112TH CONGRESS
2D SESSION

S. 2102

To provide the authority to monitor and defend against cyber threats, to improve the sharing of cybersecurity information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 13, 2012

Mrs. FEINSTEIN (for herself and Ms. MIKULSKI) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To provide the authority to monitor and defend against cyber threats, to improve the sharing of cybersecurity information, 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.

This Act may be cited as the ''Cybersecurity Information Sharing Act of 2012''.

SEC. 2. AFFIRMATIVE AUTHORITY TO MONITOR AND DEFEND AGAINST CYBERSECURITY THREATS.

Notwithstanding chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance

Act of 1978 (50 U.S.C. 1801 et seq.), and the Communications Act of 1934 (47 U.S.C. 151 et seq.), any private entity may—

(1) monitor its information systems and information that is stored on, processed by, or transiting such information systems for cybersecurity threats;

(2) monitor a third party's information systems and information that is stored on, processed by, or transiting such information systems for cybersecurity threats, if the third party lawfully authorizes such monitoring;

(3) operate countermeasures on its information systems to protect its information systems and information that is stored on, processed by, or transiting such information systems; and

(4) operate countermeasures on a third party's information systems to protect the third party's information systems and information that is stored on, processed by, or transiting such information systems, if the third party lawfully authorizes such countermeasures.

SEC. 3. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS AMONG PRIVATE ENTITIES.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, any private entity may disclose lawfully obtained cybersecurity threat indicators to any other private entity.

(b) USE AND PROTECTION OF INFORMATION.—A private entity disclosing or receiving cybersecurity threat indicators pursuant to subsection (a)—

(1) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition;

(2) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators by the disclosing entity, including, if requested, the removal of information that may be used to identify specific persons from such indicators;

(3) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the entity that authorized such sharing; and

(4) may only use, retain, or further disclose such cybersecurity threat indicators for the purpose

of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats.

SEC. 4. CYBERSECURITY EXCHANGES.

(a) DESIGNATION OF CYBERSECURITY EXCHANGES.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall establish—

(1) a process for designating appropriate Federal entities, such as 1 or more Federal cybersecurity centers, and non-Federal entities as cybersecurity exchanges;

(2) procedures to facilitate and encourage the sharing of classified and unclassified cybersecurity threat indicators with designated cybersecurity exchanges and other appropriate Federal entities and non-Federal entities; and

(3) a process for identifying certified entities to receive classified cybersecurity threat indicators in accordance with paragraph (2).

(b) PURPOSE.—The purpose of a cybersecurity exchange is to efficiently receive and distribute cybersecurity threat indicators as provided in this Act.

(c) REQUIREMENT FOR A LEAD FEDERAL CYBERSECURITY EXCHANGE.—

(1) IN GENERAL.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall designate a Federal entity as the lead cybersecurity exchange to serve as the focal point within the Federal Government for cybersecurity information sharing among Federal entities and with non-Federal entities.

(2) RESPONSIBILITIES.—The lead cybersecurity exchange designated under paragraph (1) shall—

(A) receive and distribute cybersecurity threat indicators in accordance with this Act;

(B) facilitate information sharing, interaction, and collaboration among and between—

(i) Federal entities;

(ii) State, local, tribal, and territorial governments;

(iii) private entities;

(iv) academia;

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

(vi) other cybersecurity exchanges;

(C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems;

(D) coordinate with other Federal and non-Federal entities, as appropriate, to integrate information from Federal and non-Federal entities, including Federal cybersecurity centers, non-Federal network or security operation centers, other cybersecurity exchanges, and non-Federal entities that disclose cybersecurity threat indicators under section 5(a) to provide situational awareness of the United States information security posture and foster information security collaboration among information system owners and operators;

(E) conduct, in consultation with private entities and relevant Federal and other governmental entities, regular assessments of existing and proposed information sharing models to eliminate bureaucratic obstacles to information sharing and identify best practices for such sharing; and

(F) coordinate with other Federal entities, as appropriate, to compile and analyze information about risks and incidents that threaten information systems, including information voluntarily submitted in accordance with section 5(a) or otherwise in accordance with applicable laws.

