SA 2608. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2609. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2610. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2611. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2612. Mr. FRANKEN (for himself, Mr. LEAHY, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2613. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2614. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2615. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2549. Mr. PETERS 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. ___. CERTIFICATION FOR CYBERSECURITY AND INFORMATION ASSURANCE EDUCATION PROGRAMS.

The Secretary of Homeland Security, in collaboration with the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology, shall develop a certification for existing cybersecurity and information assurance education programs, which shall be provided to those programs that provide training in proper procedure and protocol for sharing cyber threat indicators and protecting sensitive personally identifiable information.

SA 2550. Mr. PETERS 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. ___. CYBERSECURITY AWARENESS CAMPAIGN.

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

''SEC. 230. CYBERSECURITY AWARENESS CAMPAIGN.

''(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall develop and implement an ongoing and comprehensive cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks.

''(b) REQUIREMENTS.—The campaign developed under subsection (a) shall, at a minimum, publish and disseminate, on an ongoing basis, the following:

''(1) Public service announcements targeted at improving awareness among State, local, and tribal governments, the private sector, academia, and stakeholders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans.

''(2) Vendor and technology-neutral voluntary best practices information.

''(c) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection shall consult with a wide range of stakeholders in government, industry, academia, and the non-profit community in carrying out this section.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following:

''Sec. 230. Cybersecurity Awareness Campaign.''.

SA 2551. Mr. PETERS 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) ensure collaboration with State, local and tribal governments to enhance the effectiveness of sharing cyber threat indicators and ensure cooperation to prevent, protect, mitigate, respond to, and recover from cybersecurity incidents.

SA 2552. Mr. COONS 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:

Beginning on page 21, strike line 23 and all that follows through page 31, line 5 and insert the following:

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 that are received through the process described in subsection (c) of this section and that satisfy the requirements of the guidelines developed under subsection (b)—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this Act; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this Act that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) shall require the Department of Homeland Security to review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such indicator or defensive measure with appropriate Federal entities;

(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators as quickly as operationally possible from the Department of Homeland Security;

(E) is in compliance with the policies, procedures, and guidelines required by this section; and

(F) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this Act; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.

SA 2553. Mr. SCHATZ 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:

Strike paragraph (2) of section 3(b) and insert the following:

(2) COORDINATION AND CONSULTATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall, to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner—

(A) consult with appropriate private entities; and

(B) coordinate with appropriate Federal entities, including the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)).

SA 2554. Mr. SCHATZ 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:

Beginning on page 13, strike line 4, and all that follows through page 14, line 1.

SA 2555. Ms. HEITKAMP 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. ___. ENHANCEMENT OF EMERGENCY SERVICES.

(a) COLLECTION OF DATA.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit a report to Congress on the methods developed under paragraph (1) and shall make such report publically available on the website of the National Institute of Standards and Technology.

SA 2556. Mr. LEE (for himself, Mr. LEAHY, Mr. DURBIN, and Mr. HELLER) 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—ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS

SEC. 201. SHORT TITLE.

This title may be cited as the ''Electronic Communications Privacy Act Amendments Act of 2015''.

SEC. 202. CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS.

Section 2702(a)(3) of title 18, United States Code, is amended to read as follows:

''(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.''.

SEC. 203. ELIMINATION OF 180-DAY RULE; SEARCH WARRANT REQUIREMENT; REQUIRED DISCLOSURE OF CUSTOMER RECORDS.

(a) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a), (b), and (c) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS.—A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure.

''(b) NOTICE.—Except as provided in section 2705, not later than 10 business days in the case of a law enforcement agency, or not later than 3 business days in the case of any other governmental entity, after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

''(1) a copy of the warrant; and

''(2) a notice that includes the information referred to in clauses (i) and (ii) of section 2705(a)(4)(B).

''(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

''(1) IN GENERAL.—Subject to paragraph (2), a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of the provider or service (not including the contents of communications), only if the governmental entity—

''(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure;

''(B) obtains a court order directing the disclosure under subsection (d);

''(C) has the consent of the subscriber or customer to the disclosure; or

''(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of the provider or service that is engaged in telemarketing (as defined in section 2325).

''(2) INFORMATION TO BE DISCLOSED.—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means authorized under paragraph (1), disclose to a governmental entity the—

''(A) name;

''(B) address;

''(C) local and long distance telephone connection records, or records of session times and durations;

''(D) length of service (including start date) and types of service used;

''(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

''(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber or customer of such service.

''(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer.''; and

(2) by adding at the end the following:

''(h) RULE OF CONSTRUCTION.—Nothing in this section or in section 2702 shall be construed to limit the authority of a governmental entity to use an administrative subpoena authorized under a Federal or State statute or to use a Federal or State grand jury, trial, or civil discovery subpoena to—

''(1) require an originator, addressee, or intended recipient of an electronic communication to disclose the contents of the electronic communication to the governmental entity; or

''(2) require an entity that provides electronic communication services to the officers, directors, employees, or agents of the entity (for the purpose of carrying out their duties) to disclose the contents of an electronic communication to or from an officer, director, employee, or agent of the entity to a governmental entity, if the electronic communication is held, stored, or maintained on an electronic communications system owned or operated by the entity.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2703(d) of title 18, United States Code, is amended—

(1) by striking ''A court order for disclosure under subsection (b) or (c)'' and inserting ''A court order for disclosure under subsection (c)''; and

(2) by striking ''the contents of a wire or electronic communication, or''.

SEC. 204. DELAYED NOTICE.

Section 2705 of title 18, United States Code, is amended to read as follows:

''§ 2705. Delayed notice

''(a) DELAY OF NOTIFICATION.—

''(1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(2) DETERMINATION.—A court shall grant a request for delayed notification made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

''(A) endangering the life or physical safety of an individual;

''(B) flight from prosecution;

''(C) destruction of or tampering with evidence;

''(D) intimidation of potential witnesses; or

''(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

''(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of the delay of notification granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(4) EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon expiration of the period of delay of notification under paragraph (2) or (3), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court approving the search warrant, the customer or subscriber—

''(A) a copy of the warrant; and

''(B) notice that informs the customer or subscriber—

''(i) of the nature of the law enforcement inquiry with reasonable specificity;

''(ii) that information maintained for the customer or subscriber by the provider of electronic communication service or remote computing service named in the process or request was supplied to, or requested by, the governmental entity;

''(iii) of the date on which the warrant was served on the provider and the date on which the information was provided by the provider to the governmental entity;

''(iv) that notification of the customer or subscriber was delayed;

''(v) the identity of the court authorizing the delay; and

''(vi) of the provision of this chapter under which the delay was authorized.

''(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—

''(1) IN GENERAL.—A governmental entity that is obtaining the contents of a communication or information or records under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive may result in—

''(A) endangering the life or physical safety of an individual;

''(B) flight from prosecution;

''(C) destruction of or tampering with evidence;

''(D) intimidation of potential witnesses; or

''(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

''(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of an order granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(4) PRIOR NOTICE TO LAW ENFORCEMENT.—Upon expiration of the period of delay of notice under this section, and not later than 3 business days before providing notice to a customer or subscriber, a provider of electronic communication service or remote computing service shall notify the governmental entity that obtained the contents of a communication or information or records under section 2703 of the intent of the provider of electronic communication service or remote computing service to notify the customer or subscriber of the existence of the warrant, order, or subpoena seeking that information.

''(c) DEFINITION.—In this section and section 2703, the term 'law enforcement agency' means an agency of the United States, a State, or a political subdivision of a State, authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal law, or any other Federal or State agency conducting a criminal investigation.''.

SEC. 205. EVALUATION BY THE GOVERNMENT ACCOUNTABILITY OFFICE.

Not later than September 30, 2017, the Comptroller General of the United States shall submit to Congress a report regarding the disclosure of customer communications and records under section 2703 of title 18, United States Code, which shall include—

(1) an analysis and evaluation of such disclosure under section 2703 of title 18, United States Code, as in effect before the date of enactment of this Act, including—

(A) a comprehensive analysis and evaluation regarding the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which Federal, State, or local law enforcement officers used section 2703 of title 18, United States Code, to obtain information relevant to an ongoing criminal investigation;

(B) an analysis of the average length of time taken by a provider of an electronic communication service or a remote computing service to comply with requests by law enforcement officers for information under section 2703 of title 18, United States Code;

(C) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under a warrant as authorized under section 2703(a) of title 18, United States Code;

(D) the number of individual instances and type of request, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under the other information request provisions in section 2703 of title 18, United States Code; and

(E) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which law enforcement officers requested delayed notification to the subscriber or customer under section 2705 of title 18, United States Code; and

(2) an analysis and evaluation of such disclosure under section 2703 of title 18, United States Code, as amended by this title, including—

(A) an evaluation of the effects of the amendments to the warrant requirements on judges, court dockets, or any other court operations;

(B) a survey of Federal, State, and local judges and law enforcement officers to determine the average length of time required for providers of an electronic communication service or a remote computing service to provide the contents of communications requested under a search warrant, which shall include identifying the number of instances in which a judge was required to order a provider of an electronic communication service or a remote computing service to appear to show cause for failing to comply with a warrant or to issue an order of contempt against a provider of an electronic communication service or a remote computing service for such a failure; and

(C) determining whether the amendments to the warrant requirements resulted in an increase in the use of the emergency exception under section 2702(b)(8) of title 18, United States Code.

SEC. 206. RULE OF CONSTRUCTION.

Nothing in this title or an amendment made by this title shall be construed to preclude the acquisition by the United States Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, including the authorities under chapter 119 of title 18 (commonly known as the ''Wiretap Act''), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this title; or

(2) records or other information relating to a subscriber or customer of any electronic communications service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18 (commonly known as the ''Wiretap Act''), or any other provision of Federal law not specifically amended by this title.

SA 2557. Ms. MIKULSKI (for herself, Mr. CARDIN, and Mr. WARNER) 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. ____. FUNDING.

(a) IN GENERAL.—Effective on the date of enactment of this Act, there is appropriated, out of any money in the Treasury not otherwise appropriated, for the fiscal year ending September 30, 2015, an additional amount for the appropriations account appropriated under the heading ''SALARIES AND EXPENSES'' under the heading ''OFFICE OF PERSONNEL MANAGEMENT'', $37,000,000, to remain available until September 30, 2017, for accelerated cybersecurity in response to data breaches.

(b) EMERGENCY DESIGNATION.—The amount appropriated under subsection (a) is designated by the Congress as an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985, and shall be available only if the President subsequently so designates such amount and transmits such designation to the Congress.

SA 2558. Mr. BENNET (for himself and Mr. PORTMAN) 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 WORKFORCE ASSESSMENT

SECTION 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Workforce Assessment Act''.

SEC. 202. DEFINITIONS.

In this title:

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

(A) the Committee on Armed Services of the Senate;

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

(C) the Committee on Armed Services in the House of Representatives;

(D) the Committee on Homeland Security of the House of Representatives; and

(E) the Committee on Oversight and Government Reform of House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(3) ROLES.—The term ''roles'' has the meaning given the term in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

SEC. 203. NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.

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

(1) identify all positions within the agency that require the performance of information technology, cybersecurity, or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection (b).

(b) EMPLOYMENT CODES.—

(1) PROCEDURES.—

(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the National Institute of Standards and Technology, shall update the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework to include a corresponding coding structure.

(B) IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) IDENTIFICATION OF NON-CIVILIAN CYBER PERSONNEL.—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal non-civilian positions that require the performance of information technology, cybersecurity or other cyber-related functions.

(D) BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

(i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework;

(ii) the level of preparedness of other civilian and non-civilian cyber personnel without existing credentials to pass certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions

(as defined in the National Initiative for Cybersecurity Education's coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 204. IDENTIFICATION OF CYBER-RELATED ROLES OF CRITICAL NEED.

