Calendar No. 462

113TH CONGRESS
2D SESSION

S. 2588

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 10, 2014

Mrs. FEINSTEIN, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Cybersecurity Information Sharing Act of 2014''.

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

SEC. 2. DEFINITIONS.

In this Act:

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

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

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

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

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

(3) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) COUNTERMEASURE.—The term ''countermeasure'' means an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability.

(5) CYBERSECURITY PURPOSE.—The term ''cybersecurity purpose'' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(6) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system

that may 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.

(7) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to indicate, 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;

(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 actual or potential harm caused by an incident, including information exfiltrated

when it is necessary in order to describe a cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(8) ELECTRONIC FORMAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''electronic format'' means information that is shared through electronic mail, an interactive form on an Internet website, or a real time, automated process between information systems.

(B) EXCLUSION.—The term ''electronic format'' does not include voice or video communication.

(9) ENTITY.—

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

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (in-

cluding an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

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

(10) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States, or any component, officer, employee, or agent of such a department or agency.

(11) 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.

(12) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, par-

ish, town, township, village, or other political subdivision of a State.

(13) 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.

(14) 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.

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

(16) PRIVATE ENTITY.—

(A) IN GENERAL.—The term ''private entity'' means any individual or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or

nonprofit entity, including an officer, employee, or agent thereof.

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

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

(18) 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.

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

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

(a) IN GENERAL.—Consistent with the protection of intelligence sources and methods and the protection of 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 appropriate entities;

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

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

(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; and

(B) incorporate, to the greatest extent possible, existing processes and existing roles and responsibilities of Federal and non-Federal enti-

ties for information sharing by the Federal Government, including sector specific information sharing and analysis centers.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, 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) the information systems of such private entity;

(B) the information systems of another entity, upon written consent of such other entity;

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

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

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to authorize the monitoring of information systems other than as provided in this subsection or to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF COUNTERMEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate countermeasures that are applied to—

(A) the information systems of such private entity in order to protect the rights or property of the private entity;

(B) the information systems of another entity upon written consent of such entity to protect the rights or property of such entity; and

(C) the information systems of a Federal entity upon written consent of an authorized representative of such Federal entity to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to authorize the use of countermeasures other than as provided in this subsection or to limit otherwise lawful activity.

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

(1) IN GENERAL.—Notwithstanding any other provision of law, and for the purposes permitted under this Act, an entity may, consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government cyber threat indicators and countermeasures.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to authorize the sharing or receiving of cyber threat indicators or countermeasures other than as provided in this subsection or to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity or Federal entity monitoring information systems, operating countermeasures, or providing or receiving cyber threat indicators or countermeasures under this section shall implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or countermeasures.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity or Federal entity sharing cyber threat indicators pursuant to this Act shall, prior to such sharing, remove any information contained within such indicators that the entity or 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.

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

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

(i) be used by an entity to monitor or operate countermeasures on its information systems, or the information systems 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.

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

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

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), cyber threat indicators shared with a State, tribal, or local department or agency under this section may, with the prior written consent of

the entity sharing such indicators, be used by a State, tribal, or local department or agency for the purpose of preventing, investigating, or prosecuting a computer crime.

(ii) ORAL CONSENT.—If the need for immediate use prevents obtaining written consent, such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators shared with a State, tribal, or local department or agency 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) AUTHORIZATION.—Cyber threat indicators shared with a State, tribal, or local department or agency under this section may, consistent with 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) LIMITATION.—Such cyber threat indicators shall not otherwise be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity.

(e) 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 two or more private entities to exchange or provide cyber threat indicators, or assistance relating to the prevention, investigation, or mitigation of cybersecurity threats, 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 cybersecurity threats to information systems or information that is

stored on, processed by, or transiting an information system; or

(B) communicating or disclosing cyber threat indicators to help prevent, investigate, or mitigate the effects of cybersecurity threats to information systems or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of cyber threat indicators 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 AND COUNTERMEASURES 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 and countermeasures 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, in coordination with the heads of the appropriate Federal entities, shall promulgate final policies and procedures relating to the receipt of cyber threat indicators and countermeasures by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—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, and that are received through the process described in subsection (c)—

(i) are shared in real time and simultaneous with such receipt with all of the appropriate Federal entities;

(ii) are not subject to any delay, interference, 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 process described in subsection (c)—

(i) are shared immediately with all of the appropriate Federal entities;

(ii) are not subject to any unreasonable 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) govern, consistent with this Act, any other applicable laws, 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, 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 an audit capability and 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.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—The Attorney General shall, in coordination with the heads of the appropriate Federal agencies 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 and periodically review 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) CONTENT.—The guidelines developed and reviewed under paragraph (1) 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 establishing—

(i) a process for the timely destruction of 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 if information received pursuant to this section is known by a Federal entity receiving the information not to constitute a cyber threat indicator; and

(E) protect the confidentiality of cyber threat indicators containing personal informa-

tion 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.