(3) SCHEDULE FOR DESIGNATION.—

(A) INITIAL DESIGNATION.—The initial designation of a lead cybersecurity exchange under paragraph (1) shall be made not later than 60 days after the date of the enactment of this Act.

(B) INTERIM DESIGNATION.—The National Cybersecurity and Communications Integration Center of the Department of Homeland Security shall serve as the interim lead cybersecurity exchange until the initial designation is made pursuant to subparagraph (A).

(d) ADDITIONAL FEDERAL CYBERSECURITY EXCHANGES.—In accordance with the process and procedures established in subsection (a), the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, may designate additional existing Federal entities as cybersecurity exchanges, if such cybersecu-

rity exchanges are subject to the requirements for use, retention, and disclosure of information by a cybersecurity exchange under section 5(b) and the special requirements for Federal entities under section 5(g).

(e) REQUIREMENTS FOR NON-FEDERAL CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—In considering whether to designate a non-Federal entity as a cybersecurity exchange to receive cybersecurity threat indicators under section 5(a), and what entity to designate, the Secretary of Homeland Security shall consider the following factors:

(A) The net effect that an additional cybersecurity exchange would have on the overall cybersecurity of the United States.

(B) Whether such designation could substantially improve such overall cybersecurity by serving as a hub for receiving and sharing cybersecurity threat indicators, including the capacity of the non-Federal entity for performing those functions.

(C) The capacity of such non-Federal entity to safeguard cybersecurity threat indicators from unauthorized disclosure and use.

(D) The adequacy of the policies and procedures of such non-Federal entity to protect personally identifiable information from unauthorized disclosure and use.

(E) The ability of the non-Federal entity to sustain operations using entirely non-Federal sources of funding.

(2) REGULATIONS.—The Secretary of Homeland Security may promulgate regulations as may be necessary to carry out this subsection.

(f) CONSTRUCTION WITH OTHER AUTHORITIES.—Nothing in this section may be construed to alter the authorities of a Federal cybersecurity center, unless such cybersecurity center is acting in its capacity as a designated cybersecurity exchange.

(g) NO NEW BUREAUCRACIES.—Nothing in this section may be construed to authorize additional layers of Federal bureaucracy for the receipt and disclosure of cybersecurity threat indicators.

(h) REPORT ON DESIGNATION OF CYBERSECURITY EXCHANGES.—Not later than 90 days after the date the Secretary of Homeland Security designates the initial cybersecurity exchange under this section, the Secretary of Homeland Security, the Director of National Intelligence,

the Attorney General, and the Secretary of Defense shall jointly submit to Congress a written report that—

(1) describes the processes established to designate cybersecurity exchanges under subsection (a);

(2) summarizes the policies and procedures established under section 5(g); and

(3) if none of the cybersecurity exchanges are non-Federal entities, provides recommendations concerning the advisability of designating non-Federal entities as cybersecurity exchanges.

SEC. 5. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS TO A CYBERSECURITY EXCHANGE.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, a non-Federal entity may disclose lawfully obtained cybersecurity threat indicators to a cybersecurity exchange.

(b) USE, RETENTION, AND DISCLOSURE OF INFORMATION BY A CYBERSECURITY EXCHANGE.—Except as provided in subsection (g), a cybersecurity exchange may only use, retain, or further disclose information provided pursuant to subsection (a) in order to protect information systems from cybersecurity threats or mitigate cybersecurity threats.

(c) USE AND PROTECTION OF INFORMATION RECEIVED FROM A CYBERSECURITY EXCHANGE.—A non-Federal entity receiving cybersecurity threat indicators from a cybersecurity exchange—

(1) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition;

(2) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators by the cybersecurity exchange or a third party, if the cybersecurity exchange received such information from the third party, including, if requested, the removal of information that can be used to identify specific persons from such indicators;

(3) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the third party that authorized such sharing; and

(4) may only use, retain, or further disclose such cybersecurity threat indicators for the purpose of protecting an information system or information that is stored on, processed by, or transiting an in-

formation system from cybersecurity threats or mitigating such threats.