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 203(b)(2), and annually through 2022, the head of each Federal agency, in consultation with the Director and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

(1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and

(2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

(1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and

(2) submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 205. GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.

The Comptroller General of the United States shall—

(1) analyze and monitor the implementation of sections 203 and 204; and

(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

SA 2559. Mr. MANCHIN 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 8, between lines 23 and 24, insert the following:

(16) REAL TIME; REAL-TIME.—The terms ''real time'' and ''real-time'' means as close to real time as practicable.

(17) DELAY.—The term ''delay'', with respect to the sharing of a cyber threat indicator, excludes any time necessary to ensure that the cyber threat indicator shared does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

(18) MODIFICATION.—The term ''modification'', with respect to the sharing of a cyber threat indicator, excludes any process necessary to ensure that the cyber threat indicator modified does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

SA 2560. Mr. MANCHIN 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, strike lines 4 through 10, and insert the following:

(1) IN GENERAL.—

(A) AUTHORIZATION.—Except as provided in subparagraph (B) and paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(B) EXCEPTION FOR DEPARTMENT OF DEFENSE.—Notwithstanding subparagraph (A), no entity is permitted under this Act to share with the Department of Defense or any component of the Department, including the National Security Agency, a cyber threat indicator or defensive measure.

SA 2561. Mr. PAUL 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:

TITLE ____—CARRYING OF FIREARMS ON MILITARY INSTALLATIONS

SEC. ____1. SHORT TITLE.

This title may be cited as the ''Servicemembers Self-Defense Act of 2015''.

SEC. ____2. FIREARMS PERMITTED ON DEPARTMENT OF DEFENSE PROPERTY.

Section 930(g)(1) of title 18, United States Code, is amended—

(1) by striking ''The term 'Federal facility' means'' and inserting the following: ''The term 'Federal facility'—

''(A) means'';

(2) by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(B) with respect to a qualified member of the Armed Forces, as defined in section 926D(a), does not include any land, a building, or any part thereof owned or leased by the Department of Defense.''.

SEC. ____3. LAWFUL POSSESSION OF FIREARMS ON MILITARY INSTALLATIONS BY MEMBERS OF THE ARMED FORCES.

(a) MODIFICATION OF GENERAL ARTICLE.—Section 934 of title 10, United States Code (article 134 of the Uniform Code of Military Justice), is amended—

(1) by inserting ''(a) IN GENERAL.—'' before ''Though not specifically mentioned''; and

(2) by adding at the end the following new subsection:

''(b) POSSESSION OF A FIREARM.—The possession of a concealed or open carry firearm by a member of the armed forces subject to this chapter on a military installation, if lawful under the laws of the State in which the installation is located, is not an offense under this section.''.

(b) MODIFICATION OF REGULATIONS.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Defense shall amend Department of Defense Directive number 5210.56 to provide that members of the Armed Forces may possess firearms for defensive purposes on facilities and installations of the Department of Defense in a manner consistent with the laws of the State in which the facility or installation concerned is located.

SEC. ____4. CARRYING OF CONCEALED FIREARMS BY QUALIFIED MEMBERS OF THE ARMED FORCES.

(a) IN GENERAL.—Chapter 44 of title 18, United States Code, is amended by inserting after section 926C the following

''§ 926D. Carrying of concealed firearms by qualified members of the Armed Forces

''(a) DEFINITIONS.—As used in this section—

''(1) the term 'firearm'—

''(A) except as provided in this paragraph, has the same meaning as in section 921;

''(B) includes ammunition not expressly prohibited by Federal law or subject to the provisions of the National Firearms Act; and

''(C) does not include—

''(i) any machinegun (as defined in section 5845 of the National Firearms Act);

''(ii) any firearm silencer; or

''(iii) any destructive device; and

''(2) the term 'qualified member of the Armed Forces' means an individual who—

''(A) is a member of the Armed Forces on active duty status, as defined in section 101(d)(1) of title 10;

''(B) is not the subject of disciplinary action under the Uniform Code of Military Justice;

''(C) is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

''(D) is not prohibited by Federal law from receiving a firearm.

''(b) AUTHORIZATION.—Notwithstanding any provision of the law of any State or any political subdivision thereof, an individual who is a qualified member of the Armed Forces and who is carry identification required by subsection (d) may carry a concealed firearm that has been shipped or transported in interstate or foreign commerce, subject to subsection (c).

''(c) LIMITATIONS.—This section shall not be construed to superseded or limit the laws of any State that—

''(1) permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property; or

''(2) prohibit or restrict the possession of firearms on any State or local government property, installation, building, base, or park.

''(d) IDENTIFICATION.—The identification required by this subsection is the photographic identification issued by the Department of Defense for the qualified member of the Armed Forces.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 44 of title 18, United States Code, is amended by inserting after the item relating to section 926C the following:

''926D. Carrying of concealed firearms by qualified members of the Armed Forces.''.

SA 2562. Mr. PAUL 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 of the bill, add the following:

SEC. 11. LIMITATION ON FEDERAL FUNDS TO SANCTUARY CITIES.

(a) IN GENERAL.—Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1373) is amended by adding at the end the following:

''(d) LIMITATION ON FEDERAL FUNDS TO SANCTUARY CITIES.—

''(1) SANCTUARY CITY DEFINED.—In this section, the term 'sanctuary city' means a State or subdivision of a State that the Attorney General determines—

''(A) has in effect a statute, policy, or practice that is not in compliance with subsection (a) or (b); or

''(B) does not have a statute, policy, or practice that requires law enforcement officers—

''(i) to notify the U.S. Immigration and Customs Enforcement if the State or unit has custody of an alien without lawful status in the United States and detain the alien for no more than six hours for no other purpose than to determine whether or not U.S. Immigration and Customs Enforcement will issue a detainer request; and

''(ii) to maintain custody of such an alien for a period of not less than 48 hours (excluding Saturdays, Sundays, and holidays) if U.S. Immigration and Customs Enforcement issues a detainer for such alien.

''(2) LIMITATION ON GRANTS.—A sanctuary city shall not be eligible to receive, for a minimum period of at least 1 year, any funds pursuant to—

''(A) the Edward Byrne Memorial Justice Assistance Grant Program established pursuant to subpart 1 of part E of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3750 et seq.);

''(B) the 'Cops' program under part Q of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3796dd et seq.);

''(C) the Urban Area Security Initiative authorized under section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604);

''(D) the State Homeland Security Grant Program authorized under section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605);

''(E) the port security grant program authorized under section 70107 of title 46, United States Code;

''(F) the State Criminal Alien Assistance Program under section 241(i) of the Immigration and Nationality Act (8 U.S.C. 1231(i)); or

''(G) any other non-disaster preparedness grant program administered by the Federal Emergency Management Agency.

''(3) TERMINATION OF INELIGIBILITY.—A jurisdiction that is found to be a sanctuary city shall only become eligible to receive funds under a program set out under paragraph (1) after the Attorney General certifies that the jurisdiction is no longer a sanctuary city.''.

(b) CLERICAL AMENDMENTS.—Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1373) is amended by striking ''Immigration and Naturalization Service'' each place that term appears and inserting ''Department of Homeland Security''.

SEC. 12. TRANSFER OF ALIENS FROM BUREAU OF PRISONS CUSTODY.

(a) TRANSFER TO U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT.—The Attorney General shall prioritize a request from the Secretary of Homeland Security to transfer a covered alien to the custody of U.S. Immigration and Customs Enforcement before a request from the appropriate official of a State or a subdivision of a State to transfer the covered alien to the custody of such State or subdivision.

(b) COVERED ALIEN DEFINED.—In this section, the term ''covered alien'' means an alien who—

(1) is without lawful status in the United States; and

(2) is in the custody of the Bureau of Prisons.

SA 2563. Mr. PAUL 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:

TITLE _____—FEDERAL RESERVE TRANSPARENCY

SEC. __01. SHORT TITLE.

This title may be cited as the ''Federal Reserve Transparency Act of 2015''.

SEC. __02. AUDIT REFORM AND TRANSPARENCY FOR THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM.

(a) IN GENERAL.—Notwithstanding section 714 of title 31, United States Code, or any other provision of law, an audit of the Board of Governors of the Federal Reserve System and the Federal reserve banks under subsection (b) of such section 714 shall be completed within 12 months of the date of enactment of this Act.

(b) REPORT.—

(1) IN GENERAL.—A report on the audit required under subsection (a) shall be submitted by the Comptroller General to the Congress before the end of the 90-day period beginning on the date on which such audit is completed and made available to the Speaker of the House, the majority and minority leaders of the House of Representatives, the majority and minority leaders of the Senate, the Chairman and Ranking Member of the committee and each subcommittee of jurisdiction in the House of Representatives and the Senate, and any other Member of Congress who requests it.

(2) CONTENTS.—The report under paragraph (1) shall include a detailed description of the findings and conclusion of the Comptroller General with respect to the audit that is the subject of the report, together with such recommendations for legislative or administrative action as the Comptroller General may determine to be appropriate.

(c) REPEAL OF CERTAIN LIMITATIONS.—Subsection (b) of section 714 of title 31, United States Code, is amended by striking all after ''in writing.''.

(d) TECHNICAL AND CONFORMING AMENDMENT.—Section 714 of title 31, United States Code, is amended by striking subsection (f).

SEC. __03. AUDIT OF LOAN FILE REVIEWS REQUIRED BY ENFORCEMENT ACTIONS.

(a) IN GENERAL.—The Comptroller General of the United States shall conduct an audit of the review of loan files of homeowners in foreclosure in 2009 or 2010, required as part of the enforcement actions taken by the Board of Governors of the Federal Reserve System against supervised financial institutions.

(b) CONTENT OF AUDIT.—The audit carried out pursuant to subsection (a) shall consider, at a minimum—

(1) the guidance given by the Board of Governors of the Federal Reserve System to independent consultants retained by the supervised financial institutions regarding the procedures to be followed in conducting the file reviews;

(2) the factors considered by independent consultants when evaluating loan files;

(3) the results obtained by the independent consultants pursuant to those reviews;

(4) the determinations made by the independent consultants regarding the nature and extent of financial injury sustained by each homeowner as well as the level and type of remediation offered to each homeowner; and

(5) the specific measures taken by the independent consultants to verify, confirm, or rebut the assertions and representations made by supervised financial institutions regarding the contents of loan files and the extent of financial injury to homeowners.

(c) REPORT.—Not later than the end of the 6-month period beginning on the date of the enactment of this Act, the Comptroller General shall issue a report to the Congress containing all findings and determinations made in carrying out the audit required under subsection (a).

SA 2564. Mr. PAUL 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 38, line between lines 19 and 20, insert the following:

(d) EXCEPTION.—This section shall not apply to any private entity that, in the course of monitoring information under section 4(a) or sharing information under section 4(c), breaks a user agreement or privacy agreement with a customer of the private entity.

SA 2565. Mr. PAUL 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 23 and 24, insert the following:

(iv) For inclusion in the unclassified form of this report under paragraph (4) of this subsection, to the greatest extent practicable, the number of United States persons who have been the subject of monitoring authorized under section 4.

(v) For inclusion in the unclassified form of this report under paragraph (4) of this subsection, to the greatest extent practicable, the number of United States persons with respect to whom personal information of or identifying the persons was shared with a Federal entity under this Act.

SA 2566. Mr. PAUL 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 11, line 19, insert ''with an entity or another Federal entity'' after ''indicator''.