(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 countermeasures in an electronic format, 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 countermeasures under this Act in an electronic format that are shared

by a private entity with the Federal Government except—

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

(ii) voluntary or legally compelled participation in an open Federal investigation;

(iii) information received through an automated malware analysis capability operated by the Federal Bureau of Investigation that is designed to ensure that information received through and analysis produced by such capability is also immediately shared through the capability and process developed by the Secretary of Homeland Security under this paragraph;

(iv) communications with a Federal regulatory authority by regulated entities regarding a cybersecurity threat; and

(v) cyber threat indicators or countermeasures shared with a Federal entity as part of a contractual or statutory requirement;

(C) ensures that all of the appropriate Federal entities receive such cyber threat indi-

cators in real time and simultaneous with receipt through the process within the Department of Homeland Security; and

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

(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 cyber threat indicators and countermeasures in an electronic format 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 any entity may share cyber threat indicators and countermeasures through such process with

the Federal Government and that all of the appropriate Federal entities receive such cyber threat indicators and countermeasures in real time and simultaneous 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 and countermeasures shared with the Federal Government through the process created in this subsection.

(5) REPORTS.—

(A) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(i) 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.

(ii) CLASSIFIED ANNEX.—The report required by clause (i) shall be submitted in

unclassified form, but may include a classified annex.

(B) REPORT ON AUTOMATED MALWARE ANALYSIS CAPABILITY.—Not later than 1 year after the date of the enactment of this Act, the Director of the Federal Bureau of Investigation and the Secretary of Homeland Security shall submit to Congress a report on the implementation of the automated malware analysis capability described in paragraph (1)(B)(iii), including an assessment of the feasibility and advisability of transferring the administration and operation of such capability to the Department of Homeland Security.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and countermeasures 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.—A cyber threat indicator or countermeasure 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 such entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and countermeasures 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 cyber threat indicators and countermeasures to the Federal Government under this Act shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decisionmaking official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and countermeasures provided

to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death or serious bodily harm;

(iii) 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

(iv) the purpose of preventing, investigating, or prosecuting an offense arising out of a threat described in clause (ii) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and countermeasures 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 and countermeasures 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 information of, or that identifies, a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Cyber threat indicators and countermeasures 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) LIMITATION.—Cyber threat indicators and countermeasures provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government department or agency to regulate the lawful activities of an entity, including activities relating to monitoring, operation of countermeasures, or sharing of cyber threat indicators.

(iii) EXCEPTION.—Procedures developed and implemented under this Act shall not be considered regulations within the meaning of this subparagraph.

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 subsection (a) of section 4 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 or countermeasures under subsection (c) of section 4 if—

(1) such sharing or receipt is conducted in accordance with this Act; and

(2) in a case in which a cyber threat indicator or countermeasure is shared with the Federal Government in an electronic format, the cyber threat indicator or countermeasure is shared in a manner that is consistent with section 5(c).

(c) GOOD FAITH DEFENSE IN CERTAIN CAUSES OF ACTION.—If a cause of action is not otherwise dismissed or precluded under subsection (a) or (b), a good faith reliance by an entity that the conduct complained of was permitted under this Act shall be a complete defense against any action brought in any court against such entity.

(d) CONSTRUCTION.—Nothing in this section shall be construed to require dismissal of a cause of action against an entity that has engaged in—

(1) gross negligence or wilful misconduct in the course of conducting activities authorized by this Act; or

(2) conduct that is otherwise not in compliance with the requirements of this Act.

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 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 capa-

bility 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—

(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 Fed-

eral Government on privacy and civil liberties of specific persons; and

(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 classified 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 such recommendations as the heads of the appropriate Fed-

eral entities may have 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 shall 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 privacy and civil liberties impact of 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 privacy and civil liberties concerns.

(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, and the Inspector General of the Department of Defense shall jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and countermeasures 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 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.

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

(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 impact 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 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;

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

(5) 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 the Federal Government.

(g) 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

(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.

(h) 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.

(i) 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.

(j) FEDERAL PREEMPTION.—

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

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

(k) 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 any regulatory authority not specifically established under Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under Federal law.

SEC. 9. REPORT ON CYBERSECURITY THREATS.

(a) REQUIREMENT FOR REPORT.—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. Such report 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 non-state 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.

(b) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the mean-

ing given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(c) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

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 adding at the end the following:

''(10) information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2014.''.

(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) 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 countermeasures 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 2014.''.

Calendar No. 462

113TH CONGRESS
2D SESSION

S. 2588

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

JULY 10, 2014

Read twice and placed on the calendar