labor Statistics that is after 1 year after the date of the enactment of this Act, and each year thereafter, each of the amounts specified in subsection (a) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(c) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under section 243, the maximum civil penalty for which any covered entity may be liable under this section in such actions shall not exceed—

(1) $6,000,000 for any related series of violations of any rule promulgated under subtitle A; and

(2) $6,000,000 for any related series of violations of subtitle B.

SEC. 245. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—The provisions of this title shall supersede any provisions of the law of any State relating to those entities covered by the regulations issued pursuant to this title, to the extent that such provisions relate to the collection, use, or disclosure of—

(1) covered information addressed in this title; or

(2) personally identifiable information or personal identification information addressed in provisions of the law of a State.

(b) UNAUTHORIZED CIVIL ACTIONS; CERTAIN STATE LAWS.—

(1) UNAUTHORIZED ACTIONS.—No person other than a person specified in section 243 may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating this title or a regulation promulgated under this title.

(2) PROTECTION OF CERTAIN STATE LAWS.—This title shall not be construed to preempt the applicability of—

(A) State laws that address the collection, use, or disclosure of health information or financial information; or

(B) other State laws to the extent that those laws relate to acts of fraud.

(c) RULE OF CONSTRUCTION RELATING TO REQUIRED DISCLOSURES TO GOVERNMENT ENTITIES.—This title shall not be construed to expand or limit the duty or authority of a covered entity or third party to disclose personally identifiable information to a government entity under any provision of law.

SEC. 246. NO PRIVATE RIGHT OF ACTION.

This title may not be construed to provide any private right of action.

Subtitle E—Co-regulatory Safe Harbor Programs

SEC. 251. ESTABLISHMENT OF SAFE HARBOR PROGRAMS.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to establish requirements for the establishment and administration of safe harbor programs under which a nongovernmental organization will administer a program that—

(1) establishes a mechanism for participants to implement the requirements of this title with regards to—

(A) certain types of unauthorized uses of covered information as described in paragraph (2); or

(B) any unauthorized use of covered information; and

(2) offers consumers a clear, conspicuous, persistent, and effective means of opting out of the transfer of covered information by a covered entity participating in the safe harbor program to a third party for—

(A) behavioral advertising purposes;

(B) location-based advertising purposes;

(C) other specific types of unauthorized use; or

(D) any unauthorized use.

(b) SELECTION OF NONGOVERNMENTAL ORGANIZATIONS TO ADMINISTER PROGRAM.—

(1) SUBMITTAL OF APPLICATIONS.—An applicant seeking to administer a program under the requirements established pursuant to subsection (a) shall submit to the Commission an application therefor at such time, in such manner, and containing such information as the Commission may require.

(2) NOTICE AND RECEIPT OF APPLICATIONS.—Upon completion of the rulemaking proceedings required by subsection (a), the Commission shall—

(A) publish a notice in the Federal Register that it will receive applications for approval of safe harbor programs under this subtitle; and

(B) begin receiving applications under paragraph (1).

(3) SELECTION.—Not later than 270 days after the date on which the Commission receives a completed application under this subsection, the Commission shall grant or deny the application on the basis of the Commission's evaluation of the applicant's capacity to provide protection of individuals' covered information with regard to specific types of unauthorized uses of covered information as described in subsection (a)(2) that is substantially equivalent to or superior to the protection otherwise provided under this title.

(4) WRITTEN FINDINGS.—Any decision reached by the Commission under this subsection shall be accompanied by written findings setting forth the basis for and reasons supporting such decision.

(c) SCOPE OF SAFE HARBOR PROTECTION.—The scope of protection offered by safe harbor programs approved by the Commission that establish mechanisms for participants to implement the requirements of the title only for certain uses of covered information as described in subsection (a)(2) shall be limited to participating entities' use of those particular types of covered information.

(d) SUPERVISION BY FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—The Commission shall exercise oversight and supervisory authority of a safe harbor program approved under this section through—

(A) ongoing review of the practices of the nongovernmental organization administering the program;

(B) the imposition of civil penalties on the nongovernmental organization if it is not compliant with the requirements established under subsection (a); and

(C) withdrawal of authorization to administer the safe harbor program under this subtitle.

(2) ANNUAL REPORTS BY NONGOVERNMENTAL ORGANIZATIONS.—Each year, each nongovernmental organization administering a safe harbor program under this section shall submit to the Commission a report on its activities under this subtitle during the preceding year.

SEC. 252. PARTICIPATION IN SAFE HARBOR PROGRAM.

(a) EXEMPTION.—Any covered entity that participates in, and demonstrates compliance with, a safe harbor program administered under section 251 shall be exempt from any provision of subtitle B or subtitle C if the Commission finds that the requirements of the safe harbor program are substantially the same as or more protective of privacy of individuals than the requirements of the provision from which the exemption is granted.

(b) LIMITATION.—Nothing in this subtitle shall be construed to exempt any covered entity participating in a safe harbor program from compliance with any other requirement of the regulations promulgated under this title for which the safe harbor does not provide an exception.

Subtitle F—Application With Other Federal Laws

SEC. 261. APPLICATION WITH OTHER FEDERAL LAWS.

(a) QUALIFIED EXEMPTION FOR PERSONS SUBJECT TO OTHER FEDERAL PRIVACY LAWS.—If a person is subject to a provision of this title and a provision of a Federal privacy law described in subsection (d), such provision of this title shall not apply to such person to the extent that such provision of Federal privacy law applies to such person.

(b) PROTECTION OF OTHER FEDERAL PRIVACY LAWS.—Nothing in this title may be construed to modify, limit, or supersede the operation of the Federal privacy laws described in subsection (d) or the provision of information permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(c) COMMUNICATIONS INFRASTRUCTURE AND PRIVACY.—If a person is subject to a provision of section 222 or 631 of the Communications Act of 1934 (47 U.S.C. 222 and 551) and a provision of this title, such provision of such section 222 or 631 shall not apply to such person to the extent that such provision of this title applies to such person.

(d) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—The Federal privacy laws described in this subsection are as follows:

(1) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974).

(2) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.).

(3) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(4) The Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.).

(5) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(6) Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 et seq.).

(7) Chapters 119, 123, and 206 of title 18, United States Code.

(8) Section 2710 of title 18, United States Code.

(9) Section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly referred to as the ''Family Educational Rights and Privacy Act of 1974'').