SA 2567. Mr. PAUL 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 of section 8, add the following:

(n) PRESERVATION OF PRIVACY LAW.—Notwithstanding any other provision of this Act, nothing in this Act shall supersede any provision of law as it relates to the retention by a Federal entity of personal information of or identifying a specific United States person.

SA 2568. Mr. PAUL 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 45, line 4, add ''Nothing in this Act shall be construed to prohibit or limit the disclosure of such information to the Privacy and Civil Liberties Oversight Board.'' after ''law.''.

SA 2569. Mr. PAUL 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. _____. RULE OF CONSTRUCTION.

Nothing in this Act or amendments made by this Act shall be construed as permitting the Federal Government to access communications content outside of networks of the Federal Government, including e-mail and messaging content, of a person located in the United States without prior court approval.

SA 2570. Mr. PAUL 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. _____. FOURTH AMENDMENT PRESERVATION AND PROTECTION.

(a) SHORT TITLE.—This section may be cited as the ''Fourth Amendment Preservation and Protection Act of 2015''.

(b) FINDINGS.—Congress finds that the right under the Fourth Amendment to the Constitution of the United States of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures is violated when the Federal Government or a State or local government acquires information voluntarily relinquished by a person to another party for a limited business purpose without the express informed consent of the person to the specific request by the Federal Government or a State or local government or a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

(c) DEFINITION.—In this section, the term ''system of records'' means any group of records from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular associated with the individual.

(d) PROHIBITION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Federal Government and a State or local government may not obtain or seek to obtain information relating to an individual or group of individuals held by a third party in a system of records, and no such information shall be admissible in a criminal prosecution in a court of law.

(2) EXCEPTION.—The Federal Government or a State or local government may obtain, and a court may admit, information relating to an individual held by a third party in a system of records if—

(A) the individual whose name or identification information the Federal Government or State or local government is using to access the information provides express and informed consent to the search; or

(B) the Federal Government or State or local government obtains a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

SA 2571. Mr. PAUL 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. _____. CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS TO CONDUCT WARRANTLESS SEARCHES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS.

Section 702(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(b)) is amended—

(1) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting such subparagraphs, as so redesignated, an additional two ems from the left margin;

(2) by striking ''An acquisition'' and inserting the following:

''(1) IN GENERAL.—An acquisition''; and

(3) by adding at the end the following:

''(2) CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS OF UNITED STATES PERSONS.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), no officer or employee of the United States may conduct a search of a collection of communications acquired under this section in an effort to find communications of a particular United States person (other than a corporation).

''(B) CONCURRENT AUTHORIZATION AND EXCEPTION FOR EMERGENCY SITUATIONS.—Subparagraph (A) shall not apply to a search for communications related to a particular United States person if—

''(i) such United States person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105, 304, 703, 704, or 705 of this Act, or under title 18, United States Code, for the effective period of that order;

''(ii) the entity carrying out the search has a reasonable belief that the life or safety of such United States person is threatened and the information is sought for the purpose of assisting that person; or

''(iii) such United States person has consented to the search.''.

SA 2572. Mr. PAUL 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. ___. PROHIBITION ON DATA SECURITY VULNERABILITY MANDATES.

(a) IN GENERAL.—Except as provided in subsection (b), no agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency.

(b) EXCEPTION.—Subsection (a) shall not apply to mandates authorized under the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(c) COVERED PRODUCT DEFINED.—In this section, the term ''covered product'' means any computer hardware, computer software, or electronic device that is made available to the general public.

SA 2573. 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. _____. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

(a) IN GENERAL.—Part II of the Federal Power Act is amended by inserting after section 215 (16 U.S.C. 824o) the following:

''SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

''(a) DEFINITIONS.—In this section:

''(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms 'bulk-power system', 'Electric Reliability Organization', and 'regional entity' have the meanings given those terms in section 215.

''(2) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of those matters.

''(3) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(A) IN GENERAL.—The term 'critical electric infrastructure information' means information related to critical electric infrastructure, or proposed critical electric infrastructure, generated by or provided to the Commission or other Federal agency, other than classified national security information, that is designated as critical electric infrastructure information by the Commission under subsection (c)(2).

''(B) INCLUSIONS.—The term 'critical electric infrastructure information' includes information that qualifies as critical energy infrastructure information under regulations promulgated by the Commission.

''(4) CYBERSECURITY THREAT.—The term ''cybersecurity threat' means the imminent danger of an act that severely disrupts, attempts to severely disrupt, or poses a significant risk of severely disrupting the operation of programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of the bulk-power system.

''(5) ELECTROMAGNETIC PULSE.—The term 'electromagnetic pulse' means 1 or more pulses of electromagnetic energy emitted by

a device capable of disabling or disrupting operation of, or destroying, electronic devices or communications networks, including hardware, software, and data, by means of such a pulse.

''(6) GEOMAGNETIC STORM.—The term 'geomagnetic storm' means a temporary disturbance of the magnetic field of the Earth resulting from solar activity.

''(7) GRID SECURITY EMERGENCY.—The term 'grid security emergency' means the imminent danger of—

''(A) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system; and

''(B) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk-power system, as a result of such act or event.

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

''(b) AUTHORITY TO ADDRESS GRID SECURITY EMERGENCY.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—If the President issues and provides to the Secretary a written directive or determination identifying a cybersecurity threat or grid security emergency, the Secretary may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect the bulk-power system during the cybersecurity threat or grid security emergency.

''(B) RULES.—As soon as practicable but not later than 180 days after the date of enactment of this section, the Secretary shall, after notice and opportunity for comment, establish rules of procedure that ensure that the authority described in subparagraph (A) can be exercised expeditiously.

''(2) NOTIFICATION OF CONGRESS.—If the President issues and provides to the Secretary a written directive or determination under paragraph (1), the President shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, the directive or determination.

''(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Secretary shall, to the extent practicable in light of the nature of the cybersecurity threat or grid security emergency and the urgency of the need for action, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Commission, and other appropriate Federal agencies regarding implementation of the emergency measures.

''(4) APPLICATION.—An order for emergency measures under this subsection may apply to—

''(A) the Electric Reliability Organization;

''(B) a regional entity; or

''(C) any owner, user, or operator of the bulk-power system.

''(5) EXPIRATION AND REISSUANCE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), an order for emergency measures issued under paragraph (1) shall expire not later than 30 days after the issuance of the order.

''(B) EXTENSIONS.—The Secretary may reissue an order for emergency measures issued under paragraph (1) for subsequent periods, not to exceed 30 days for each such period, if the President, for each such period, issues and provides to the Secretary a written directive or determination that the cybersecurity threat or grid security emergency identified under paragraph (1) continues to exist or that the emergency measure continues to be required.

''(6) COST RECOVERY FOR CRITICAL ELECTRIC INFRASTRUCTURE.—If the Commission determines that owners, operators, or users of the critical electric infrastructure have incurred substantial costs to comply with an order for emergency measures issued under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission may, after notice and an opportunity for comment, prescribe standards for a public utility to seek to recover such costs by filing a rate schedule or tariff pursuant to section 205 for sales of electric energy or the transmission of electric energy subject to the jurisdiction of the Commission.

''(7) TEMPORARY ACCESS TO CLASSIFIED INFORMATION.—The Secretary, and other appropriate Federal agencies, shall, to the extent practicable and consistent with the obligations of the Secretary and Federal agencies to protect classified information, provide temporary access to classified information related to a cybersecurity threat or grid security emergency for which emergency measures are issued under paragraph (1) to key personnel of any entity subject to the emergency measures to enable optimum communication between the entity and the Secretary and other appropriate Federal agencies regarding the cybersecurity threat or grid security emergency.

''(c) PROTECTION AND SHARING OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(1) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE.—Critical electric infrastructure information—

''(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

''(B) shall not be made available by any State, political subdivision, or tribal authority pursuant to any State, political subdivision, or tribal law requiring disclosure of information or records.

''(2) DESIGNATION AND SHARING OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Not later than 1 year after the date of enactment of this section, the Commission, in consultation with the Secretary, shall promulgate such regulations and issue such orders as necessary—

''(A) to designate critical electric infrastructure information;

''(B) to prohibit the unauthorized disclosure of critical electric infrastructure information; and

''(C) to ensure there are appropriate sanctions in place for Commissioners, officers, employees, or agents of the Commission who knowingly and willfully disclose critical electric infrastructure information in a manner that is not authorized under this section.

''(3) CONSIDERATIONS.—In promulgating regulations and issuing orders under paragraph (2), the Commission shall take into consideration the role of State commissions in—

''(A) reviewing the prudence and cost of investments;

''(B) determining the rates and terms of conditions for electric services; and

''(C) ensuring the safety and reliability of the bulk-power system and distribution facilities within the respective jurisdictions of the State commissions.

''(4) NO REQUIRED SHARING OF INFORMATION.—Nothing in this section requires a person or entity in possession of critical electric infrastructure information to share the information with Federal, State, local, or tribal authorities, or any other person or entity.

''(5) DISCLOSURE OF NONCRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—In carrying out this section, the Commission shall segregate critical electric infrastructure information within documents and electronic communications, wherever feasible, to facilitate disclosure of information that is not designated as critical electric infrastructure information.

''(d) SECURITY CLEARANCES.—

''(1) IN GENERAL.—The Secretary shall facilitate and, to the extent practicable, expedite the acquisition of adequate security clearances by key personnel of any entity subject to this section, to enable optimum communication with Federal agencies regarding threats to the security of the critical electric infrastructure.

''(2) SHARING.—The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with the obligations of the Secretary, Commission, and Federal agencies to protect classified and critical electric infrastructure information, share timely actionable information regarding grid security with appropriate key personnel of owners, operators, and users of the critical electric infrastructure.

''(e) CLARIFICATIONS OF LIABILITY.—

''(1) IN GENERAL.—Except as provided in paragraph (3), to the extent any action or omission taken by an entity that is necessary to comply with an order for emergency measures issued under subsection (b)(1), including any action or omission taken to voluntarily comply with the order, results in noncompliance with, or causes the entity not to comply with, any rule, order, regulation, or provision of this Act, including any reliability standard approved by the Commission pursuant to section 215, the action or omission shall not be considered a violation of the rule, order, regulation, or provision.

''(2) RELATIONSHIP TO OTHER LAW.—Except as provided in paragraph (3), an action or omission taken by an owner, operator, or user of the bulk-power system to comply with an order for emergency measures issued under subsection (b)(1) shall be treated as an action or omission taken to comply with an order issued under section 202(c) for purposes of section 215.

''(3) ADMINISTRATION.—Nothing in this subsection requires dismissal of a cause of action against an entity that, in the course of complying with an order for emergency measures issued under subsection (b)(1) by taking an action or omission for which the entity would be liable but for paragraph (1) or (2), takes the action or omission in a grossly negligent manner.''.

(b) CONFORMING AMENDMENTS.—Section 201 of the Federal Power Act (16 U.S.C. 824) is amended by inserting ''215A,'' after ''215,'' each place it appears in subsections (b)(2) and (e).

SA 2574. Mr. HATCH 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—LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT

SEC. 201. SHORT TITLE.

This title may be cited as the ''The Law Enforcement Access to Data Stored Abroad Act''.

SEC. 202. FINDINGS.

Congress finds the following:

(1) The Electronic Communications Privacy Act of 1986 (Public Law 99–508; 100 Stat. 1848) (referred to in this section as ''ECPA'') was intended to protect the privacy of electronic communications stored with providers of electronic communications services and remote computing services, while balancing the legitimate needs of law enforcement to access records stored by such providers.

(2) To strike this balance, ECPA authorized governmental entities to obtain certain categories of communications data from providers using established, pre-existing forms of process—warrants and subpoenas. It also created a new form of court order, in section 2703(d) of title 18, United States Code, that governmental entities could use to obtain additional types of communications data.

