114TH CONGRESS
1ST SESSION

S. 456

To codify mechanisms for enabling cybersecurity threat indicator sharing between private and government entities, as well as among private entities, to better protect information systems.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 11, 2015

Mr. CARPER introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To codify mechanisms for enabling cybersecurity threat indicator sharing between private and government entities, as well as among private entities, to better protect information systems.

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 ''Cyber Threat Sharing Act of 2015''.

SEC. 2. CYBER THREAT INDICATOR SHARING.

(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. 229. CYBER THREAT INDICATOR SHARING.

''(a) DEFINITIONS.—In this section, the following definitions shall apply:

''(1) CENTER.—The term 'Center' means the national cybersecurity and communications integration center established under the second section designated as section 226.

''(2) CYBER THREAT.—The term 'cyber threat'—

''(A) means any action that may result in—

''(i) unauthorized access in order to damage or impair the integrity, confidentiality, or availability of an information system; or

''(ii) unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system; and

''(B) does not include exceeding authorized access of an information system, if such access

solely involves a violation of consumer terms of service or consumer licensing agreements.

''(3) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information—

''(A) that is necessary to indicate, describe, or identify—

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

''(ii) a method of defeating a technical control or an operational control;

''(iii) a technical vulnerability;

''(iv) 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 inadvertently to enable the defeat of a technical control or an operational control;

''(v) malicious cyber command and control; or

''(vi) any combination of clauses (i) through (v); and

''(B) from which reasonable efforts have been made to remove information that may be used to identify specific persons reasonably believed to be unrelated to the cyber threat.

''(4) FEDERAL ENTITY.—The term 'Federal entity' means—

''(A) an agency or department of the United States; or

''(B) any component, officer, employee, or agent of such an agency or department, acting in his or her official capacity.

''(5) GOVERNMENTAL ENTITY.—The term 'governmental entity' means—

''(A) any Federal entity;

''(B) any agency or department of a State, local, tribal, or territorial government; or

''(C) any component, officer, employee, or agent of such an agency or department, acting in his or her official capacity.

''(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' has the meaning given that term in section 212.

''(7) INFORMATION SYSTEM.—The term 'information system' means a discrete set of hardware

and software information resources that collects, processes, maintains, uses, shares, disseminates, or disposes of information and communications.

''(8) 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 that is known or reasonably suspected of being associated with a known or suspected cyber threat.

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

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

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

''(12) PRIVATE ENTITY.—The term 'private entity'—

''(A) has the meaning given the term 'person' in section 1 of title 1, United States Code; and

''(B) does not include a governmental entity or a foreign government, or any component thereof.

''(13) SECTOR-SPECIFIC AGENCY.—The term 'sector-specific agency' has the meaning given that term in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

''(14) 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 information system or the information processed or stored by that information system.

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

''(b) VOLUNTARY DISCLOSURE AND RECEIPT OF CYBER THREAT INDICATORS.—

''(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may—

''(A) disclose a lawfully obtained cyber threat indicator to—

''(i) a private Information Sharing and Analysis Organization; and

''(ii) the Center; and

''(B) receive a cyber threat indicator disclosed under this section by a Federal or non-Federal entity.

''(2) VOLUNTARY SHARING WITH LAW ENFORCEMENT.—Any entity may disclose a lawfully obtained cyber threat indicator to a Federal entity for investigative purposes consistent with the lawful authorities of the Federal entity.

''(3) USE AND PROTECTION OF INFORMATION.—A private entity that discloses or receives a cyber threat indicator under paragraph (1)—

''(A) may only use, retain, or further disclose the cyber threat indicator for the purpose of—

''(i) protecting an information system or information that is stored on, processed

by, or transiting an information system from cyber threats;

''(ii) identifying or mitigating such cyber threats; or

''(iii) reporting a crime;

''(B) shall take reasonable efforts—

''(i) to minimize information that may be used to identify specific persons and is reasonably believed to be unrelated to a cyber threat; and

''(ii) to safeguard information that may be used to identify specific persons from unintended disclosure and unauthorized access or acquisition; and

''(C) shall comply with reasonable restrictions that a private entity places on the subsequent disclosure or retention of a cyber threat indicator that the private entity discloses to other private entities.