(d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall be—

(1) exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable State law; and

(2) treated as voluntarily shared information under section 552 of title 5, United States Code, or any comparable State law.

(e) EXEMPTION FROM EX PARTE LIMITATIONS.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall not be subject to the rules of any governmental entity or judicial doctrine regarding ex parte communications with a decisionmaking official.

(f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) may not be construed to be a waiver of any applicable privilege or protection provided under Federal, State, tribal, or territorial law, including any trade secret protection.

(g) SPECIAL REQUIREMENTS FOR FEDERAL ENTITIES.—

(1) PERMITTED DISCLOSURES.—Notwithstanding any other provision of law and consistent with the requirements of this subsection, a Federal entity that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record, or other information from its electronic communications system, may disclose that communication, record, or other information if—

(A) the disclosure is made for the purpose of—

(i) protecting the information system of a Federal entity from cybersecurity threats; or

(ii) mitigating cybersecurity threats to—

(I) another component, officer, employee, or agent of such Federal entity with cybersecurity responsibilities;

(II) any cybersecurity exchange; or

(III) a private entity that is acting as a provider of electronic commu-

nication services, remote computing service, or cybersecurity services to a Federal entity; and

(B) the recipient of the communication, record, or other information has agreed to comply with such Federal entity's lawful requirements regarding the protection and further disclosure of such information, except to the extent such requirements are inconsistent with the policies and procedures developed by the Secretary of Homeland Security and approved by the Attorney General under paragraph (4).

(2) DISCLOSURE TO LAW ENFORCEMENT.—A cybersecurity exchange that is a Federal entity may disclose cybersecurity threat indicators received pursuant to subsection (a) to a law enforcement entity if—

(A) the information appears to pertain to a crime which has been, is being, or is about to be committed; and

(B) the disclosure is permitted under the procedures developed by the Secretary and approved by the Attorney General under paragraph (4).

(3) FURTHER DISCLOSURE AND USE OF INFORMATION BY A FEDERAL ENTITY.—

(A) AUTHORITY TO RECEIVE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange may receive cybersecurity threat indicators from a cybersecurity exchange pursuant to section 4, but shall only use or retain such cybersecurity threat indicators in a manner that is consistent with this subsection in order—

(i) to protect information systems from cybersecurity threats and to mitigate cybersecurity threats; or

(ii) to disclose such cybersecurity threat indicators to law enforcement pursuant to paragraph (2).

(B) AUTHORITY TO USE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange shall ensure, by written agreement, that if disclosing cybersecurity threat indicators to a non-Federal entity under this section, such non-Federal entity shall use or retain such cybersecurity threat indicators in a manner that is consistent with the requirements in—

(i) section 3(b) on the use and protection of information; and

(ii) paragraph (2) of this subsection.

(4) PRIVACY AND CIVIL LIBERTIES.—

(A) REQUIREMENT FOR POLICIES AND PROCEDURES.—In consultation with privacy and civil liberties experts, the Director of National Intelligence, and the Secretary of Defense, the Secretary of Homeland Security shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of cybersecurity threat indicators by a Federal entity obtained in connection with activities authorized in this Act. Such policies and procedures shall—

(i) minimize the impact on privacy and civil liberties, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats;

(ii) reasonably limit the receipt, retention, use and disclosure of cybersecurity threat indicators associated with specific persons consistent with the need to carry out the responsibilities of this Act, includ-

ing establishing a process for the timely destruction of cybersecurity threat indicators that are received pursuant to this section that do not reasonably appear to be related to protecting information systems from cybersecurity threats and mitigating cybersecurity threats, unless such indicators appear to pertain to a crime which has been, is being, or is about to be committed;

(iii) include requirements to safeguard cybersecurity threat indicators that can be used to identify specific persons from unauthorized access or acquisition; and

(iv) protect the confidentiality of cybersecurity threat indicators associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or disclosed to law enforcement pursuant to paragraph (2).

(B) ADOPTION OF POLICIES AND PROCEDURES.—The head of an agency responsible for a Federal entity designated as a cybersecurity exchange under section 4 shall adopt and comply with the policies and procedures developed under this paragraph.