(3) It has been well established that courts in the United States lack the power to issue warrants authorizing extraterritorial searches and seizures, and neither ECPA nor subsequent amendments extended the warrant power of courts in the United States beyond the territorial reach of the United States.

(4) Nevertheless, Congress also recognizes the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications relevant to criminal investigations related to United States persons wherever that content may be stored. Therefore, this title authorizes the use of search warrants extraterritorially only where the Government seeks to obtain the contents of electronic communications belonging to a United States person.

SEC. 203. SCOPE AND CLARIFICATION OF WARRANT REQUIREMENT.

(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended—

(1) in section 2702(a), by amending paragraph (3) to read as follows:

''(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.'';

(2) in section 2703—

(A) by striking subsections (a) and (b) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. Subject to subsection (b), a warrant issued pursuant to this subsection may be used to require the disclosure of contents of a wire or electronic communication that are in the provider's electronic storage within the United States or otherwise stored, held, or maintained within the United States by the provider.

''(b) WARRANT REQUIREMENTS.—A warrant issued under subsection (a) may require the disclosure of the contents of a wire or electronic communication, regardless of where such contents may be in electronic storage or otherwise stored, held, or maintained by the provider, if the account-holder whose contents are sought by the warrant is a United States person. A court issuing a warrant pursuant to this subsection, on a motion made promptly by the service provider, shall modify or vacate such warrant if the court finds that the warrant would require the provider of an electronic communications or remote computing service to violate the laws of a foreign country.'';

(B) in subsection (d), in the first sentence—

(i) by striking ''(b) or'';

(ii) by striking ''the contents of a wire or electronic communication, or''; and

(iii) by striking ''sought, are'' and inserting ''sought are''; and

(C) by adding at the end the following:

''(h) RULE OF CONSTRUCTION.—Nothing in this section or in section 2702 shall be construed to limit the authority of a governmental entity to use an administrative subpoena authorized under a Federal or State statute or to use a Federal or State grand jury, trial, or civil discovery subpoena to—

''(1) require an originator, addressee, or intended recipient of an electronic communication to disclose the contents of the electronic communication to the governmental entity; or

''(2) require an entity that provides electronic communication services to the officers, directors, employees, or agents of the entity (for the purpose of carrying out their duties) to disclose the contents of an electronic communication to or from an officer, director, employee, or agent of the entity to a governmental entity, if the electronic communication is held, stored, or maintained on an electronic communications system owned or operated by the entity.

''(i) NOTICE.—Except as provided in section 2705, not later than 10 business days after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

''(1) a copy of the warrant; and

''(2) notice that informs the customer or subscriber—

''(A) of the nature of the law enforcement inquiry with reasonable specificity; and

''(B) that information maintained for the customer or subscriber by the provider of electronic communication service or remote computing service named in the process or request was supplied to, or requested by, the governmental entity.'';

(3) in section 2704(a)(1), by striking ''section 2703(b)(2)'' and inserting ''section 2703'';

(4) in section 2705—

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

''(1) A governmental entity that is seeking a warrant under section 2703 may include in the application for the warrant a request, which the court shall grant, for an order delaying the notification required under section 2703(i) for a period of not more than 90 days, if the court determines that there is reason to believe that notification of the existence of the warrant may have an adverse result described in paragraph (2) of this subsection.''; and

(B) in subsection (b), in the matter preceding paragraph (1), by striking ''under section 2703(b)(1)''; and

(5) in section 2711—

(A) in paragraph (3)(B) by striking ''warrants; and'' and inserting ''warrants'';

(B) in paragraph (4) by striking ''thereof.'' and inserting ''thereof; and''; and

(C) by adding at the end the following:

''(5) the term 'United States person' means a citizen or permanent resident alien of the United States, or an entity or organization organized under the laws of the United States or a State or political subdivision thereof.''.

SEC. 204. MUTUAL LEGAL ASSISTANCE TREATY REFORMS.

(a) MUTUAL LEGAL ASSISTANCE TREATY TRANSPARENCY AND EFFICIENCY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall establish—

(A) a form for use by a foreign government filing a mutual legal assistance treaty request (referred to in this section as an ''MLAT request''), which shall—

(i) be made available on the website of the Department of Justice; and

(ii) require sufficient information and be susceptible for use by a foreign government to provide all the information necessary for the MLAT request; and

(B) an online docketing system for all MLAT requests, which shall allow a foreign government to track the status of an MLAT request filed by the foreign government.

(2) ANNUAL PUBLICATION.—Beginning not later than 1 year after the date of enactment of this Act, and each year thereafter, the Attorney General shall publish on the website of the Department of Justice statistics on—

(A)(i) the number of MLAT requests made by the Department of Justice to foreign governments for the purpose of obtaining the contents of an electronic communication or other information or records from a provider of electronic communications or remote computing services; and

(ii) the average length of time taken by foreign governments to process the MLAT requests described in clause (i); and

(B)(i) the number of MLAT requests made to the Department of Justice by foreign governments for the purpose of obtaining the contents of an electronic communication or other information or records from a provider of electronic communications or remote computing services; and

(ii) the average length of time taken by the Department of Justice to process the MLAT requests described in clause (i).

(3) NOTICE TO DEPARTMENT OF STATE.—The Attorney General shall notify the Secretary of State not later than 7 days after the date on which disclosure of electronic communications content to a foreign government is made pursuant to an MLAT request.

(b) PRESERVATION OF RECORDS.—The Attorney General may issue a request pursuant to section 2703(f) of title 18, United States Code, upon receipt of an MLAT request that appears to be facially valid.

(c) NOTIFICATION TO PROVIDER OF MLAT REQUEST.—When the Attorney General makes use of the process provided in section 2703 of title 18, United States Code, to obtain information from an electronic communications provider or a remote computing provider based on an MLAT request, the Attorney General shall notify that provider in writing that the request has been made pursuant to a mutual legal assistance treaty.

SEC. 205. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) data localization requirements imposed by foreign governments on data providers are—

(A) incompatible with the borderless nature of the Internet;

(B) an impediment to online innovation; and

(C) unnecessary to meet the needs of law enforcement; and

(2) the Department of Justice, the Department of State, and the United States Trade Representatives should pursue open data flow policies with foreign nations.

SA 2575. Ms. HIRONO 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:

On page 38, strike lines 7, 8, and 9, and insert the following:

(A) the date on which the interim policies and procedures are submitted to Congress under section 5(a)(1) and guidelines are submitted to Congress under section 5(b)(1); or

---

SA 2576. Mr. MARKEY 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 51, strike line 8 and insert the following:

SEC. 10. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended—

(1) in section 30102(a)—

(A) by redesignating paragraphs (4) through (11) as paragraphs (10) through (17), respectively;

(B) by redesignating paragraphs (1) through (3) as paragraphs (4) through (6), respectively;

(C) by inserting before paragraph (3), as redesignated, the following:

''(1) 'Administrator' means the Administrator of the National Highway Traffic Safety Administration;

''(2) 'Commission' means the Federal Trade Commission;

''(3) 'critical software systems' means software systems that can affect the driver's control of the vehicle movement;''; and

(D) by inserting after paragraph (6), as redesignated, the following:

''(7) 'driving data' include, but are not limited to, any electronic information collected about—

''(A) a vehicle's status, including, but not limited to, its location or speed; and

''(B) any owner, lessee, driver, or passenger of a vehicle;

''(8) 'entry points' include, but are not limited to, means by which—

''(A) driving data may be accessed, directly or indirectly; or

''(B) control signals may be sent or received either wirelessly or through wired connections;

''(9) 'hacking' means the unauthorized access to electronic controls or driving data, either wirelessly or through wired connections;''; and

(2) by adding at the end the following:

''§ 30129. Cybersecurity standards

''(a) CYBERSECURITY STANDARDS.—

''(1) REQUIREMENT.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to section 10(b)(2) of the Cybersecurity Information Sharing Act of 2015 shall comply with the cybersecurity standards set forth in paragraphs (2) through (4).

''(2) PROTECTION AGAINST HACKING.—

''(A) IN GENERAL.—All entry points to the electronic systems of each motor vehicle manufactured for sale in the United States shall be equipped with reasonable measures to protect against hacking attacks.

''(B) ISOLATION MEASURES.—The measures referred to in subparagraph (A) shall incorporate isolation measures to separate critical software systems from noncritical software systems.

''(C) EVALUATION.—The measures referred to in subparagraphs (A) and (B) shall be evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.

''(D) ADJUSTMENT.—The measures referred to in subparagraphs (A) and (B) shall be adjusted and updated based on the results of the evaluation described in subparagraph (C).

''(3) SECURITY OF COLLECTED INFORMATION.—All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access—

''(A) while such data are stored onboard the vehicle;

''(B) while such data are in transit from the vehicle to another location; and

''(C) in any subsequent offboard storage or use.

''(4) DETECTION, REPORTING, AND RESPONDING TO HACKING.—Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.

''(b) PENALTIES.—A person that violates this section is liable to the United States Government for a civil penalty of not more than $5,000 for each violation in accordance with section 30165.''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue a Notice of Proposed Rulemaking to carry out section 30129 of title 49, United States Code, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section 30129 of title 49, United States Code, as added by subsection (a).

(3) UPDATES.—Not later than 3 years after final regulations are issued pursuant to paragraph (2) and not less frequently than once every 3 years thereafter, the Administrator, after consultation with the Commission, shall—

(A) review the regulations issued pursuant to paragraph (2); and

(B) update such regulations, as necessary.

(c) CLERICAL AMENDMENT.—The table of sections for chapter 301 of title 49, United States Code, is amended by striking the item relating to section 30128 and inserting the following:

''30128. Vehicle rollover prevention and crash mitigation.
''30129. Cybersecurity standards.''.

(d) CONFORMING AMENDMENT.—Section 30165(a)(1) of title 49, United States Code, is amended by inserting ''30129,'' after ''30127,''.

SEC. 11. CYBER DASHBOARD.

(a) IN GENERAL.—Section 32302 of title 49, United States Code, is amended by inserting after subsection (b) the following:

''(c) CYBER DASHBOARD.—

''(1) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to section 11(b)(2) of the Cybersecurity Information Sharing Act of 2015 shall display a 'cyber dashboard', as a component of the label required to be affixed to each motor vehicle under section 32908(b).

''(2) FEATURES.—The cyber dashboard required under paragraph (1) shall inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements set forth in section 30129 of this title and in section 27 of the Federal Trade Commission Act.''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall prescribe regulations for the cybersecurity and privacy information required to be displayed under section 32302(c) of title 49, United States Code, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section 32302 of title 49, United States Code, as added by subsection (a).

(3) UPDATES.—Not less frequently than once every 3 years, the Administrator, after consultation with the Commission, shall—

(A) review the regulations issued pursuant to paragraph (2); and

(B) update such regulations, as necessary.

SEC. 12. PRIVACY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—The Federal Trade Commission Act (15 U.S.C. 41 et seq.) is amended by inserting after section 26 (15 U.S.C. 57c–2) the following:

''SEC. 27. PRIVACY STANDARDS FOR MOTOR VEHICLES.

''(a) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to subsection (e) shall comply with the features required under subsections (b) through (d).

''(b) TRANSPARENCY.—Each motor vehicle shall provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle.

''(c) CONSUMER CONTROL.—

''(1) IN GENERAL.—Subject to paragraphs (2) and (3), owners or lessees of motor vehicles shall be given the option of terminating the collection and retention of driving data.

''(2) ACCESS TO NAVIGATION TOOLS.—If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data under paragraph (1), the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.

''(3) EXCEPTION.—Paragraph (1) shall not apply to driving data stored as part of the electronic data recorder system or other safety systems on-board the motor vehicle that are required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.