''(4) BEST PRACTICES FOR PRIVATE INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.—The Secretary, in consultation with the Secretary of Commerce, the Attorney General, the Director of the Office of Management and Budget, and the heads of

sector-specific agencies and other appropriate Federal agencies, shall—

''(A) through an open and competitive process, select a private entity to identify a common set of best practices for the creation and operation of private Information Sharing and Analysis Organizations; or

''(B) if necessary, develop through an open and consultative process the common set of best practices described in subparagraph (A).

''(c) FEDERAL CYBER THREAT INDICATOR SHARING.—

''(1) CIVILIAN PORTAL.—The Secretary shall designate the Center to receive and disclose cyber threat indicators to Federal and non-Federal entities in as close to real time as practicable, consistent with, and in accordance with the purposes of, this section.

''(2) SHARING WITH NON-FEDERAL ENTITIES.—

''(A) IN GENERAL.—To protect information systems or information that is stored on, processed by, or transiting an information system from cyber threats, the Secretary shall coordinate Federal efforts to ensure that useful

classified and unclassified cyber threat indicators are shared in a timely manner with non-Federal entities.

"(B) REPORT.—

"(i) IN GENERAL.—Not later than 1 year after the date of enactment of this section, and every year thereafter for 2 years, the Secretary, in consultation with the Attorney General, the Director of the Office of Management and Budget, the Director of National Intelligence, the Secretary of Defense, and the heads of sector-specific agencies and other appropriate Federal agencies, shall submit to Congress a report including—

"(I) a review of all Federal efforts to share classified and unclassified cyber threat indicators to protect information systems from cyber threats, including summaries of the nature of those efforts and the quantities of information shared;

"(II) challenges to the appropriate sharing of cyber threat indicators; and

"(III) recommendations to enhance the appropriate sharing of cyber threat indicators.

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

"(3) SHARING AMONG FEDERAL ENTITIES.—

"(A) IN GENERAL.—The Secretary, in consultation with the heads of appropriate agencies, shall coordinate and establish procedures for the sharing of cyber threat indicators among Federal agencies, with appropriate consideration of privacy and civil liberties and agency equities.

"(B) SHARING BY THE CENTER.—The Secretary, in consultation with the Attorney General, the Director of the Office of Management and Budget, the Director of National Intelligence, the Secretary of Defense, and the heads of sector-specific agencies and other appropriate Federal agencies, shall ensure that cyber threat indicators received and disclosed by the Center under paragraph (1) are shared

with other Federal entities in as close to real time as practicable.

''(4) REAL TIME SHARING.—

''(A) IN GENERAL.—The Secretary, in coordination with the Director of the National Institute for Standards and Technology, and consistent with the Cybersecurity Enhancement Act of 2014 (Public Law 113–274; 128 Stat. 2971), shall develop a program that supports and rapidly advances the development, adoption, and implementation of automated mechanisms for the real time sharing of cyber threat indicators.

''(B) BEST PRACTICES.—To the maximum extent feasible, the Secretary shall ensure that the program developed under subparagraph (A) relies on open source software development best practices.

''(d) LIMITATION OF LIABILITY.—

''(1) LIABILITY FOR DISCLOSURE OF CYBER THREAT INDICATORS.—

''(A) IN GENERAL.—A civil or criminal action may not be filed or maintained in a Federal or State court against an entity for the voluntary disclosure or receipt under this section

of a lawfully obtained cyber threat indicator, that the entity was not otherwise required to disclose, to or from—

"(i) the Center; or

"(ii) a private Information Sharing and Analysis Organization, if the organization maintains a publicly-available self-certification that the organization has adopted the best practices identified or developed under subsection (b)(4).

"(B) EFFECTIVE DATE.—Subparagraph (A) shall take effect on the date on which the policies and procedures are developed under subsection (e)(1).

"(2) PROTECTION FROM PUBLIC DISCLOSURE.—

"(A) IN GENERAL.—A cyber threat indicator that is submitted by a non-Federal entity to the Center shall be exempt from disclosure under—

"(i) section 552(b)(3) of title 5, United States Code;

"(ii) section 552a(d) of title 5, United States Code; and

''(iii) any State law otherwise requiring disclosure.