(C) REVIEW BY THE ATTORNEY GENERAL.—Not later than 1 year after the date of the enactment of this Act, the policies and procedures developed under this subsection shall be reviewed and approved by the Attorney General.

(D) PROVISION TO CONGRESS.—The policies and procedures issued under this Act and any amendments to such policies and procedures shall be provided to Congress.

(5) OVERSIGHT.—

(A) REQUIREMENT FOR OVERSIGHT.—The Secretary of Homeland Security and the Attorney General shall establish a mandatory program to monitor and oversee compliance with the policies and procedures issued under this subsection.

(B) NOTIFICATION OF THE ATTORNEY GENERAL.—The head of each Federal entity that receives information under this Act shall—

(i) comply with the policies and procedures developed by the Secretary of Homeland Security and approved by the Attorney General under paragraph (4);

(ii) promptly notify the Attorney General of significant violations of such policies and procedures; and

(iii) provide the Attorney General with any information relevant to the violation that any Attorney General requires.

(C) ANNUAL REPORT.—On an annual basis, the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Department of Homeland Security, in consultation with the most senior privacy and civil liberties officer or officers of any appropriate agencies, shall jointly submit to Congress a report assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this Act.

(6) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD REPORT.—Not later than two years after the date of the enactment of this Act, 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 activities carried out by the Federal entities under this Act; and

(B) recommendations for improvements to or modifications of the law to address privacy and civil liberties concerns.

(7) SANCTIONS.—The heads of Federal entities shall develop and enforce appropriate sanctions for officers, employees, or agents of the Federal entities who conduct activities under this Act—

(A) outside the normal course of their specified duties;

(B) in a manner inconsistent with the discharge of the responsibilities of such governmental entities; or

(C) in contravention of the requirements, policies and procedures required by this subsection.

SEC. 6. SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.

(a) SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.—The procedures established under section 4(a)(2) shall provide that classified cybersecurity threat indicators may only be—

(1) shared with certified entities;

(2) shared in a manner that is consistent with the need to protect the national security of the United States;

(3) shared with a person with an appropriate security clearance to receive such cybersecurity threat indicators; and

(4) used by a certified entity in a manner that protects such cybersecurity threat indicators from unauthorized disclosure.

(b) REQUIREMENT FOR GUIDELINES.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall issue guidelines providing that appropriate Federal officials may, as the Director considers necessary to carry out this Act—

(1) grant a security clearance on a temporary or permanent basis to an employee of a certified entity;

(2) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; or

(3) expedite the security clearance process for such an employee or entity, if appropriate, in a manner consistent with the need to protect the national security of the United States.

(c) DISTRIBUTION OF PROCEDURES AND GUIDELINES.—Following the establishment of the procedures under section 4(a)(2) and the issuance of the guidelines under subsection (b), the Secretary of Homeland Security and the Director of National Intelligence shall expeditiously distribute such procedures and guidelines to—

(1) appropriate governmental entities and private entities;

(2) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate; and

(3) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 7. LIMITATION ON LIABILITY AND GOOD FAITH DEFENSE FOR CYBERSECURITY ACTIVITIES.

(a) IN GENERAL.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity, and any such action shall be dismissed promptly, based on—

(1) the cybersecurity monitoring activities authorized by paragraph (1) or (2) of section 2; or

(2) the voluntary disclosure of a lawfully obtained cybersecurity threat indicator—

(A) to a cybersecurity exchange pursuant to section 5(a);

(B) by a provider of cybersecurity services to a customer of that provider;

(C) to a private entity or governmental entity that provides or manages critical infrastructure (as that term is used in section 1016 of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c)); or

(D) to any other private entity under section 3(a), if the cybersecurity threat indicator is also disclosed within a reasonable time to a cybersecurity exchange.

(b) GOOD FAITH DEFENSE.—If a civil or criminal cause of action is not barred under subsection (a), good faith reliance that this Act permitted the conduct complained of is a complete defense against any civil or criminal action brought under this Act or any other law.