''(d) LIMITATION ON USE OF PERSONAL DRIVING INFORMATION.—

''(1) IN GENERAL.—A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.

''(2) REQUESTS.—Consent requests under paragraph (1)—

''(A) shall be clear and conspicuous;

''(B) shall be made in clear and plain language; and

''(C) may not be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.

''(e) ENFORCEMENT.—A violation of this section shall be treated as an unfair and deceptive act or practice in violation of a rule prescribed under section 18(a)(1)(B).''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Commission, after consultation with the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ''Administrator''), shall prescribe regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Commission, after consultation with the Administrator, shall issue final regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act, as added by subsection (a).

(3) UPDATES.—Not less frequently than once every 3 years, the Commission, after consultation with the Administrator, shall—

(A) review the regulations prescribed pursuant to paragraph (2); and

(B) update such regulations, as necessary.

SEC. 13. CONFORMING AMENDMENTS.

SA 2577. Mr. MARKEY 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 17, between lines 18 and 19, insert the following:

(B) PROHIBITION ON USE FOR PURPOSES OTHER THAN CYBERSECURITY PURPOSES.—A private entity may not use a cyber threat indicator or a defensive measure received under this section for any other purpose than as authorized in subparagraph (A), including for commercial, marketing, and sales purposes not authorized in subparagraph (A).

SA 2578. Mr. VITTER (for himself and Mr. TESTER) 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 UPDATE OF GUIDANCE REGARDING SECURITY CLEARANCES FOR CERTAIN SENATE EMPLOYEES.

(a) DEFINITIONS.—In this section—

(1) the term ''covered committee of the Senate'' means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate;

(D) the Subcommittee on State, Foreign Operations, and Related Programs of the Committee on Appropriations of the Senate;

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

(F) the Committee on the Judiciary of the Senate;

(2) the term ''covered Member of the Senate'' means a Member of the Senate who serves on a covered committee of the Senate; and

(3) the term ''Senate employee'' means an employee whose pay is disbursed by the Secretary of the Senate.

(b) REVIEW OF PROCEDURES.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), shall—

(A) conduct a review of whether procedures in effect enable 1 Senate employee designated by each covered Member of the Senate to obtain security clearances necessary for access to classified national security information, including top secret and sensitive compartmentalized information, if the Senate employee meets the criteria for such clearances; and

(B) if the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), determines the procedures described in subparagraph (A) are inadequate, issue guidelines on the establishment and implementation of such procedures.

(2) REPORT.—Not later than 90 days after the date of enactment of this Act, the Director of Senate Security shall submit to each covered committee of the Senate a report regarding the review conducted under paragraph (1)(A) and guidance, if any, issued under paragraph (1)(B).

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter—

(1) the rule of the Information Security Oversight Office implementing Standard Form 312, which Members of Congress sign in order to be permitted to access classified information;

(2) the requirement that Members of the Senate satisfy the ''need-to-know'' requirement to access classified information;

(3) the scope of the jurisdiction of any committee or subcommittee of the Senate; or

(4) the inherent authority of the executive branch of the Government, the Office of Senate Security, any Committee of the Senate, or the Department of Defense to determine recipients of all classified information.

SA 2579. Mr. VITTER 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. _____. SMALL BUSINESS CYBER SECURITY OPERATIONS CENTER.

(a) FINDINGS.—Congress finds the following:

(1) The Federal Government has been hit by a barrage of high-profile cyber assaults over the past year, including the attacks on the Office of Personnel Management and the Department of State.

(2) These attacks exposed the most sensitive personal information of millions of Federal employees and their families.

(3) The President has instituted emergency procedures to immediately deploy so-called indicators, or tell-tale signs of cybercrime operations, into agency anti-malware tools.

(4) According to the Federal Bureau of Investigation, small business concerns have lost more than $1,000,000,000 during the period beginning October 2013 and ending June 2015 as a result of cyber corporate account takeover and business email fraud.

(5) The Federal Government leverages the creative genius of small business concerns across the country to accomplish its missions.

(6) The Federal Acquisition Regulations dictates that a percentage of all Federal Government acquisition be set aside for small business concerns.

(7) Over 90 percent of small business concerns use the Internet through the course of their activities to conduct business.

(8) Small business concerns tend to have weaker online security and do not have necessary funding for high-end encryption technology or staff expertise.

(9) Industry reports indicate that 30 percent of cyber attacks target small business concerns and of those businesses that are attacked, 59 percent have no contingency plan, while according to a First Data report, the average cost for a data breach at a small business concern is $36,000 and rising annually.

(10) A 2012 Verizon study shows that in 855 data breaches examined, 71 percent occurred in businesses with fewer than 100 employees.

(11) Small business concerns are increasingly attacked with data breaches and ransomware, where an attacker encrypts the businesses data until a ransom is paid to the attacker.

(12) It is imperative that small business concerns are provided improved secured guidance to limit negative impacts on the economy of the United States.

(13) There is a vast cyber threat facing the business sector of the United States, which poses a direct threat against the national security of the United States, the Department of Defense, private industry, and critical infrastructure components.

(14) The current layer of protection from cyber threats does not exist for small business concerns.

(b) DEFINITIONS.—In this section—

(1) the term ''Center'' means the Small Business Cyber Security Operations Center established under subsection (c);

(2) the term ''cyber lab'' means—

(A) a Joint Cyber Training Lab; and

(B) a facility that works in conjunction with the National Guard Cyber Teams;

(3) the term ''Secretary'' means the Secretary of Homeland Security; and

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

(c) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall begin carrying out a 3-year pilot program to establish a cybersecurity operations center for small business concerns, to be known as the Small Business Cyber Security Operations Center.

(d) PART OF EXISTING CENTER.—The Secretary shall establish the Center as part of and co-locate the Center with a center providing situational awareness information to businesses on the date of enactment of this Act.

(e) DUTIES.—The Center shall—

(1) work with cyber labs to provide realistic scenario based training to network managers and security personnel of small business concerns, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities;

(2) provide periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of—

(A) the Federal Government;

(B) the Business Emergency Operations Center operated by the Federal Emergency Management Agency; and

(C) other technology and cyber research centers, as determined appropriate by the Secretary;

(3) collaborate with private industry, academia, and the Department of Defense to develop a secure business supply chain which is capable of adapting, evolving, and responding to emergent cybersecurity threats;

(4) review and develop the necessary tools to—

(A) facilitate security information flow and mitigation actions;

(B) provide cyber attack sensing, warning, and response services;

(5) place an emphasis on accessibility and relevance to small business concerns; and

(6) review the policy limitations and restrictions on information sharing relating to cybersecurity.

(f) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is authorized to be appropriated to carry out this section $2,000,000 for each of fiscal years 2016 through 2019, to remain available until expended.

(2) OFFSET.—Section 21(a)(4)(C)(vii) of the Small Business Act (15 U.S.C. 648(a)(4)(C)(vii)) is amended—

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

(B) in subclause (II), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(III) $133,000,000 for each of fiscal years 2016 through 2019.''.

SA 2580. 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:

Beginning on page 46, strike line 10 and all that follows through page 47, line 12, and insert the following:

(3) to require a new information sharing relationship between any entity and the Federal Government or another entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act shall be construed to permit the Federal Government—

(1) to require an entity to provide information to the Federal Government or anther entity;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government or another entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another entity.

SA 2581. Mr. COTTON 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 29, strike line 9 and insert the following:

authority regarding a cybersecurity threat; and

(iii) communications between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding a cybersecurity threat;

SA 2582. Mr. FLAKE (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:

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 be in effect during the 6-year period beginning on 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 2583. Ms. BALDWIN 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:

In section 7(a)(2), by striking subparagraph (F) and inserting the following:

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this Act, including—

(i) the number of actions taken by each agency, department, or component of the Federal Government with which the cyber threat indicators were shared;

(ii) the specific purpose under section 5(d)(5)(A) for which the cyber threat indicators were disclosed to, retained by, or used by each agency, department, or component of the Federal Government; and

(iii) the appropriateness of any subsequent retention, use, or dissemination of such cyber threat indicators by a Federal entity under section 5.

In section 7(b)(2)(B), by striking clause (ii) and inserting the following:

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators, including the number of actions taken by each Federal entity and the specific purpose under section 5(d)(5)(A) for which cyber threat indicators were disclosed to, retained by, or used by each Federal entity.

SA 2584. Mr. BLUMENTHAL 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 44, between lines 5 and 6, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $50,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2585. Mr. BLUMENTHAL 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 44, between lines 5 and 6, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2586. Mr. HEINRICH (for himself and Ms. HIRONO) 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 51, strike lines 9 through 19.

SA 2587. Mr. LEAHY 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:

Beginning on page 32, strike line 17 and all that follows through page 33, line 5.

SA 2588. Mrs. BOXER 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 end of section 7, insert the following:

(c) ANNUAL DATA SECURITY CERTIFICATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act and not less frequently than annually thereafter, the Director of the Office of Management and Budget shall certify the adequacy of the security controls utilized by Federal entities to protect information shared or received under this Act.

(2) CONTENTS.—Each certificate issued by the Director under paragraph (1) shall include a description of the adequacy of the security controls of each Federal entity based on—

(A) a review of the annual reports and evaluations submitted under sections 3554(c) and 3555 of title 44, United States Code; and

(B) any additional certification requirements determined necessary by the Director.

(3) ACTIONS IF INADEQUATE SECURITY CONTROLS ARE DETECTED.—

(A) IN GENERAL.—If the Director determines the security controls of a Federal entity are not adequate to protect the information shared or received under this Act, the Director shall submit to such Federal entity, in writing, a notice of the actions the Federal entity shall take in order to ensure that the information is adequately protected.

(B) SCHEDULE AND EXPLANATION.—Not later than 30 days after the date the Director submits a notice under subparagraph (A), the Federal entity shall—

(i) take the actions required by the notice; or

(ii) submit to the Director and the appropriate committees of Congress, in writing, an explanation of why such actions have not been taken and an estimate of the number of days until such actions shall be taken.

(C) APPROPRIATE COMMITTEES OF CONGRESS.—In this paragraph, the term ''appropriate committees of Congress'' means the following:

(i) The Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate.

(ii) The Committee on Homeland Security, the Permanent Select Committee on Intelligence, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

(4) FORM.—Each certification, notice, and explanation required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SA 2589. Mr. MURPHY (for himself and Mr. HATCH) 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. ___. JUDICIAL REDRESS.

(a) SHORT TITLE.—This section may be cited as the ''Judicial Redress Act of 2015''.

(b) EXTENSION OF PRIVACY ACT REMEDIES TO CITIZENS OF DESIGNATED COUNTRIES.—

(1) CIVIL ACTION; CIVIL REMEDIES.—With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under—

(A) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

(B) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

(2) EXCLUSIVE REMEDIES.—The remedies set forth in paragraph (1) are the exclusive remedies available to a covered person under this subsection.

(3) APPLICATION OF THE PRIVACY ACT WITH RESPECT TO A COVERED PERSON.—For purposes of a civil action described in paragraph (1), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in subparagraphs (A) and (B) of paragraph (1).

(4) DESIGNATION OF COVERED COUNTRY.—

(A) IN GENERAL.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a ''covered country'' for purposes of this subsection if—

(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or

(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information.

(B) REMOVAL OF DESIGNATION.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, revoke the designation of a foreign country or regional economic integration organization, or member country of such organization, as a ''covered country'' if the Attorney General determines that such designated ''covered country''—

(i) is not complying with the agreement described under subparagraph (A)(i);

(ii) no longer meets the requirements for designation under subparagraph (A)(ii); or

(iii) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person.