(10) Section 445 of the General Education Provisions Act (20 U.S.C. 1232h).

(11) The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et seq.).

(12) The regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), as such regulations relate to a person described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d–1(a)) or to transactions referred to in section 1173(a)(1) of such Act (42 U.S.C. 1320d–2(a)(1)).

(13) The Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(14) Section 227 of the Communications Act of 1934 (47 U.S.C. 227).

Subtitle G—Development of Commercial Data Privacy Policy in the Department of Commerce

SEC. 271. DIRECTION TO DEVELOP COMMERCIAL DATA PRIVACY POLICY.

The Secretary of Commerce shall contribute to the development of commercial data privacy policy by—

(1) convening private sector stakeholders, including members of industry, civil society groups, academia, in open forums, to develop codes of conduct in support of applications for safe harbor programs under subtitle E;

(2) expanding interoperability between the United States commercial data privacy framework and other national and regional privacy frameworks;

(3) conducting research related to improving privacy protection under this title; and

(4) conducting research related to improving data sharing practices, including the use of anonymised data, and growing the information economy.

SA 2619. Mr. MCCAIN (for himself and Mr. FLAKE) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REVIEW AND NOTIFICATIONS OF CATEGORICAL EXCLUSIONS GRANTED FOR NEXT GENERATION FLIGHT PROCEDURES.

Section 213(c) of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 40101 note) is amended by adding at the end the following:

''(3) NOTIFICATIONS AND CONSULTATIONS.—Not less than 30 days before granting a categorical exclusion under this subsection for a new procedure, the Administrator shall notify and consult with the affected public and the operator of the airport at which the procedure would be implemented.

''(4) REVIEW OF CERTAIN CATEGORICAL EXCLUSIONS.—

''(A) IN GENERAL.—The Administrator shall review a decision of the Administrator made on or after February 14, 2012, and before the date of the enactment of this paragraph to grant a categorical exclusion under this subsection with respect to a procedure to be implemented at an airport to determine if the implementation of the procedure had a significant effect on the human environment in the community in which the airport is located if the operator of that airport requests such a review and demonstrates that there is good cause to believe that the implementation of the procedure had such an effect.

''(B) CONTENT OF REVIEW.—If, in conducting a review under subparagraph (A) with respect to a procedure implemented at an airport, the Administrator, in consultation with the operator of the airport, determines that implementing the procedure had a significant effect on the human environment in

the community in which the airport is located, the Administrator shall—

''(i) consult with the operator of the airport to identify measures to mitigate the effect of the procedure on the human environment; and

''(ii) in conducting such consultations, consider the use of alternative flight paths.''.

SA 2620. Mr. WHITEHOUSE (for himself and Mr. BLUNT) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—CYBERSECURITY PUBLIC AWARENESS ACT

SEC. 201. SHORT TITLE.

This title may be cited as the ''Cybersecurity Public Awareness Act of 2015''.

SEC. 202. ENFORCEMENT OF CYBERSECURITY LAWS.

(a) PROSECUTION FOR CYBERCRIME.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General, in consultation with the Director of the United States Secret Service, the Director of U.S. Immigration and Customs Enforcement, and the Director of the Federal Bureau of Investigation, shall submit to Congress a report—

(A) describing investigations and prosecutions relating to cyber intrusions, computer or network compromise, or other forms of illegal hacking the preceding year, including—

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

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

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

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

(I) the number of defendants prosecuted;

(II) whether the prosecutions resulted in a conviction; and

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

(B) identifying the number of employees, financial resources, and other resources (such as technology and training) devoted to the enforcement, investigation, and prosecution of cyber intrusions, computer or network compromised, or other forms of illegal hacking, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting cyber intrusions, computer or network compromise, or other forms of illegal hacking; and

(C) discussing any impediments under the laws of the United States or international law to prosecutions for cyber intrusions, computer or network compromise, or other forms of illegal hacking, including discussion of ways to improve the mutual legal assistance process used to obtain evidence abroad and to provide domestic evidence to foreign requestors.

(2) UPDATES.—The Attorney General, in consultation with the Director of the United States Secret Service, the Director of Immigration and Customs Enforcement, and the Director of the Federal Bureau of Investigation, shall annually submit to Congress a report updating the report submitted under paragraph (1) at the same time the Attorney General submits annual reports under section 404 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (42 U.S.C. 3713d).

(b) PREPAREDNESS OF FEDERAL COURTS TO PROMOTE CYBERSECURITY.—Not later than 180 days after the date of enactment of this Act, the Attorney General, in coordination with the Administrative Office of the United States Courts, shall submit to Congress a report—

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

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

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

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

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

(D) Federal civil and criminal laws.

SEC. 203. CYBERSECURITY PUBLIC AWARENESS CAMPAIGNS.

(a) EVALUATION OF EXISTING CYBERSECURITY PUBLIC AWARENESS CAMPAIGNS.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report examining—

(1) the number of cybersecurity public awareness campaigns run by Federal agencies;

(2) the estimated costs of Federal cybersecurity public awareness campaigns; and

(3) the effectiveness of Federal cybersecurity public awareness campaigns.

(b) RECOMMENDATIONS FOR IMPROVING CYBERSECURITY PUBLIC AWARENESS CAMPAIGNS.—The report required under subsection (a) shall include recommendations for improving and, if appropriate, consolidating Federal cybersecurity public awareness campaigns.

SEC. 204. DEVELOPING TECHNOLOGIES TO ENHANCE CRITICAL INFRASTRUCTURE CYBERSECURITY.

(a) DEFINITION.—In this section, the term ''critical infrastructure sector'' has the meaning given the term in section 203.

(b) REPORTS.—

(1) IN GENERAL.—The Secretary of Homeland Security shall enter into a contract with the National Research Council, or another Federally funded research and development corporation, under which the Council or corporation shall submit to Congress a report on opportunities to develop innovative or experimental technologies or technological approaches that would enhance the cybersecurity of the critical infrastructure sector.

(2) LIMITATIONS.—The report required under paragraph (1) shall—

(A) consider only technologies or technological options that can be deployed consistent with constitutional and statutory privacy rights; and

(B) identify any technologies or technological options described in subparagraph (A) that merit Federal research support.

(3) TIMING.—The contract entered into under paragraph (1) shall require that the report described in paragraph (1) be submitted not later than 1 year after the date of enactment of this Act. The Secretary of Homeland Security may enter into additional subsequent contracts as appropriate.