''(B) APPLICATION OF SECTION 214.—

''(i) IN GENERAL.—Except as provided under clause (ii), a cyber threat indicator that is submitted by a non-Federal entity to the Center shall be treated in the same manner as voluntarily submitted critical infrastructure information is treated under section 214.

''(ii) EXCEPTION.—For purposes of clause (i), the requirements under subsection (a)(2) (regarding an express statement) and subsection (e)(2)(A) (regarding acknowledgment of receipt) of section 214 shall not apply.

''(3) LIMITATION OF REGULATORY ENFORCEMENT ACTIONS.—

''(A) IN GENERAL.—A Federal entity may not use a cyber threat indicator received under this section as evidence in a regulatory enforcement action against an entity that disclosed the cyber threat indicator to the Federal Government under subsection (c).

''(B) EXCEPTION.—Nothing in subparagraph (A) shall be construed to prevent a Federal entity from using a cyber threat indicator received through lawful means other than under this section as evidence in a regulatory enforcement action, even if the Federal entity also receives the cyber threat indicator under this section.

''(4) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit or otherwise limit an Information Sharing and Analysis Organization, information sharing and analysis center, or other non-Federal entity from self-certifying under paragraph (1)(A)(ii) that the entity has adopted the best practices identified or developed under subsection (b)(4).

''(e) PRIVACY PROTECTIONS.—

''(1) POLICIES AND PROCEDURES.—

''(A) IN GENERAL.—The Secretary, in consultation with the Attorney General, the Chief Privacy Officer of the Department, the Chief Privacy and Civil Liberties Officer of the Department of Justice, the Secretary of Commerce, the Director of National Intelligence, the Secretary of Defense, the Director of the Office

of Management and Budget, the heads of sector-specific agencies and other appropriate agencies, and the Privacy and Civil Liberties Oversight Board, shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of a cyber threat indicator obtained by a Federal entity under this section.

''(B) REQUIREMENTS.—The policies and procedures developed under subparagraph (A) shall—

''(i) reasonably limit the acquisition, interception, retention, use, and disclosure of a cyber threat indicator that is reasonably likely to identify specific persons, including by establishing a process—

''(I) for the timely destruction of information that is known not to be directly related to a purpose or use authorized under the section; and

''(II) to anonymize and safeguard information received and disclosed that may be used to identify specific persons unrelated to a cyber threat;

"(ii) except as provided under clause (iii), limit the reception, use, and retention of a cyber threat indicator by a Federal entity only to protect information systems from cyber threats;

"(iii) for cyber threat indicators received by the Center under subsection (c)(1), establish publicly available guidelines that authorize law enforcement use of a cyber threat indicator received by a Federal entity under subsection (c) only to investigate, prosecute, disrupt, or otherwise respond to—

"(I) a computer crime;

"(II) a threat of death or serious bodily harm;

"(III) a serious threat to a minor, including sexual exploitation and threats to physical safety; or

"(IV) an attempt or conspiracy to commit an offense described in subclause (I), (II), or (III);

"(iv) preserve the confidentiality of disclosed proprietary information to the greatest extent practicable, and require re-

cipients of such information to be informed that the cyber threat indicator disclosed may only be used for the purposes authorized under this section; and

''(v) provide for appropriate penalties for any officer, employee, or agent of an agency or department of the United States who violates the provisions of this section with respect to the receipt, retention, or disclosure of a cyber threat indicator.

''(2) OVERSIGHT BY FEDERAL ENTITIES.—The head of each Federal entity that receives or discloses a cyber threat indicator under this section shall establish a program to monitor and oversee compliance with the policies and procedures developed under paragraph (1)(A).

''(3) PUBLICATION.—The policies and procedures developed under paragraph (1)(A) shall—

''(A) be provided to the appropriate congressional committees; and

''(B) to the maximum extent practicable, shall be posted on the Internet website of each Federal entity that receives or discloses a cyber threat indicator under this section.

''(4) REPORTS.—

''(A) ANNUAL REPORT ON PRIVACY AND CIVIL LIBERTIES.—The Chief Privacy Officer of the Department and the Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with the privacy and civil liberties officers of other appropriate Federal agencies, shall submit to Congress an annual report assessing the privacy and civil liberties impact of the governmental activities conducted under this section.