(5) DESIGNATION OF DESIGNATED FEDERAL AGENCY OR COMPONENT.—

(A) IN GENERAL.—The Attorney General shall determine whether an agency or component thereof is a ''designated Federal agency or component'' for purposes of this subsection. The Attorney General shall not designate any agency or component thereof other than the Department of Justice or a component of the Department of Justice without the concurrence of the head of the relevant agency, or of the agency to which the component belongs.

(B) REQUIREMENTS FOR DESIGNATION.—The Attorney General may determine that an agency or component of an agency is a ''designated Federal agency or component'' for purposes of this subsection, if—

(i) the Attorney General determines that information exchanged by such agency with a covered country is within the scope of an agreement referred to in paragraph (4)(A)(i); or

(ii) with respect to a country or regional economic integration organization, or member country of such organization, that has been designated as a ''covered country'' under paragraph (4)(A)(ii), the Attorney General determines that designating such agency or component thereof is in the law enforcement interests of the United States.

(6) FEDERAL REGISTER REQUIREMENT; NONREVIEWABLE DETERMINATION.—The Attorney General shall publish each determination made under paragraphs (4) and (5). Such determination shall not be subject to judicial or administrative review.

(7) JURISDICTION.—The United States District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this subsection.

(8) DEFINITIONS.—In this section:

(A) AGENCY.—The term ''agency'' has the meaning given that term in section 552(f) of title 5, United States Code.

(B) COVERED COUNTRY.—The term ''covered country'' means a country or regional economic integration organization, or member country of such organization, designated in accordance with paragraph (4).

(C) COVERED PERSON.—The term ''covered person'' means a natural person (other than an individual) who is a citizen of a covered country.

(D) COVERED RECORD.—The term ''covered record'' has the same meaning for a covered person as a record has for an individual under section 552a of title 5, United States Code, once the covered record is transferred—

(i) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and

(ii) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

(E) DESIGNATED FEDERAL AGENCY OR COMPONENT.—The term ''designated Federal agency or component'' means a Federal agency or component of an agency designated in accordance with paragraph (5).

(F) INDIVIDUAL.—The term ''individual'' has the meaning given that term in section 552a(a)(2) of title 5, United States Code.

(9) PRESERVATION OF PRIVILEGES.—Nothing in this subsection shall be construed to waive any applicable privilege or require the disclosure of classified information. Upon an agency's request, the district court shall review in camera and ex parte any submission by the agency in connection with this paragraph.

(10) EFFECTIVE DATE.—This section shall take effect 90 days after the date of the enactment of this Act.

SA 2590. Mr. CARDIN (for himself, Ms. MIKULSKI, Mr. WARNER, Mr. KAINE, 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:

At the appropriate place, insert the following:

SEC. ___. RECOVER ACT.

(a) SHORT TITLE.—This section may be cited as the ''Reducing the Effects of the Cyberattack on OPM Victims Emergency Response Act of 2015'' or the ''RECOVER Act''.

(b) DEFINITION.—In this section, the term ''affected individual'' means any individual whose personally identifiable information was compromised during—

(1) the data breach of personnel records of current and former Federal employees, at a network maintained by the Department of the Interior, that was announced by the Office of Personnel Management on June 4, 2015; or

(2) the data breach of systems of the Office of Personnel Management containing information related to the background investigations of current, former, and prospective Federal employees, and of other individuals.

(c) IDENTITY PROTECTION COVERAGE FOR INDIVIDUALS AFFECTED BY FEDERAL AGENCY DATA BREACHES.—The Office of Personnel Management shall provide to each affected individual complimentary identity protection coverage that—

(1) is not less comprehensive than the complimentary identify protection coverage that the Office provided to affected individuals before the date of enactment of this Act;

(2) is effective for the remainder of the life of the individual; and

(3) includes not less than $5,000,000 in identity theft insurance.

SA 2591. Mr. SANDERS 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—COMMISSION ON PRIVACY RIGHTS IN THE DIGITAL AGE

SEC. 201. SHORT TITLE.

This title may be cited as the ''Commission on Privacy Rights in the Digital Age Act of 2015''.

SEC. 202. FINDINGS.

Congress makes the following findings:

(1) Today, technology that did not exist 30 years ago pervades every aspect of life in the United States.

(2) Nearly ⅔ of adults in the United States own a smartphone, and 43 percent of adults in the United States rely solely on their cell phone for telephone use.

(3) 84 percent of households in the United States own a computer and 73 percent of households in the United States have a computer with an Internet broadband connection.

(4) Federal policies on privacy protection have not kept pace with the rapid expansion of technology.

(5) Innovations in technology have led to the exponential expansion of data collection by both the public and private sectors.

(6) Consumers are often unaware of the collection of their data and how their information can be collected, bought, and sold by private companies.

SEC. 203. PURPOSE.

The purpose of this title is to establish, for a 2-year period, a Commission on Privacy Rights in the Digital Age to—

(1) examine—

(A) the ways in which public agencies and private companies gather data on the people of the United States; and

(B) the ways in which that data is utilized, either internally or externally; and

(2) make recommendations concerning potential policy changes needed to safeguard the privacy of the people of the United States.

SEC. 204. COMPOSITION OF THE COMMISSION.

(a) ESTABLISHMENT.—To carry out the purpose of this title, there is established in the legislative branch a Commission on Privacy Rights in the Digital Age (in this title referred to as the ''Commission'').

(b) COMPOSITION.—The Commission shall be composed of 13 members, as follows:

(1) Five members appointed by the President, of whom—

(A) 2 shall be appointed from the executive branch of the Government; and

(B) 3 shall be appointed from private life.

(2) Two members appointed by the majority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(3) Two members appointed by the minority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(4) Two members appointed by the Speaker of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(5) Two members appointed by the minority leader of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(c) CHAIRPERSON.—The Commission shall elect a Chairperson and Vice-Chairperson from among its members.

(d) MEETINGS; QUORUM; VACANCIES.—

(1) MEETINGS.—After its initial meeting, the Commission shall meet upon the call of the Chairperson or a majority of its members.

(2) QUORUM.—Seven members of the Commission shall constitute a quorum.

(3) VACANCIES.—Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

(e) APPOINTMENT OF MEMBERS; INITIAL MEETING.—

(1) APPOINTMENT OF MEMBERS.—Each member of the Commission shall be appointed not later than 60 days after the date of enactment of this Act.

(2) INITIAL MEETING.—On or after the date on which all members of the Commission have been appointed, and not later than 60 days after the date of enactment of this Act, the Commission shall hold its initial meeting.

SEC. 205. DUTIES OF THE COMMISSION.

The Commission shall—

(1) conduct an investigation of relevant facts and circumstances relating to the expansion of data collection and surveillance practices in the public, private, and national security sectors, including implications for—

(A) constitutional and statutory rights of privacy;

(B) transparency, as it relates to—

(i) government practices;

(ii) consumers; and

(iii) shareholders;

(C) waste, fraud, and abuse; and

(D) the effectiveness of congressional oversight; and

(2) submit to the President and Congress reports containing findings, conclusions, and recommendations for corrective measures relating to the facts and circumstances investigated under paragraph (1), in accordance with section 212.

SEC. 206. POWERS OF THE COMMISSION.

(a) IN GENERAL.—

(1) HEARINGS AND EVIDENCE.—The Commission or, at its direction, any subcommittee or member of the Commission, may, for the purpose of carrying out this title—

(A) hold such hearings, sit and act at such times and places, take such testimony, receive such evidence, and administer such oaths as the Commission or such subcommittee or member determines advisable; and

(B) subject to paragraph (2)(A), require, by subpoena or otherwise, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, documents, tapes, and materials as the Commission or such subcommittee or member determines advisable.

(2) SUBPOENAS.—

(A) ISSUANCE.—

(i) IN GENERAL.—A subpoena may be issued under paragraph (1) only—

(I) by the agreement of the Chairperson and the Vice Chairperson; or

(II) by the affirmative vote of 8 members of the Commission.

(ii) SIGNATURE.—Subject to clause (i), a subpoena issued under paragraph (1) may—

(I) be issued under the signature of—

(aa) the Chairperson; or

(bb) a member designated by a majority of the Commission; and

(II) be served by—

(aa) any person designated by the Chairperson; or

(bb) a member designated by a majority of the Commission.

(B) ENFORCEMENT.—

(i) IN GENERAL.—In the case of contumacy or failure to obey a subpoena issued under paragraph (1), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found, or where the subpoena is returnable, may issue an order requiring such person to appear at any designated place to testify or to produce documentary or other evidence.

(ii) CONTEMPT OF COURT.—Any failure to obey the order of the court under clause (i) may be punished by the court as a contempt of that court.

(3) WITNESS ALLOWANCES AND FEES.—

(A) IN GENERAL.—Section 1821 of title 28, United States Code, shall apply to witnesses requested or subpoenaed to appear at any hearing of the Commission.

(B) SOURCE OF FUNDS.—The per diem and mileage allowances for witnesses shall be paid from funds available to pay the expenses of the Commission.

(b) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriations Acts, enter into

contracts to enable the Commission to discharge its duties under this title.

(c) INFORMATION FROM FEDERAL AGENCIES.—

(1) IN GENERAL.—The Commission may secure directly from any Federal department or agency such information as the Commission considers necessary to carry out this title.

(2) FURNISHING OF INFORMATION.—If the Chairperson, the chairperson of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission submits to a Federal department or agency a request for information under paragraph (1), the head of the department or agency shall, to the extent authorized by law, furnish the information directly to the Commission.

(3) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information furnished under paragraph (2) shall only be received, handled, stored, and disseminated by members of the Commission and its staff consistent with all applicable statutes, regulations, and executive orders.

(d) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall provide to the Commission on a reimbursable basis administrative support and other services for the performance of the Commission's functions.

(2) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance provided under paragraph (1), departments and agencies of the United States may provide to the Commission such services, funds, facilities, staff, and other support services as the departments and agencies may determine advisable and as authorized by law.

(e) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as a department or agency of the United States.

SEC. 207. WHISTLEBLOWER PROTECTION.

(a) DISCHARGE OR DISCRIMINATION PROHIBITED.—No employer may discharge, demote, suspend, threaten, harass, or otherwise discriminate against an employee with respect to the terms and conditions of employment because the employee, or any person acting pursuant to a request of the employee—

(1) commenced, caused to be commenced, or is about to commence or cause to be commenced a proceeding with the Commission under this title;

(2) testified or is preparing to testify in a proceeding described in paragraph (1);

(3) lawfully assisted or is preparing to lawfully assist in any manner in a proceeding described in paragraph (1) or in any other action to carry out the purposes of this title; or

(4) refuses to violate the provisions of this title.

(b) ENFORCEMENT ACTION.—

(1) IN GENERAL.—An employee who alleges discharge or other discrimination by an employer in violation of subsection (a) may seek relief under subsection (c) by—

(A) filing a complaint with the Secretary of Labor; or

(B) if the Secretary of Labor has not issued a final decision within 180 days of the filing of the complaint and there is no showing that such delay is due to the bad faith of the claimant, bringing an action at law or equity for de novo review in the appropriate district court of the United States, which shall have jurisdiction over such an action without regard to the amount in controversy.

(2) PROCEDURE.—

(A) IN GENERAL.—A complaint filed under paragraph (1)(A) shall be governed under the rules and procedures set forth in section 42121(b) of title 49, United States Code.

(B) EXCEPTION.—Notification made under section 42121(b)(1) of title 49, United States Code, shall be made to any individual named in the complaint and to the employer.

(C) BURDENS OF PROOF.—An action brought under paragraph (1)(B) shall be governed by the legal burdens of proof set forth in section 42121(b) of title 49, United States Code.