SA 2621. Mr. WYDEN (for himself, Mr. UDALL, Mr. BROWN, Mr. FRANKEN, Mr. MARKEY, Mr. BLUMENTHAL, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 16, strike lines 9 through 21 and insert the following:

(A) review such cyber threat indicator and remove, to the extent feasible, any personal information of or identifying a specific individual that is not necessary to describe or identity a cybersecurity threat; or

(B) implement and utilize a technical capability configured to remove, to the extent feasible, any personal information of or identifying a specific individual contained within such indicator that is not necessary to describe or identify a cybersecurity threat.

SA 2622. Mr. WYDEN (for himself, Mr. UDALL, Mr. BROWN, Mr. FRANKEN, Mr. MARKEY, Mr. BLUMENTHAL, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 12, between lines 7 and 8, insert the following:

(F) include procedures for notifying in a timely manner any person whose personal information is known or determined to have been shared or disclosed in contravention of this Act.

SA 2623. Ms. COLLINS (for herself, Ms. HIRONO, Mr. WARNER, and Mr. COATS) submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REPORTING ON INTRUSIONS OF INFORMATION SYSTEMS ESSENTIAL TO OPERATION OF CRITICAL INFRASTRUCTURE AT GREATEST RISK.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE AGENCY.—The term ''appropriate agency'' means, with respect to a covered entity—

(A) except as provided in subparagraph (B), the applicable sector-specific agency; or

(B) in the case of a covered entity that is regulated by a Federal entity, such Federal entity.

(2) APPROPRIATE AGENCY HEAD.—The term ''appropriate agency head'' means, with respect to a covered entity, the head of the appropriate agency.

(3) COVERED ENTITY.—The term ''covered entity'' means an entity that owns or controls critical cyber infrastructure.

(4) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' means a system or asset, whether physical or virtual, that is so vital to the United States that the incapacity or destruction of such system or asset would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(5) CRITICAL CYBER INFRASTRUCTURE.—The term ''critical cyber infrastructure'' means critical infrastructure identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742; relating to

identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security), or any successor order.

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

(7) SECTOR-SPECIFIC AGENCY.—The term ''sector specific agency'' has the meaning given such term in Presidential Policy Directive–21, issued February 12, 2013, or any successor directive.

(b) REPORTING REQUIRED.—

(1) IN GENERAL.—Notwithstanding subsections (f) and (h) of section 8, if an information system of a covered entity that is essential to the operation of critical cyber infrastructure is successfully intruded upon, such covered entity shall submit to the Secretary or the appropriate agency head a report on such intrusion as soon as practicable after the covered entity discovers such intrusion.

(2) ELEMENTS.—Each report submitted by a covered entity under paragraph (1) with respect to an intrusion shall include the following:

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

(B) A sample of the malicious software, if discovered and isolated by the covered entity, involved in such intrusion.

(C) Damage assessment.

(D) Such other matters as the Secretary or the appropriate agency head, as the case may be, consider appropriate.

(3) CONSISTENCY.—Reports submitted under paragraph (1) shall be submitted in a manner that is consistent with the other requirements of this Act.

(c) PROTECTION FROM LIABILITY.—A submittal of a report under subsection (b)(1) shall be treated as a sharing of a cyber threat indicator or defensive measure under section 4(c) for purposes of section 6.

(d) POLICIES AND PROCEDURES.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall, in consultation with the appropriate agency heads of covered entities, promulgate policies and procedures to carry out this section.

(2) ELEMENTS.—The policies and procedures promulgated under paragraph (1) shall include the following:

(A) Policies and procedures for submitting reports under subsection (b).

(B) Policies and procedures for making cyber threat indicators available under subsection (e).

(C) Policies and procedures for taking action under subsection (f).

(3) EXISTING PROCESSES, ROLES, AND RESPONSIBILITIES.—The Secretary shall ensure that the policies and procedures promulgated pursuant to paragraph (1) incorporate, to the greatest extent practicable, processes, roles, and responsibilities of appropriate agencies and entities, including sector specific information sharing and analysis centers, that were in effect on the day before the date of the enactment of this Act.

(e) TWO-WAY SHARING.—In a case in which the Secretary or an appropriate agency head receives a report under subsection (b) from a covered entity, the Secretary or appropriate agency head, as the case may be, shall, pursuant to section 3 and to the greatest extent practicable, make available to such covered entity such cyber threat indicators as the Secretary or appropriate agency head considers appropriate.

(f) PROTECTION FROM IDENTIFICATION.—In a case in which the Secretary or an appropriate agency head shares with a non-Federal entity information from or information derived from a report submitted by a covered entity under this section, the Secretary or the appropriate agency head (as the case may be) shall take such actions as the Secretary or the appropriate agency head (as the case may be) considers appropriate to protect from disclosure the identity of the covered entity.

(g) EFFECTIVE DATE.—The requirements of subsection (b) shall take effect on the date on which the Secretary first promulgates policies and procedures under subsection (d)(1) and shall apply with respect to intrusions of critical cyber infrastructure occurring on or after such date.

SA 2624. Mr. MENENDEZ submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 15, lines 4 and 5, strike ''paragraph (2)'' and insert ''paragraphs (2) and (3)''.

On page 15, between lines 16 and 17, insert the following:

(3) COMPLIANCE WITH CYBERSECURITY CROSS-AGENCY PRIORITY GOAL.—

(A) DEFINITIONS.—In this paragraph—

(i) the term ''appropriate committees of Congress'' means—

(I) the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(II) the Committee on the Judiciary, the Committee on Homeland Security, the Permanent Select Committee on Intelligence, and the Committee on Oversight and Government Reform of the House of Representatives; and

(ii) the term ''independent auditor'' means—

(I) for each Federal entity with an Inspector General appointed under the Inspector General Act of 1978, the Inspector General or an independent external auditor, as determined by the Inspector General of the Federal entity; and

(II) for each Federal entity not described in subclause (I), an independent external auditor as determined by the head of the Federal entity.

(B) REQUIREMENTS.—A Federal entity may not receive defensive measures under this Act unless the independent auditor for the Federal entity certifies that the Federal entity—

(i) is capable of properly using any defensive measures received; and

(ii) meets any additional metrics, as determined by Secretary of Homeland Security.