(c) LIMITATION ON USE OF CYBERSECURITY THREAT INDICATORS FOR REGULATORY ENFORCEMENT ACTIONS.—No Federal entity may use a cybersecurity

threat indicator received pursuant to this Act as evidence in a regulatory enforcement action against the entity that lawfully shared the cybersecurity threat indicator with a cybersecurity exchange that is a Federal entity.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity, and any such action shall be dismissed promptly, for a failure to disclose a cybersecurity threat indicator if—

(1) the Attorney General determines that disclosure of a cybersecurity threat indicator would impede a civil or criminal investigation and submits a written request to delay notification for up to 30 days, except that the Attorney General may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary; or

(2) the Secretary of Homeland Security, the Attorney General, or the Director of National Intelligence determines that disclosure of a cybersecurity threat indicator would threaten national or homeland security and submits a written request to delay notification, except that the Secretary, the Attorney

General, or the Director may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(e) LIMITATION ON LIABILITY FOR FAILURE TO ACT.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any private entity, or any officer, employee, or agent of such an entity, and any such action shall be dismissed promptly, for the reasonable failure to act on information received under this Act.

(f) LIMITATION ON PROTECTIONS.—Any person who knowingly and willfully violates restrictions under this Act shall not receive the protections of this Act.

(g) PRIVATE RIGHT OF ACTION.—Nothing in this Act may be construed to limit liability for a failure to comply with the requirements of section 3(b) and section 5(c) on the use and protection of information.

(h) DEFENSE FOR BREACH OF CONTRACT.—Compliance with lawful restrictions placed on the disclosure or use of cybersecurity threat indicators is a complete defense to any tort or breach of contract claim originating in a failure to disclose cybersecurity threat indicators to a third party.

SEC. 8. CONSTRUCTION AND FEDERAL PREEMPTION.

(a) CONSTRUCTION.—Nothing in this Act may be construed—

(1) to permit the unauthorized disclosure of—

(A) information that has been determined by the Federal Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations;

(B) any restricted data (as that term is defined in paragraph (y) of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014));

(C) information related to intelligence sources and methods; or

(D) information that is specifically subject to a court order or a certification, directive, or other authorization by the Attorney General precluding such disclosure;

(2) to limit or prohibit otherwise lawful disclosures of communications, records, or information by a private entity to a cybersecurity exchange or any other governmental or private entity not conducted under this Act;

(3) to limit the ability of a private entity or governmental entity to receive data about its infor-

mation systems, including lawfully obtained cybersecurity threat indicators;

(4) to authorize or prohibit any law enforcement, homeland security, or intelligence activities not otherwise authorized or prohibited under another provision of law;

(5) 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; or

(6) to prevent a governmental entity from using information not acquired through a cybersecurity exchange for regulatory purposes.

(b) FEDERAL PREEMPTION.—This Act supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the provision of cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this Act.

(c) PRESERVATION OF OTHER STATE LAW.—Except as expressly provided, nothing in this Act shall be con-

strued to preempt the applicability of any other State law or requirement.

(d) NO CREATION OF A RIGHT TO INFORMATION.—The provision of information to a non-Federal entity under this Act may not create a right or benefit to similar information by any other non-Federal entity.

(e) PROHIBITION ON REQUIREMENT TO PROVIDE INFORMATION TO THE FEDERAL GOVERNMENT.—Nothing in this Act may be construed to permit a Federal entity—

(1) to require a non-Federal entity to share information with the Federal Government; or

(2) to condition the disclosure of unclassified or classified cybersecurity threat indicators pursuant to this Act with a non-Federal entity on the provision of cybersecurity threat information to the Federal Government.

(f) LIMITATION ON USE OF INFORMATION.—No cybersecurity threat indicators obtained pursuant to this Act may be used, retained, or disclosed by a Federal entity or non-Federal entity, except as authorized under this Act.

(g) DECLASSIFICATION AND SHARING OF INFORMATION.—Consistent with the exemptions from public disclosure of section 5(d), the Director of National Intelligence, in consultation with the Secretary of Homeland Security, shall facilitate the declassification and sharing of informa-

tion in the possession of a Federal entity that is related to cybersecurity threats, as the Director deems appropriate.