(D) STATUTE OF LIMITATIONS.—A complaint under paragraph (1)(A) shall be filed not later than 180 days after the date on which the violation occurs, or after the date on which the employee became aware of the violation.

(E) JURY TRIAL.—A party to an action brought under paragraph (1)(B) shall be entitled to trial by jury.

(c) REMEDIES.—

(1) IN GENERAL.—An employee prevailing in any action under subsection (b)(1) shall be entitled to all relief necessary to make the employee whole.

(2) COMPENSATORY DAMAGES.—Relief for any action under paragraph (1) shall include—

(A) reinstatement with the same seniority status that the employee would have had, but for the discrimination;

(B) the amount of back pay, with interest; and

(C) compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees.

(d) RIGHTS RETAINED BY EMPLOYEE.—Nothing in this section shall be deemed to diminish the rights, privileges, or remedies of any employee under any Federal or State law, or under any collective bargaining agreement.

(e) NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRATION OF DISPUTES.—

(1) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided for in this section may not be waived by any agreement, policy form, or condition of employment, including by a predispute arbitration agreement.

(2) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or enforceable, if the agreement requires arbitration of a dispute arising under this section.

SEC. 208. NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.

(a) IN GENERAL.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

(b) PUBLIC HEARINGS AND MEETINGS.—The Commission shall—

(1) hold public hearings and meetings to the extent appropriate; and

(2) conduct public hearings and meetings in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or executive order.

SEC. 209. STAFF OF COMMISSION.

(a) IN GENERAL.—

(1) APPOINTMENT AND COMPENSATION.—The Chairperson, in consultation with the Vice Chairperson and in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of an executive director and such other personnel as may be necessary to enable the Commission to carry out the functions of the Commission, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of that title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this paragraph may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) PERSONNEL AS FEDERAL EMPLOYEES.—

(A) IN GENERAL.—The executive director and any personnel of the Commission who are employees shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, 89A, 89B, and 90 of that title.

(B) MEMBERS OF COMMISSION.—Subparagraph (A) shall not be construed to apply to members of the Commission.

(b) DETAILEES.—Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

(c) CONSULTANT SERVICES.—The Commission may procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of that title.

SEC. 210. COMPENSATION AND TRAVEL EXPENSES.

(a) COMPENSATION.—Each member of the Commission who is not an officer or employee of the Federal Government may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

SEC. 211. SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.

The appropriate departments or agencies of the Federal Government shall cooperate with the Commission in expeditiously providing to the members and staff of the Commission appropriate security clearances, up to the level of sensitive compartmented information, to the extent possible under applicable procedures and requirements, and no person shall be provided with access to classified information under this title without the appropriate security clearances.

SEC. 212. REPORTS OF COMMISSION; TERMINATION.

(a) INTERIM REPORTS.—The Commission shall submit to the President and Congress, and make publicly available online, interim reports containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

(b) FINAL REPORT.—Not later than 2 years after the date of enactment of this Act, the Commission shall submit to the President and Congress, and make publicly available online, a final report containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

(c) CLASSIFIED INFORMATION.—Each report submitted under subsection (a) or (b) shall be in unclassified form, but may include a classified annex.

(d) TERMINATION.—

(1) IN GENERAL.—The Commission, and all the authorities under this title, shall terminate 60 days after the date on which Commission submits the final report under subsection (b).

(2) ADMINISTRATIVE ACTIVITIES BEFORE TERMINATION.—The Commission may use the 60-

day period referred to in paragraph (1) for the purpose of concluding its activities, including providing testimony to committees of Congress concerning its reports and disseminating the final report.

SEC. 213. FUNDING.

(a) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this title.

(b) DURATION OF AVAILABILITY.—Amounts made available to the Commission under subsection (a) shall remain available until the termination of the Commission.

SA 2592. Mr. PAUL 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. ___. WHISTLEBLOWER REPORTS AND PROTECTION AGAINST RETALIATION.

(a) AUTHORIZATION TO REPORT COMPLAINTS OR INFORMATION.—An employee of or contractor to a Federal entity that has knowledge of the programs and activities authorized under this Act may submit a covered complaint—

(1) to the Comptroller General of the United States;

(2) to the Privacy and Civil Liberties Oversight Board;

(3) to the Select Committee on Intelligence of the Senate;

(4) to the Permanent Select Committee on Intelligence of the House of Representatives; or

(5) in accordance with the process established under section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)).

(b) INVESTIGATIONS AND REPORTS TO CONGRESS.—

(1) IN GENERAL.—The Comptroller General shall investigate a covered complaint submitted pursuant to subsection (a)(1) and shall submit to Congress a report containing the results of the investigation.

(2) AVAILABILITY TO CONGRESS.—A report submitted to Congress under paragraph (1) shall be accessible to all members of Congress.

(c) REQUIREMENT TO PERMIT SUBMISSION.—No Federal entity may promulgate a rule or prohibition on its employees, on contractors of that Federal entity, or on any entity sharing cyber threat indicators or defensive measures with the Federal Government under this Act that prohibits submission of complaints under this section.

(d) PROHIBITION ON RETALIATORY ACTIONS.—Notwithstanding any other provision of law, no officer or employee of a Federal entity shall take any retaliatory action against an employee of or contractor to a Federal entity who seeks to disclose or discloses covered information to—

(1) the Comptroller General;

(2) the Privacy and Civil Liberties Oversight Board;

(3) the Select Committee on Intelligence of the Senate;

(4) the Permanent Select Committee on Intelligence of the House of Representatives; or

(5) the Office of the Inspector General of the Intelligence Community.

(e) ADMINISTRATIVE SANCTIONS.—An officer or employee of a Federal entity who violates subsection (d) shall be subject to administrative sanctions, up to and including termination.

(f) DEFINITIONS.—In this section:

(1) COVERED COMPLAINT.—The term ''covered complaint'' means a complaint or information concerning programs and activities authorized by this Act that an employee or contractor reasonably believes is evidence of—

(A) a violation of any law, rule, or regulation; or

(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(2) COVERED INFORMATION.—The term ''covered information'' means any information (including classified or sensitive information) that an employee or contractor reasonably believes is evidence of—

(A) a violation of any provision of law; or

(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

SA 2593. Mr. DURBIN 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 18, line 24, strike ''records.'' and insert ''records, except disclosure required under any State, tribal, or local law in any criminal prosecution.''.

On page 32, line 17, strike ''Cyber'' and insert ''Except for disclosure of evidence required by law or rule in any criminal prosecution, cyber''.

SA 2594. Mr. DURBIN 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 48, between lines 8 and 9, insert the following:

(3) CONSTRUCTION REGARDING OPERATION OF DEFENSIVE MEASURES AND TORT LIABILITY.—Nothing in this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State that establishes a right of action or remedy for damages to a party other than an entity described in section 4(b)(1) resulting from the operation of a defensive measure under this Act.

SA 2595. Mr. DURBIN 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 35, line 6, strike ''Cyber'' and insert

(i) IN GENERAL.—Cyber

On page 35, between lines 11 and 12, insert the following:

(ii) LIMITATION ON USE IN PROCEEDINGS.—Cyber threat indicators, defensive measures, and any other information provided to the Federal Government under this Act and all evidence derived therefrom may not be received in evidence in any trial, hearing or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or any political subdivision thereof if the sharing, disclosure or use of such cyber threat indicator, defensive measure, or other information was or would be in violation of this Act.

SA 2596. Mr. DURBIN 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 11, line 10, strike ''contravention;'' and insert ''contravention, and instructions to remedy or mitigate such error or contravention, including the destruction of such cyber threat indicator and the cessation of any defensive measures based on such indicator;''.

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

(3) NOTIFICATION AND MITIGATION OF ERROR OR CONTRAVENTION.—

(A) REQUIREMENT TO NOTIFY.—An entity that shares a cyber threat indicator or defensive measure and subsequently determines that such cyber threat indicator or defensive measure was in error or in contravention of the requirements of this Act or another provision of Federal law or policy shall notify each entity with which such indicator or measure was shared of such error or contravention.

(B) REQUIREMENTS FOR RECEIVING ENTITY.—An entity that receives a notice under subparagraph (A)—

(i) shall cease use of such cyber threat indicator or defensive measure;

(ii) shall not further share such indicator or measure; and

(iii) shall provide a similar notice to each other entity with which the receiving entity has shared such indicator or measure.

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

(II) a notification of error or contravention received from a Federal entity or sharing entity pursuant to section 3(b)(1)(C) or section 4(c)(3); or

---

SA 2597. Mrs. SHAHEEN 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:

On page 10, line 8, strike ''and''.

On page 10, line 13, strike the period at the end and insert ''; and''.

On page 10, between lines 13 and 14, insert the following:

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

On page 12, line 13, insert ''the Small Business Administration and'' after ''including''.

SA 2598. 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:

Beginning on page 5, strike line 10 and all that follows through page 52, line 6, and insert the following:

(7) ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

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

(C) EXCLUSION.—The term ''entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(8) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(9) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

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

(11) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

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

(13) MONITOR.—The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(14) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing electric utility services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(16) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

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

SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities;

(2) the timely sharing with relevant entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the sharing with relevant entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government; and

(4) the sharing with entities, if appropriate, of information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats.

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed and promulgated under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying entities that have received a cyber threat indicator from a Federal entity under this Act that is known or determined to be in error or in contravention of the requirements of this Act or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities receiving cyber threat indicators to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators; and

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any personal information of or identifying a specific person not directly related to a cybersecurity threat.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall coordinate with appropriate Federal entities, including the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this Act; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator by the sharing entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity monitoring an information system or providing or receiving a cyber threat indicator under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS BY ENTITIES.—

(A) IN GENERAL.—Consistent with this Act, a cyber threat indicator shared or received under this section may, for cybersecurity purposes—

(i) be used by an entity to monitor—

(I) an information system of the entity; or

(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by an entity subject to—

(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on such cyber threat indicator; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 5(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this Act shall not be directly used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any entity, including an activity relating to monitoring or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(d) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 8(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this Act.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(e) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this Act shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 5. SHARING OF CYBER THREAT INDICATORS WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General, in coordination with the heads of the appropriate Federal entities, shall develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators are shared with the Federal Government by any entity pursuant to section 4(b) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any delay, modification, or any other action that could impede real-time receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the real-time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not directly related to a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this Act; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons

from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators under this Act that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator under this Act; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators in real time with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators shared with the Federal Government through such process.

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 4(b)(2), a cyber threat indicator provided by an entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators provided to the Federal Government under this Act shall be—

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

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

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator to the Federal Government under this Act shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;

(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;

(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in—

(I) section 3559(c)(2)(F) of title 18, United States Code (relating to serious violent felonies);

(II) sections 1028 through 1030 of such title (relating to fraud and identity theft);

(III) chapter 37 of such title (relating to espionage and censorship); and

(IV) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators provided to the Federal Government under this Act shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators provided to the Federal Government under this Act shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information of or identifying specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information of or identifying a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators provided to the Federal Government under this Act may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS ACT.—Clause (i) shall not apply to procedures developed and implemented under this Act.

SEC. 6. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under section 4(a) that is conducted in accordance with this Act.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators under section 4(b) if—

(1) such sharing or receipt is conducted in accordance with this Act; and

(2) in a case in which a cyber threat indicator is shared with the Federal Government, the cyber threat indicator is shared in a manner that is consistent with section

5(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 5(a)(1); or

(B) the date that is 60 days after the date of the enactment of this Act.

(c) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this Act; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the heads of the appropriate Federal entities shall jointly submit and the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a detailed report concerning the implementation of this Act.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 5 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 5(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 3 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this Act.