(C) RULES.—Not later than 120 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget, shall promulgate rules for updating the certification of the compliance of a Federal entity with the Cybersecurity Cross-Agency Priority Goal for purposes of receiving defensive measures.

(D) REPORT TO CONGRESS.—

(i) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the independent auditor for each Federal entity, in consultation with the Secretary of Homeland Security, shall submit to the appropriate committees of Congress and the head of the Federal entity a report detailing whether the Federal entity is capable of—

(I) adequately protecting the information shared or received under this Act;

(II) determining the original source of a cybersecurity threat; and

(III) determining whether a cybersecurity threat originates from a foreign entity.

(ii) FORM.—Each report required under clause (i) shall be submitted in writing and in unclassified form, but may include a classified annex.

On page 15, line 17, strike ''(3)'' and insert ''(4)''

SA 2625. Mr. JOHNSON (for himself, Mr. CARPER, Ms. AYOTTE, Mrs. MCCASKILL, Ms. COLLINS, and Mr. WARNER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT ACT

SECTION 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

SEC. 202. DEFINITIONS.

In this title—

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

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);

(3) the term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(7) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

''SEC. 228. CYBERSECURITY PLANS.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227;

''(3) the term 'information sharing and analysis organization' has the meaning given the term in section 212(5); and

''(4) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

''SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

''(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

''(3) the term 'agency information system' has the meaning given the term in section 228; and

''(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

''(b) REQUIREMENT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

''(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and

''(7) shall ensure that—

''(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

''(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

''(d) PRIVATE ENTITIES.—

''(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

''(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.''.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

''Sec. 226. Cybersecurity recruitment and retention.
''Sec. 227. National cybersecurity and communications integration center.
''Sec. 228. Cybersecurity plans.
''Sec. 229. Clearances.
''Sec. 230. Federal intrusion detection and prevention system.''.

SEC. 204. ADVANCED INTERNAL DEFENSES.

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting '', operating, and maintaining'' after ''deploying''.

SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to—

(A) the Department of Defense or an element of the intelligence community; or

(B) an agency information system for which—

(i) the head of the agency has personally certified to the Director with particularity that—

(I) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(II) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(III) the agency has all taken necessary steps to secure the agency information system and agency information stored on or transiting it; and

(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and the authorizing committees of the agency.

(3) RULES OF CONSTRUCTION.—Nothing in this section shall be construed—

(A) to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code;

(B) to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of title 44, United States Code; or

(C) to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

SEC. 206. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.

(b) THIRD PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and

(v) a list by agency of compliance with the requirements of section 205(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 204(a)(2); and

(ii) the improved metrics developed pursuant to section 204(b).

SEC. 207. TERMINATION.

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system, as defined in section 11103 of title 40, United States Code; and

(2) the Director of National Intelligence shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense or an element of the intelligence community.

SEC. 209. DIRECTION TO AGENCIES.

(a) IN GENERAL.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

''(h) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

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

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

''(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

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

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

''(C) minimize the impact of a directive under this subsection by—

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

''(ii) limiting directives to the shortest period practicable;

''(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

''(E) consult with the Director of the National Institute of Standards and Technology regarding any directive issued under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

''(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

''(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and

''(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system for the purpose of ensuring the security of the information or information system or other agency information systems, if—

''(i) the Secretary determines that there is an imminent threat to agency information systems;

''(ii) the Secretary determines that a directive issued under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

''(iii) the Secretary determines that the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;

''(iv) the Secretary provides prior notice to the Director and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this subparagraph, and notifies the appropriate congressional committees and authorizing committees of each such agencies within 7 days of taking an action under this subparagraph, of—

''(I) any action taken under this subparagraph; and

''(II) the reasons for and duration and nature of the action;

''(v) the action of the Secretary is consistent with applicable law; and

''(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).

''(B) LIMITATION ON DELEGATION.—The authority under subparagraph (A) may not be delegated by the Secretary.

''(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director and in consultation with the heads of agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

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

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

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

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

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

''(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

''(j) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term 'appropriate congressional committees' means—

''(1) the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, and the Committee on Commerce, Science, and Transportation of the Senate; and

''(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.''.

(b) TECHNICAL AMENDMENT.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—

(1) in clause (iii), by striking ''and'' at the end; and

(2) by adding at the end the following: ''(v) emergency directives issued by the Secretary under section 3553(h); and''.

''(v) emergency directives issued by the Secretary under section 3553(h); and''.

SA 2626. Mr. WHITEHOUSE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking ''if—'' and all that follows through ''therefrom.'' and inserting ''if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

SEC. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate paragraph (1), (4), (5), or (7) of section 1030(a) where such conduct would affect 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing malicious software on the computers, or using the computers without authorization;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

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

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

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

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

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

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

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

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

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

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

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

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).''.

(b) TABLE OF SECTIONS.—The table of sections 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. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a), by striking paragraph (6) and inserting the following:

''(6) knowing such conduct to be wrongful, intentionally traffics in any password or similar information, or any other means of access, further knowing or having reason to know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;'';

(2) in subsection (c)—

(A) in paragraph (2), by striking '', (a)(3), or (a)(6)'' each place it appears and inserting ''or (a)(3)''; and

(B) in paragraph (4)—

(i) in subparagraph (C)(i), by striking ''or an attempt to commit an offense''; and

(ii) in subparagraph (D), by striking clause (ii) and inserting the following:

''(ii) an offense, or an attempt to commit an offense, under subsection (a)(6);''; and

(3) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(6),'' after ''of this section''.

SA 2627. Mr. CARPER (for himself, Mr. JOHNSON, Ms. AYOTTE, Mrs. MCCASKILL, Ms. COLLINS, and Mr. WARNER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT ACT

SECTION 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

SEC. 202. DEFINITIONS.

In this title—

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

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);

(3) the term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(7) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

''SEC. 228. CYBERSECURITY PLANS.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227;

''(3) the term 'information sharing and analysis organization' has the meaning given the term in section 212(5); and

''(4) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

''SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

''(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

''(3) the term 'agency information system' has the meaning given the term in section 228; and

''(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

''(b) REQUIREMENT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

''(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and

''(7) shall ensure that—

''(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

''(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

''(d) PRIVATE ENTITIES.—

''(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

''(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.''.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

''Sec. 226. Cybersecurity recruitment and retention.
''Sec. 227. National cybersecurity and communications integration center.
''Sec. 228. Cybersecurity plans.
''Sec. 229. Clearances.
''Sec. 230. Federal intrusion detection and prevention system.''.