''(B) ADDITIONAL REPORT.—

''(i) IN GENERAL.—Not later than 2 years after the date of enactment of this section, and every year thereafter for 2 years, the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly submit to Congress a report that—

''(I) describes the extent to which the authorities provided under this section have enabled the Federal Government and the private sector to mitigate cyber threats;

''(II) discloses any significant acts of noncompliance by a non-Fed-

eral entity with this section, with special emphasis on privacy and civil liberties, and any measures taken by the Federal Government to uncover such noncompliance;

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

''(IV) describes the uses by Federal agencies of information received under this section, including the general quantity of information being used for each purpose; and

''(V) identifies the emergence of new threats or technologies that challenge the adequacy of this section, including the definitions, authorities, and requirements of this section, for keeping pace with the threat.

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

''(f) CONSTRUCTION AND FEDERAL PREEMPTION.—

''(1) CONSTRUCTION.—Nothing in this section may be construed—

''(A) except as provided in subsection (d)(2), to limit any law or regulation that requires the disclosure, receipt, or retention of information;

''(B) to limit the authority of an entity to share information concerning potential criminal activity or investigations with law enforcement entities;

''(C) to limit or prohibit otherwise lawful disclosures of information by a private entity to any governmental or private entity not conducted under this section;

''(D) to allow the otherwise unauthorized disclosure by a private entity of information or material that has been determined by the Federal Government pursuant to an Executive order, statute, or regulation to require protection against unauthorized disclosure for reasons of national defense or foreign relations of the United States, including—

''(i) any restricted data, as defined in section 11(y) of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y));

''(ii) information related to intelligence sources and methods; and

''(iii) information that is specifically subject to a court order or a certification, directive, or other authority precluding such disclosure;

''(E) to authorize or limit liability for actions that would—

''(i) violate the Report and Order of the Federal Communications Commission with regard to Preserving the Open Internet; Broadband Industry Practices (GN Docket No. 09–191, WC Docket No. 07–52) (adopted December 21, 2010) or any successor Report or Order thereto; or

''(ii) modify or alter the obligations of private entities under Report or Order described in clause (i); or

''(F) to allow price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting or exchanges of price or cost information, cus-

tomer lists, or information regarding future competitive planning.

''(2) FEDERAL PREEMPTION.—This section supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the retention, use, or disclosure of a cyber threat indicator by a private entity.

''(3) PRESERVATION OF OTHER STATE LAW.—Except as expressly provided, nothing in this section shall be construed to preempt the applicability of any other State law or requirement.

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

''(5) NO WAIVER OF PRIVILEGE.—No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this section shall lose its privileged character.

''(6) PROHIBITION ON REQUIREMENT TO PROVIDE INFORMATION TO THE FEDERAL GOVERNMENT.—Nothing in this section shall be construed to authorize a Federal entity—

''(A) to require a non-Federal entity to share information with the Federal Government;

''(B) to condition the disclosure of a cyber threat indicator under to this section to a non-Federal entity on the provision of cyber threat information to the Federal Government; or

''(C) to condition the award of any Federal grant, contract or purchase on the provision of a cyber threat indicator to a Federal entity, if the provision of the cyber threat indicator does not reasonably relate to the protection of the information system of the Federal entity or information, goods, or services covered by the award.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by inserting after the item relating to section 228 the following:

''Sec. 229. Cyber threat sharing.''.

(c) SUNSET.—Effective on the date that is 5 years after the date of enactment of this Act—

(1) section 229 of the Homeland Security Act of 2002, as added by subsection (a), is repealed; and

(2) the table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the item relating to section 229.

SEC. 3. SENSE OF CONGRESS.

It is the sense of Congress that the statement issued by the Department of Justice and the Federal Trade Commission on April 10, 2014 entitled ''Antitrust Policy Statement On Sharing Of Cybersecurity Information'' provides protections against antitrust concerns for the legitimate sharing of cyber threat indicators (as defined in section 229 of the Homeland Security Act of 2002 (as added by section 2)).

○