(E) A review of the type of cyber threat indicators shared with the Federal Government under this Act, including the following:

(i) The degree to which such information may impact the privacy and civil liberties of specific persons.

(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons.

(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 5.

(G) A description of any significant violations of the requirements of this Act by the Federal Government.

(H) A summary of the number and type of entities that received classified cyber threat indicators from the Federal Government under this Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include recommendations for improvements or modifications to the authorities and processes under this Act.

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

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under this Act; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 5 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy shall, in consultation with the Council of Inspectors General on Financial Oversight, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators that have been shared with Federal entities under this Act.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this Act.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SEC. 8. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this Act; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.—Nothing in this Act shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this Act shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this Act shall be construed—

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

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal Government; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act shall be construed to permit the Federal Government—

(1) to require an entity to provide information to the Federal Government;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

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

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act for any use other than permitted in this Act.

(k) FEDERAL PREEMPTION.—

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

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

(l) REGULATORY AUTHORITY.—Nothing in this Act shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this Act;

(2) to establish or limit any regulatory authority not specifically established or limited under this Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this Act shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

SEC. 9. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 10. CONFORMING AMENDMENTS.

(a) PUBLIC INFORMATION.—Section 552(b) of title 5, United States Code, is amended—

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

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

(3) by inserting after paragraph (9) the following:

''(10) information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2015.''.

(b) MODIFICATION OF LIMITATION ON DISSEMINATION OF CERTAIN INFORMATION CONCERNING PENETRATIONS OF DEFENSE CONTRACTOR NETWORKS.—Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following: ''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and such information is shared consistent with the policies and procedures promulgated by the Attorney General under section 5 of the Cybersecurity Information Sharing Act of 2015.''.

SA 2599. 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 14, line 5, strike ''provision of law,'' and insert ''statute or regulation,''.

SA 2600. 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 13, line 6, strike ''provision of law,'' and insert ''statute or regulation,''.

SA 2601. 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 15, strike lines 4 through 10 and insert the following:

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other statute or regulation, an entity may, for a cybersecurity purpose, and in accordance with the provisions of this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

SA 2602. 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 3, line 21, strike ''may'' and insert ''is reasonably likely to''.

SA 2603. Mr. KIRK (for himself and Mrs. GILLIBRAND) 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. ___. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is physically present within a country with which the United States does not have a mutual legal assistance treaty or an extradition treaty;

(2) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or its citizens; and

(3) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) BILATERAL CONSULTATIONS.—The Secretary of State, or designee, shall consult with the appropriate government official of each country in which one or more international cyber criminals are physically present to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that identifies—

(A) the number of international cyber criminals who are located in countries that do not have an extradition treaty or mutual legal assistance treaty with the United States, broken down by country;

(B) the dates on which an official of the Department of State, as a result of this Act, discussed ways to thwart or prosecute international cyber criminals in a bilateral conversation with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited into the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Appropriations of the Senate;

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

(D) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(E) the Committee on Foreign Affairs of the House of Representatives;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives; and

(H) the Committee on Financial Services of the House of Representatives.

SA 2604. Mr. COATS 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 51, strike line 8 and insert the following:

SEC. 10. STUDY ON CYBERSECURITY THREATS TO MOBILE DEVICES.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security shall—

(1) complete a study on cybersecurity threats relating to mobile devices; and

(2) submit a report to Congress that contains the findings of such study and the recommendations developed under subsection (b)(3).

(b) MATTERS STUDIED.—In carrying out the study under subsection (a)(1), the Secretary shall—

(1) assess cybersecurity threats relating to mobile devices;

(2) assess the effect such threats may have on the cyber security of the information systems and networks of the Federal Government (except for the information systems and networks of the Department of Defense and the Intelligence Community); and

(3) develop recommendations for addressing such threats.

SEC. 11. CONFORMING AMENDMENTS.

SA 2605. Ms. WARREN 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. _____. STRENGTHENING PUBLIC NOTIFICATION REQUIREMENTS.

Section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) is amended—

(1) by redesignating paragraphs (1) through (3) as subparagraphs (A) through (C), respectively, and adjusting the margins accordingly;

(2) in the matter preceding subparagraph (A), as so redesignated, by striking ''In furtherance'' and inserting the following:

''(1) IN GENERAL.—In furtherance''; and

(3) by adding at the end the following:

''(2) STANDARDS NOT LIMITED TO UNAUTHORIZED ACCESS OR USE OF SENSITIVE CUSTOMER RECORD OR INFORMATION.—The standards established in accordance with paragraph (1)—

''(A) shall require financial institutions to disclose the unauthorized access to or use of any customer record or information; and

''(B) shall not be limited to only require financial institutions to disclose the unauthorized access to or use of sensitive customer records or information.''.

SA 2606. Ms. WARREN 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. _____. IMPROVING EXPERTISE OF BANKING REGULATORS.

(a) DEFINITIONS.—In this section—

(1) the term ''appropriate Federal banking agency'' has the meaning given that term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813);

(2) the term ''banking regulators'' means—

(A) the appropriate Federal banking agencies; and

(B) the National Credit Union Administration; and

(3) the term ''covered entity'' means any entity that—

(A) is subject to examination by a banking regulator;

(B) has more than $10,000,000,000 in assets.

(b) PARTICIPATION IN EXAMINATION OF COVERED ENTITIES BY SPECIALISTS.—Each banking regulator shall ensure that an information security specialist participates in an examination by the banking regulator of a covered entity not less frequently than once every 3 years.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter the frequency of examinations conducted by a banking regulator.

SA 2607. Ms. WARREN 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. _____. REGULATION AND EXAMINATION OF SERVICE PROVIDERS.

Title II of the Federal Credit Union Act (12 U.S.C. 1781 et seq.) is amended by striking section 206A (12 U.S.C. 1786a) and inserting the following:

''SEC. 206A. REGULATION AND EXAMINATION OF SERVICE PROVIDERS.

''(a) SERVICE PERFORMED BY CONTRACT OR OTHERWISE.—If an insured credit union that is regularly examined or subject to examination by the Board, causes to be performed for itself, by contract or otherwise, any service authorized under this Act, or in the case of a State credit union, any applicable State law, whether on or off its premises—

''(1) such performance, including any cybersecurity practice, shall be subject to regulation and examination by the Board to the same extent as if such services were being performed by the insured credit union itself on its own premises; and

''(2) the insured credit union shall notify the Board of the existence of the service relationship not later than 30 days after the earlier of—

''(A) the date on which the contract is entered into; or

''(B) the date on which the performance of the service is initiated.

''(b) ADMINISTRATION BY THE BOARD.—The Board may issue such regulations and orders as may be necessary to enable the Board to administer and carry out this section and to prevent evasion of this section.''.

SA 2608. Ms. WARREN 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:

On page 39, between lines 12 and 13, insert the following:

(3) to protect an entity from liability for a failure to take action to address a cybersecurity threat or a security vulnerability.

SA 2609. Ms. WARREN 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:

In section 6, after subsection (b), insert the following:

(c) LIABILITY FOR FAILURE TO ACT.—An entity that receives information regarding a cybersecurity threat or a security vulnerability under this Act shall take action to address the threat or vulnerability or the entity may be subject to liability for a failure to act.

SA 2610. Ms. KLOBUCHAR 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. ___. DHS ANNUAL REPORT ON ECONOMIC IMPLICATIONS OF CYBER ATTACKS.

(a) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and once every year thereafter, the Secretary of Homeland Security shall submit to Congress a report detailing the economic impact of cyber attacks during the year for which the report is prepared and the year-to-year trends of the economic impact of cyber attacks, in aggregate form, including—

(1) an estimate of losses (in dollars) as a result of cyber attacks; and

(2) the approximate number of cyber attacks on the networks of private entities that have been reported to the Department of Homeland Security.

(b) PROHIBITION.—Each report submitted under subsection (a) may not include the name, or other identifying information, of any private entity that has experienced a cyber attack.

SA 2611. Ms. KLOBUCHAR 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. ___. GAO REPORT ON IMPLEMENTATION.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the implementation of the information sharing system developed under this Act.

(b) REPORT.—Not later than 1 year after the date on which the information sharing procedures described in this Act are implemented, the Comptroller General shall submit to Congress a report on the study conducted under subsection (a), which shall include an assessment of—

(1) the effectiveness of the information sharing system in sharing cyber threat indicators, including an approximate number of cyber threat indicators shared;

(2) the extent to which the information sharing procedures described in this Act—

(A) are used by private entities; and

(B) are effective at screening out personal information or information that identifies a specific person not directly related to a cybersecurity threat;

(3) the extent to which private entities have implemented procedures to remove personal information or information that identifies a specific person not directly related to a cybersecurity threat prior to sharing cyber threat indicators with a Federal entity, consistent with the requirements of this Act;

(4) the extent to which the Department of Homeland Security has implemented procedures to remove personal information or information that identifies a specific person not directly related to a cybersecurity threat prior to sharing cyber threat indicators with private entities or other Federal entities, consistent with the requirements of this Act; and

(5) the effectiveness of data security implemented by Federal entities that are involved in the sharing of cyber threat indicators.

SA 2612. Mr. FRANKEN (for himself, Mr. LEAHY, and 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:

Beginning on page 3, strike line 21 and all that follows through page 5, line 8, and insert the following:

system that is reasonably likely to result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such information is not otherwise prohibited by law; or

---

SA 2613. Mr. CARPER 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 22, strike lines 13 through 19 and insert the following:

(i) are shared in as close to real time as practicable with all appropriate Federal entities and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements; and

On page 22, line 20, strike ''(iii)'' and insert ''(ii)''.

On page 30, strike lines 4 through 8 and insert the following:

(C) ensures that the appropriate Federal entities receive such cyber threat indicators in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements;

Beginning on page 31, strike line 20 and all that follows through page 32, line 6, and insert the following:

(B) the appropriate Federal entities receive such cyber threat indicators and defensive measures through the process within the Department of Homeland Security in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive such cyber threat indicators and defensive measures shared with the Federal Government through the process in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements.

SA 2614. Mr. CARPER 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:

Strike paragraph (1) of section 4(c) and insert the following:

(1) IN GENERAL.—

(A) SHARING WITH ALL ENTITIES.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government in a manner consistent with section 5(c)(1)(B) a cyber threat indicator or defensive measure.

(B) SHARING WITH FEDERAL ENTITIES.—Except as provided in paragraph (2) and consistent with other applicable laws, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, the Federal Government a cyber threat indicator or defensive measure.

SA 2615. Mr. CARPER 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 22, line 16, insert ''unnecessary'' after ''delay,''.

NOTICE OF INTENT TO OBJECT TO PROCEEDING

I, Senator CHARLES E. GRASSLEY, intend to object to proceeding to the nomination of David Malcolm Robinson to be Assistant Secretary of State (Conflict and Stabilization Operations), PN337; and Coordinator for Reconstruction and Stabilization, PN336, dated August 4, 2015.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ARMED FORCES

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Armed Services be authorized to meet during the session of the Senate on August 4, 2015, at 9:30 a.m.

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

COMMITTTEE ON FINANCE

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to meet during the session of the Senate on August 4, 2015, at 10 a.m., in room SD–215 of the Dirksen Senate Office Building, to conduct a hearing entitled ''A Way Back Home: Preserving Families and Reducing the Need for Foster Care.''

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

COMMITTEE ON FOREIGN RELATIONS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 4, 2015, at 10 a.m., to conduct a hearing entitled ''JCPOA: Non-Proliferations, Inspections, and Nuclear Constraints.''

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

COMMITTEE ON FOREIGN RELATIONS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 4, 2015, at 2:30 p.m., to conduct a hearing entitled ''Nominations.''

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs be authorized to meet during the session of the Senate on August 4,