SEC. 204. ADVANCED INTERNAL DEFENSES.

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting '', operating, and maintaining'' after ''deploying''.

SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to—

(A) the Department of Defense or an element of the intelligence community; or

(B) an agency information system for which—

(i) the head of the agency has personally certified to the Director with particularity that—

(I) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(II) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(III) the agency has all taken necessary steps to secure the agency information system and agency information stored on or transiting it; and

(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and the authorizing committees of the agency.

(3) RULES OF CONSTRUCTION.—Nothing in this section shall be construed—

(A) to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code;

(B) to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of title 44, United States Code; or

(C) to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

SEC. 206. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.

(b) THIRD PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and

(v) a list by agency of compliance with the requirements of section 205(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 204(a)(2); and

(ii) the improved metrics developed pursuant to section 204(b).

SEC. 207. TERMINATION.

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system, as defined in section 11103 of title 40, United States Code; and

(2) the Director of National Intelligence shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense or an element of the intelligence community.

SEC. 209. DIRECTION TO AGENCIES.

(a) IN GENERAL.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

''(h) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

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

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

''(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

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

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

''(C) minimize the impact of a directive under this subsection by—

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

''(ii) limiting directives to the shortest period practicable;

''(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

''(E) consult with the Director of the National Institute of Standards and Technology regarding any directive issued under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

''(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

''(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and

''(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other

system traffic transiting to or from or stored on an agency information system for the purpose of ensuring the security of the information or information system or other agency information systems, if—

''(i) the Secretary determines that there is an imminent threat to agency information systems;

''(ii) the Secretary determines that a directive issued under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

''(iii) the Secretary determines that the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;

''(iv) the Secretary provides prior notice to the Director and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this subparagraph, and notifies the appropriate congressional committees and authorizing committees of each such agencies within 7 days of taking an action under this subparagraph, of—

''(I) any action taken under this subparagraph; and

''(II) the reasons for and duration and nature of the action;

''(v) the action of the Secretary is consistent with applicable law; and

''(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).

''(B) LIMITATION ON DELEGATION.—The authority under subparagraph (A) may not be delegated by the Secretary.

''(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director and in consultation with the heads of agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

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

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

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

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

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

''(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

''(j) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term 'appropriate congressional committees' means—

''(1) the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, and the Committee on Commerce, Science, and Transportation of the Senate; and

''(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.''.

(b) TECHNICAL AMENDMENT.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—

(1) in clause (iii), by striking ''and'' at the end; and

(2) by adding at the end the following: ''(v) emergency directives issued by the Secretary under section 3553(h); and''.

''(v) emergency directives issued by the Secretary under section 3553(h); and''.

SA 2628. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. RECONSIDERATION OF PROPOSED RULE ON IMPLEMENTATION OF WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS RELATING TO INTRUSION AND SURVEILLANCE ITEMS.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the Secretary of Commerce shall—

(1) review, and consider public comments received with respect to, the proposed rule of the Bureau of Industry and Security, entitled ''Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items'' and published on May 20, 2015 (80 Fed. Reg. 28,853); and

(2) revise the proposed rule in accordance with subsection (b).

(b) REQUIREMENTS FOR REVISED RULE.—In revising the proposed rule described in subsection (a)(1), the Secretary shall—

(1) develop the revisions in close consultation with civil society organizations, including privacy advocates, public and private sector technologists, security researchers, and public and private sector software developers;

(2) ensure that the proposed rule is—

(A) limited to the scope of the agreements reached at the plenary meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies in December 2013; and

(B) consistent with the regulation of cybersecurity items by other countries participating in the Wassenaar Arrangement, as appropriate;

(3) exclude cybersecurity items available for mass-market purchase from regulation under the proposed rule; and

(4) ensure that, before issuing a final rule—

(A) the proposed rule is available for public comment for not less than 60 days; and

(B) a public hearing is held on the proposed rule.

(c) REGULATORY IMPACT ANALYSIS.—

(1) IN GENERAL.—Not later than one year after issuing a final rule based on the proposed rule described in subsection (a)(1) and revised in accordance with subsection (b), the Secretary shall conduct a regulatory impact analysis of the effects of the rule on the development and export of cybersecurity items.

(2) PUBLIC AVAILABILITY.—The Secretary shall make the analysis required by paragraph (1) available to the public.

SA 2629. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REPORT ON ACCOUNTABILITY FOR THE DATA BREACH OF THE OFFICE OF PERSONNEL MANAGEMENT.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

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

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

(2) DATA BREACH.—The term ''data breach'' means the data breach of systems of the Office of Personnel Management that occurred during fiscal year 2015 which resulted in the theft of sensitive information of at least 21,500,000 Federal employees and their families.

(b) REQUIREMENT FOR REPORT.—Not later than 30 days after date of the enactment of this Act, the President shall submit to the appropriate committees of Congress and make available to the public a report that—

(1) identifies the perpetrator, including any state sponsor, of the data breach;

(2) includes a plan to impose penalties on such perpetrator under United States law; and

(3) describes a strategy to initiate diplomatic discussions with any state sponsor of the data breach.

(c) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) Identification of any individual perpetrator of the data breach, by name and nationality.

(2) Identification of any state sponsor of the data breach, including each agency of the government of the state sponsor that was responsible for authorizing, performing, or endorsing the data breach.

(3) A description of the actions proposed to penalize each individual identified under paragraph (1) under United States law.

(4) The strategy required by subsection (a)(3) shall include—

(A) a description of any action the President has undertaken to initiate or carry out diplomatic discussions with any state sponsor identified under paragraph (2); and

(B) a strategy to initiate or carry out diplomatic discussions in high-level forums and interactions during the 180-day period beginning on the date of the enactment of this Act.

SA 2630. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. BIENNIAL CYBER REVIEW.

(a) REQUIREMENT FOR REVIEW.—Beginning in 2016 and not less frequently than once every two years thereafter, the President shall complete a review of the cyber posture of the United States, including an unclassified summary of roles, missions, accomplishments, plans, and programs.

(b) PURPOSES.—The purposes of each such review are—

(1) to assess the cyber security of the United States;

(2) to determine and express the cyber strategy of the United States; and

(3) to establish a revised cyber program for the next 2-year period.