(h) REPORT ON IMPLEMENTATION.—Not later than two years after the date of the enactment of this Act, the Secretary of Homeland Security, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly submit to Congress a report that—

(1) describes the extent to which the authorities conferred by this Act have enabled the Federal Government and the private sector to mitigate cybersecurity threats;

(2) discloses any significant acts of noncompliance by a non-Federal entity with this Act, with special emphasis on privacy and civil liberties, and any measures taken by the Federal Government to uncover such noncompliance;

(3) describes in general terms the nature and quantity of information disclosed and received by governmental entities and private entities under this Act; and

(4) proposes changes to the law, including the definitions, authorities and requirements of this Act, that are necessary to ensure the law keeps pace with the threat while protecting privacy and civil liberties.

(i) REQUIREMENT FOR ANNUAL REPORT.—On an annual basis, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives on the implementation of section 6 of this Act. Such report, which shall be submitted in a classified and in an unclassified form, shall include a list of private entities that receive classified cybersecurity threat indicators under this Act, except that the unclassified report shall not contain information that may be used to identify specific private entities unless such private entities consent to such identification.

SEC. 9. DEFINITIONS.

In this Act:

(1) CERTIFIED ENTITY.—The term ''certified entity'' means a protected entity, a self-protected entity, or a provider of cybersecurity services that—

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect and use classified cybersecurity threat indicators.

(2) COUNTERMEASURE.—The term ''countermeasure'' means automated or manual actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

(3) CYBERSECURITY EXCHANGE.—The term ''cybersecurity exchange'' means any governmental entity or private entity designated by the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to receive and distribute cybersecurity threat indicators under section 4(a).

(4) CYBERSECURITY SERVICES.—The term ''cybersecurity services'' means products, goods, or services intended to detect, mitigate, or prevent cybersecurity threats.

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' means any action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system.

(6) CYBERSECURITY THREAT INDICATOR.—The term ''cybersecurity threat indicator'' means information—

(A) that may be indicative of or describe—

(i) malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(ii) a method of defeating a technical control;

(iii) a technical vulnerability;

(iv) a method of defeating an operational control;

(v) 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 technical control or an operational control;

(vi) malicious cyber command and control;

(vii) the actual or potential harm caused by an incident, including information exfiltrated as a result of subverting a technical control when it is necessary in order to identify or describe a cybersecurity threat;

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

(ix) any combination thereof; and

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat.

(7) FEDERAL CYBERSECURITY CENTER.—The term ''Federal cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Secu-

rity Service Threat Operations Center, or the United States Computer Emergency Readiness Team, or any successor to such a center.

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

(9) GOVERNMENTAL ENTITY.—The term ''governmental entity'' means any Federal entity and agency or department of a State, local, tribal, or territorial government other than an educational institution, or any component, officer, employee, or agent of such an agency or department.

(10) INFORMATION SYSTEM.—The term ''information system'' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including communications with, or commands to, specialized systems such as industrial and process control systems, telephone switching and private branch exchange, and environmental control systems.

(11) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for remote identification

of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system associated with a known or suspected cybersecurity threat.

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

(13) MONITOR.—The term ''monitor'' means the interception, acquisition, or collection of information that is stored on, processed by, or transiting an information system for the purpose of identifying cybersecurity threats.

(14) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' means a private entity or a governmental entity other than a Federal entity.

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

(16) PRIVATE ENTITY.—The term ''private entity'' has the meaning given the term ''person'' in

section 1 of title 1, United States Code, and does not include a governmental entity.

(17) PROTECT.—The term ''protect'' means actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, mitigate cybersecurity threats, or otherwise enhance information security or the resiliency of information systems or assets.

(18) PROTECTED ENTITY.—The term ''protected entity'' means an entity, other than an individual, that contracts with a provider of cybersecurity services for goods or services to be used for cybersecurity purposes.

(19) SELF-PROTECTED ENTITY.—The term ''self-protected entity'' means an entity, other than an individual, that provides cybersecurity services to itself.

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

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

(22) THIRD PARTY.—The term ''third party'' includes Federal entities and non-Federal entities.

○