(c) CONTENT.—Each review required by subsection (a) shall include—

(1) a comprehensive examination of the cyber strategy, force structure, personnel, modernization plans, infrastructure, and budget plan of the United States;

(2) an assessment of the ability of the United States to recover from a cyber emergency;

(3) an assessment of other elements of the cyber program of the United States;

(4) an assessment of critical national security infrastructure and data that is vulnerable to cyberattacks and cybertheft; and

(5) an assessment of international engagement efforts to establish viable norms of behavior in cyberspace to implement the 2011 International Strategy for Cyberspace.

(d) INVOLVEMENT OF CYBERSECURITY ADVISORY PANEL.—

(1) REQUIREMENT TO INFORM.—The President shall inform the Cybersecurity Advisory Panel established or designated under section _____, on an ongoing basis, of the actions carried out to conduct each review required by subsection (a).

(2) ASSESSMENT PRIOR TO COMPLETION OF REVIEW.—Not later than 1 year prior to the date of completion of each review required by subsection (a), the Chairman of the Cybersecurity Advisory Panel shall submit to the President, the assessment of such Panel of actions carried out to conduct the review as of the date of the submission, including any recommendations of the Panel for improvements to the review or for additional matters to be covered in the review.

(3) ASSESSMENT OF COMPLETED REVIEW.—At the time each review required by subsection (a) is completed and in time to be included in a report required by subsection (d), the Chairman of the Cybersecurity Advisory Panel shall submit to the President, on behalf of the Panel, an assessment of such review.

(e) REPORT.—Not later than September 30, 2016, and not less frequently than once every two years thereafter, the President shall submit to Congress a comprehensive report on each review required by subsection (a). Each report shall include—

(1) the results of the review, including a comprehensive discussion of the cyber strategy of the United States and the collaboration between the public and private sectors best suited to implement that strategy;

(2) a description of the threats examined for purposes of the review and the scenarios developed in the examination of such threats;

(3) the assumptions used in the review, including assumptions relating to the cooperation of other countries and levels of acceptable risk; and

(4) the assessment of the Cybersecurity Advisory Panel submitted under subsection (c)(3).

SEC. _____. CYBERSECURITY ADVISORY PANEL.

(a) IN GENERAL.—The President shall establish or designate a Cybersecurity Advisory Panel.

(b) APPOINTMENT.—The President—

(1) shall appoint as members of the Cybersecurity Advisory Panel representatives of industry, academic, nonprofit organizations, interest groups, and advocacy organizations, and State and local governments who are qualified to provide advice and information on cybersecurity research, development, demonstrations, education, personnel, technology transfer, commercial application, or societal and civil liberty concerns;

(2) shall appoint a Chairman of the Panel from among the members of the Panel; and

(3) may seek and give consideration to recommendations for appointments to the Panel from Congress, industry, the cybersecurity community, the defense community, State and local governments, and other appropriate organizations.

(c) DUTIES.—The Cybersecurity Advisory Panel shall advise the President on matters relating to the national cybersecurity program and strategy and shall assess—

(1) trends and developments in cybersecurity science research and development;

(2) progress made in implementing the strategy;

(3) the need to revise the strategy;

(4) the readiness and capacity of the Federal and national workforces to implement the national cybersecurity program and strategy, and the steps necessary to improve workforce readiness and capacity;

(5) the balance among the components of the national strategy, including funding for program components;

(6) whether the strategy, priorities, and goals are helping to maintain United States leadership and defense in cybersecurity;

(7) the management, coordination, implementation, and activities of the strategy;

(8) whether the concerns of Federal, State, and local law enforcement entities are adequately addressed; and

(9) whether societal and civil liberty concerns are adequately addressed.

(d) REPORTS.—Not less frequently than once every 4 years, the Cybersecurity Advisory Panel shall submit to the President a report on its assessments under subsection (c) and its recommendations for ways to improve the strategy.

(e) TRAVEL EXPENSES OF NON-FEDERAL MEMBERS.—Non-Federal members of the Cybersecurity Advisory Panel, while attending meetings of the Panel or while otherwise serving at the request of the head of the Panel while away from their homes or regular places of business, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for individuals in the Government serving without pay. Nothing in this subsection shall be construed to prohibit members of the Panel who are officers or employees of the United States from being allowed travel expenses, including per diem in lieu of subsistence, in accordance with law.

(f) EXEMPTION FROM FACA SUNSET.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Cybersecurity Advisory Panel.

SA 2631. Mr. GARDNER (for himself and Mr. CARDIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace.

(b) ELEMENTS.—The strategy required by subsection (a) shall include the following:

(1) A review of actions and activities undertaken by the Secretary of State to date to support the goal of the President's International Strategy for Cyberspace, released in May 2011, to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.''.

(2) A plan of action to guide the diplomacy of the Secretary of State, with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing discussions in multilateral fora to obtain agreements on international norms in cyberspace.

(3) A review of the alternative concepts with regard to international norms in cyberspace offered by foreign countries that are prominent actors, including China, Russia, Brazil, and India.

(4) A detailed description of threats to United States national security in cyberspace from foreign countries, state-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.

(5) A review of policy tools available to the President to deter foreign countries, state-sponsored actors, and private actors, including those outlined in Executive Order 13694, released on April 1, 2015.

(6) A review of resources required by the Secretary, including the Office of the Coordinator for Cyber Issues, to conduct activities to build responsible norms of international cyber behavior.

(c) CONSULTATION.—In preparing the strategy required by subsection (a), the Secretary of State shall consult, as appropriate, with other agencies and departments of the United States and the private sector and nongovernmental organizations in the United States with recognized credentials and expertise in foreign policy, national security, and cybersecurity.

(d) FORM OF STRATEGY.—The strategy required by subsection (a) shall be in unclassified form, but may include a classified annex.

(e) AVAILABILITY OF INFORMATION.—The Secretary of State shall—

(1) make the strategy required in subsection (a) available the public; and

(2) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the strategy, including any material contained in a classified annex.

SA 2632. Mr. TESTER (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 40, between lines 12 and 13, insert the following:

(i) The number of cyber threat indicators and defensive measures shared under this Act, including a breakdown of—

(I) the total number of cyber threat indicators shared through the capability described in section 5(c);

(II) a good faith estimate of the number of cyber threat indicators shared by entities with civilian Federal entities through capabilities other than those described in section 5(c);

(III) a good faith estimate of the number of cyber threat indicators shared by entities with military Federal entities through capabilities other than those described in section 5(c);

(IV) the number of times personal information or information that identifies a specific

person was removed from a cyber threat indicator shared under section 5(c);

(V) an assessment of the extent to which personal information or information that identifies a specific person was shared under this Act though such information was not necessary to describe or mitigate a cybersecurity threat or security vulnerability;

(VI) a report on any known harms caused by any defensive measure operated or shared under the authority of this Act;

(VII) the total number of times that information shared under this Act was used to prevent, investigate, disrupt, or prosecute any offense under title 18, United States Code, including an offense under section 1028, 1028A, or 1029, or chapter 37or 90 of such title 18; and

(VIII) the total number of times that information shared under this Act was used to prevent, investigate, disrupt, or prosecute a terrorism offense under chapter 113B of title 18, United States Code.

SA 2633. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. AYOTTE to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end of section 9, add the following:

(f) ASSESSMENT.—The report required under subsection (a) shall include an assessment of the implications of the Memorandum Opinion for the Assistant Attorney General dated September 20, 2011, for cybersecurity, including the potential for thefts of personally identifiable information and for the creation of opportunities for organized crime and terrorist groups to generate revenue and launder money through related online activities; provided that the Department of Justice shall not follow such Opinion with respect to which activities are covered by section 1084 of title 18, United States Code, until 18 months after such report has been received and the President certifies to Congress that the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security are in agreement that the Opinion will not increase the threat of thefts of personally identifiable information or the exploitation of online activities for criminal purposes, and that such agencies have sufficient resources and legal tools to protect consumers from such threat, and deter such criminal activities.

SA 2634. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. AYOTTE to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. RESTORATION OF AMERICA'S WIRE ACT.

(a) SHORT TITLE.—This section may be cited as the ''Restoration of America's Wire Act''.

(b) WIRE ACT CLARIFICATION.—Section 1084 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) by striking ''bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest,'' and inserting ''any bet or wager, or information assisting in the placing of any bet or wager,'';

(B) by striking ''result of bets or wagers'' and inserting ''result of any bet or wager''; and

(C) by striking ''or for information assisting in the placing of bets or wagers,''; and

(2) by striking subsection (e) and inserting the following:

''(e) As used in this section—

''(1) the term 'bet or wager' does not include any activities set forth in section 5362(1)(E) of title 31;

''(2) the term 'State' means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, or a commonwealth, territory, or possession of the United States;

''(3) the term 'uses a wire communication facility for the transmission in interstate or foreign commerce of any bet or wager' includes any transmission over the Internet carried interstate or in foreign commerce, incidentally or otherwise; and

''(4) the term 'wire communication' has the meaning given the term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).''.

(c) RULE OF CONSTRUCTION.—Nothing in this section, or the amendments made by this section, shall be construed—

(1) to preempt any State law prohibiting gambling; or

(2) to alter, limit, or extend—

(A) the relationship between the Interstate Horseracing Act of 1978 (15 U.S.C. 3001 et seq.) and other Federal laws in effect on the date of enactment of this Act;

(B) the ability of a State licensed lottery (including in conjunction with its supplier) or State licensed retailer to make on-premises retail lottery sales, including through a self-service retail lottery terminal, or to transmit information ancillary to such sales (including information relating to subscriptions or fulfillment of game play), in accordance with applicable Federal and State laws;

(C) the ability of a State licensed gaming establishment or a tribal gaming establishment to transmit information assisting in the placing of a bet or wager on the physical premises of the establishment, in accordance with applicable Federal and State laws; or

(D) the relationship between Federal laws and State charitable gaming laws.

SA 2635. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 46, between lines 15 and 16, insert the following:

(g) FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER.—As the sector-specific agency for the financial sector under Presidential Policy Directive–21, issued February 12, 2013, the Department of the Treasury shall collaborate with the private sector to—

(1) facilitate membership of depository institutions (as defined in section 19(b)(1) of the Federal Reserve Act (12 U.S.C. 461(b)(1))) that have not more than $10,000,000,000 in total consolidated assets (in this subsection referred to as ''small depository institutions'') in the Financial Services Information Sharing and Analysis Center at no cost to the small depository institutions; and

(2) ensure that the Financial Services Information Sharing and Analysis Center provides to its members that are small depository institutions information that is comprehensible to and useable by small depository institutions.

SA 2636. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 49, between lines 3 and 4, add the following:

(n) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to limit or modify the authority of the appropriate Federal financial institutions regulatory agency (as defined in section 8(e)(7)(D) of the Federal Deposit Insurance Act (12 U.S.C. 1818(e)(7)(D))) to interpret, or take enforcement action under, any other provision of Federal law for the purposes of—

(1) safety and soundness; or

(2) consumer protection.

SA 2637. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 12, after line 23, add the following:

(d) COLLABORATION BETWEEN INFORMATION SHARING AND ANALYSIS CENTERS.—

(1) DEFINITIONS.—In this subsection—

(A) the term ''critical infrastructure sector'' means any sector identified as a critical infrastructure sector in Presidential Policy Directive–21, issued February 12, 2013 (or any successor thereto); and

(B) the term ''Sector-Specific Agency'' has the meaning given the term in Presidential Policy Directive–21, issued dated February 12, 2013 (or any successor thereto).

(2) COLLABORATION.—The Sector-Specific Agencies associated with critical infrastructure sectors shall facilitate collaboration between the sector-specific information sharing and analysis centers to share cyber threat information across sectors.

(3) FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER.—As the head of the Sector-Specific Agency for the financial sector under Presidential Policy Directive–21, issued February 12, 2013, the Secretary of the Treasury shall collaborate with the private sector to ensure that risks that may impact the financial sector are shared appropriately with entities in the financial sector, which shall include facilitating information sharing between the Financial Services Information Sharing and Analysis Center and—

(A) other information sharing and analysis centers; and

(B) other information sharing and analysis organizations.

SA 2638. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. IMPROVED REGULATION AND EXAMINATION OF SERVICE PROVIDERS.

(a) BANK SERVICE COMPANY ACT.—Section 7 of the Bank Service Company Act (12 U.S.C. 1867) is amended by adding at the end the following:

''(e) REQUIRED EXAMINATIONS.—

''(1) IN GENERAL.—Except as provided in paragraph (3), the appropriate Federal banking agency shall, not less than once during each 12-month period, conduct a full-scope, on-site examination of each bank service company.

''(2) STATE EXAMINATIONS ACCEPTABLE.—Except as provided in paragraph (3), the examinations required by paragraph (1) may be conducted in alternate 12-month periods, as appropriate, if the appropriate Federal banking agency determines that an examination of the bank service company conducted by the State during the intervening 12-month period carries out the purpose of this subsection.

''(3) 18-MONTH RULE FOR CERTAIN BANK SERVICE COMPANIES.—The examinations conducted under paragraphs (1) and (2) shall be conducted during an 18-month period, tailored as needed to align with a lengthened examination cycle of a bank service company, if the appropriate Federal banking agency determines that a bank service company—

''(A) was well managed at the most recent examination of the bank service company;

''(B) is not subject to a formal enforcement proceeding or order by the appropriate Federal banking agency (as of the date on which the determination is made); and

''(C) satisfies any other requirement that the appropriate Federal banking agency determines is appropriate.

''(4) AUTHORITY TO CONDUCT MORE FREQUENT EXAMINATIONS.—Each appropriate Federal banking agency may examine any bank service company as frequently as the appropriate Federal banking agency determines is necessary.''.

(b) HOME OWNERS' LOAN ACT.—Section 5(d)(7) of the Home Owners' Loan Act (12 U.S.C. 1464(d)(7)) is amended by adding at the end the following:

''(F) REQUIRED EXAMINATIONS.—

''(i) IN GENERAL.—Except as provided in clause (iii), the appropriate Federal banking agency shall, not less than once during each 12-month period, conduct a full-scope, on-site examination of each service company.

''(ii) STATE EXAMINATIONS ACCEPTABLE.—Except as provided in clause (iii), the examinations required by clause (i) may be conducted in alternate 12-month periods, as appropriate, if the appropriate Federal banking agency determines that an examination of the service company conducted by the State during the intervening 12-month period carries out the purpose of this subparagraph.

''(iii) 18-MONTH RULE FOR CERTAIN SERVICE COMPANIES.—The examinations conducted under clauses (i) and (ii) shall be conducted during an 18-month period, tailored as needed to align with a lengthened examination cycle of a service company, if the appropriate Federal banking agency determines that a service company—

''(I) was well managed at the most recent examination of the service company;

''(II) is not subject to a formal enforcement proceeding or order by the appropriate Federal banking agency (as of the date on which the determination is made); and

''(III) satisfies any other requirement that the appropriate Federal banking agency determines is necessary.

''(iv) AUTHORITY TO CONDUCT MORE FREQUENT EXAMINATIONS.—Each appropriate Federal banking agency may examine any service company as frequently as the appropriate Federal banking agency determines is necessary.''.

SA 2639. Mr. WHITEHOUSE proposed an amendment to the bill S. 1523, to amend the Federal Water Pollution Control Act to reauthorize the National Estuary Program, and for other purposes; as follows:

On page 3, line 17, strike ''$27,000,000'' and insert ''$26,000,000''.

NOTICE OF INTENT TO OBJECT TO PROCEEDING

I, Senator CHARLES E. GRASSLEY, intend to object to proceeding to the appointments of Bradley Duane Arsenault, Bret Thomas Campbell, Karen Stone Exel, Gloria Jean Garland, Michael H. Hryshchyshyn, Jr., Ying X. Hsu, Stephen S. Kelley, Mary Catherine Leherr, Denise G. Manning, Paul Karlis Markovs, Scott Currie McNiven, Hanh Ngoc Nguyen, Denise Frances O'Toole, Marisol E. Perez, Ronald F. Savage, Adam P. Schmidt, Anna Toness, Michael J. Torreano, Nicholas John Vivio, and Jamshed Zuberi to be Foreign Service Officers of Class Two, dated August 5, 2015.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ARMED SERVICES

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Armed Services be authorized to meet during the session of the Senate on August 5, 2015, at 9:30 a.m.

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

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Banking, Housing, and Urban Affairs be authorized to meet during the session of the Senate on August 5, 2015, at 10 a.m., to conduct a hearing entitled ''The Implications of Sanctions Relief Under The Iran Agreement.''

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

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Environment and Public Works be authorized to meet during the session of the Senate on August 5, 2015, at 10 a.m., in room SD–406 of the Dirksen Senate Office Building.

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

COMMITTEE ON FINANCE

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to meet during the session of the Senate on August 5, 2015.

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

COMMITTEE ON FOREIGN RELATIONS

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 5, 2015, at 2 p.m., to conduct a hearing entitled ''Implications of the JCPOA for U.S. Policy in the Middle East.''

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

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on Health, Education, Labor, and Pensions be authorized to meet during the session of the Senate on August 5, 2015, at 10 a.m., in room SD–430 of the Dirksen Senate Office Building to conduct a hearing entitled ''Reauthorizing the Higher Education Act: Opportunities to Improve Student Success.''

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

COMMITTEE ON THE JUDICIARY

Ms. COLLINS. Mr. President, I ask unanimous consent that the Committee on the Judiciary be authorized to meet during the session of the Senate on August 5, 2015, at 10 a.m., in room SD–106 of the Dirksen Senate Office Building to conduct a hearing entitled '''All' Means 'All': the Justice Department's Failure to Comply With Its Legal Obligation to Ensure Inspector General Access to All Records Needed for Independent Oversight.''

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

PRIVILEGES OF THE FLOOR

Mr. MURPHY. Mr. President, I ask unanimous consent for my State Department fellow, Tovan McDaniel, to be granted floor privileges for the remainder of this work period.

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

GERARDO HERNANDEZ AIRPORT SECURITY ACT OF 2015

Mr. GARDNER. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 163, H.R. 720.

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

The senior assistant legislative clerk read as follows:

A bill (H.R. 720) to improve intergovernmental planning for and communication during security incidents at domestic airports, and for other purposes.

There being no objection, the Senate proceeded to consider the bill, which had been reported from the Committee on Commerce, Science, and Transportation, with an amendment to strike all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Gerardo Hernandez Airport Security Act of 2015''.

SEC. 2. DEFINITIONS.

In this Act:

(1) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Homeland Security (Transportation Security) of the Department of Homeland Security.

(2) ADMINISTRATION.—The term ''Administration'' means the Transportation Security Administration.