

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Threat Sharing
5 Act of 2015”.

1 **SEC. 2. CYBER THREAT INDICATOR SHARING.**

2 (a) IN GENERAL.—Subtitle C of title II of the Home-
3 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
4 ed by adding at the end the following:

5 **“SEC. 229. CYBER THREAT INDICATOR SHARING.**

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

8 “(1) CENTER.—The term ‘Center’ means the
9 national cybersecurity and communications integra-
10 tion center established under the second section des-
11 ignated as section 226.

12 “(2) CYBER THREAT.—The term ‘cyber
13 threat’—

14 “(A) means any action that may result
15 in—

16 “(i) unauthorized access in order to
17 damage or impair the integrity, confiden-
18 tiality, or availability of an information
19 system; or

20 “(ii) unauthorized exfiltration, dele-
21 tion, or manipulation of information that is
22 stored on, processed by, or transiting an
23 information system; and

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

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

3 “(3) CYBER THREAT INDICATOR.—The term
4 ‘cyber threat indicator’ means information—

5 “(A) that is necessary to indicate, describe,
6 or identify—

7 “(i) malicious reconnaissance, includ-
8 ing communications that reasonably ap-
9 pear to be transmitted for the purpose of
10 gathering technical information related to
11 a cyber threat;

12 “(ii) a method of defeating a technical
13 control or an operational control;

14 “(iii) a technical vulnerability;

15 “(iv) a method of causing a user with
16 legitimate access to an information system
17 or information that is stored on, processed
18 by, or transiting an information system in-
19 advertently to enable the defeat of a tech-
20 nical control or an operational control;

21 “(v) malicious cyber command and
22 control; or

23 “(vi) any combination of clauses (i)
24 through (v); and

1 “(B) from which reasonable efforts have
2 been made to remove information that may be
3 used to identify specific persons reasonably be-
4 lieved to be unrelated to the cyber threat.

5 “(4) FEDERAL ENTITY.—The term ‘Federal en-
6 tity’ means—

7 “(A) an agency or department of the
8 United States; or

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

12 “(5) GOVERNMENTAL ENTITY.—The term ‘gov-
13 ernmental entity’ means—

14 “(A) any Federal entity;

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

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

20 “(6) INFORMATION SHARING AND ANALYSIS OR-
21 GANIZATION.—The term ‘Information Sharing and
22 Analysis Organization’ has the meaning given that
23 term in section 212.

24 “(7) INFORMATION SYSTEM.—The term ‘infor-
25 mation system’ means a discrete set of hardware

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

4 “(8) MALICIOUS CYBER COMMAND AND CON-
5 TROL.—The term ‘malicious cyber command and
6 control’ means a method for remote identification of,
7 access to, or use of, an information system or infor-
8 mation that is stored on, processed by, or transiting
9 an information system that is known or reasonably
10 suspected of being associated with a known or sus-
11 pected cyber threat.

12 “(9) MALICIOUS RECONNAISSANCE.—The term
13 ‘malicious reconnaissance’ means a method for
14 probing or monitoring an information system for the
15 purpose of discerning technical vulnerabilities of the
16 information system, if such method is known or rea-
17 sonably suspected of being associated with a known
18 or suspected cyber threat.

19 “(10) NON-FEDERAL ENTITY.—The term ‘non-
20 Federal entity’ means a private entity or a govern-
21 mental entity other than a Federal entity.

22 “(11) OPERATIONAL CONTROL.—The term
23 ‘operational control’ means a security control for an
24 information system that is primarily implemented
25 and executed by people.

1 “(12) PRIVATE ENTITY.—The term ‘private en-
2 tity’—

3 “(A) has the meaning given the term ‘per-
4 son’ in section 1 of title 1, United States Code;
5 and

6 “(B) does not include a governmental enti-
7 ty or a foreign government, or any component
8 thereof.

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

13 “(14) TECHNICAL CONTROL.—The term ‘tech-
14 nical control’ means a hardware or software restric-
15 tion on, or audit of, access or use of an information
16 system or information that is stored on, processed
17 by, or transiting an information system that is in-
18 tended to ensure the confidentiality, integrity, or
19 availability of that information system or the infor-
20 mation processed or stored by that information sys-
21 tem.

22 “(15) TECHNICAL VULNERABILITY.—The term
23 ‘technical vulnerability’ means any attribute of hard-
24 ware, firmware, or software that could enable or fa-
25 cilitate the defeat of a technical control.

1 “(b) VOLUNTARY DISCLOSURE AND RECEIPT OF
2 CYBER THREAT INDICATORS.—

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

5 “(A) disclose a lawfully obtained cyber
6 threat indicator to—

7 “(i) a private Information Sharing
8 and Analysis Organization; and

9 “(ii) the Center; and

10 “(B) receive a cyber threat indicator dis-
11 closed under this section by a Federal or non-
12 Federal entity.

13 “(2) VOLUNTARY SHARING WITH LAW EN-
14 FORCEMENT.—Any entity may disclose a lawfully
15 obtained cyber threat indicator to a Federal entity
16 for investigative purposes consistent with the lawful
17 authorities of the Federal entity.

18 “(3) USE AND PROTECTION OF INFORMA-
19 TION.—A private entity that discloses or receives a
20 cyber threat indicator under paragraph (1)—

21 “(A) may only use, retain, or further dis-
22 close the cyber threat indicator for the purpose
23 of—

24 “(i) protecting an information system
25 or information that is stored on, processed

1 by, or transiting an information system
2 from cyber threats;

3 “(ii) identifying or mitigating such
4 cyber threats; or

5 “(iii) reporting a crime;

6 “(B) shall take reasonable efforts—

7 “(i) to minimize information that may
8 be used to identify specific persons and is
9 reasonably believed to be unrelated to a
10 cyber threat; and

11 “(ii) to safeguard information that
12 may be used to identify specific persons
13 from unintended disclosure and unauthor-
14 ized access or acquisition; and

15 “(C) shall comply with reasonable restric-
16 tions that a private entity places on the subse-
17 quent disclosure or retention of a cyber threat
18 indicator that the private entity discloses to
19 other private entities.

20 “(4) BEST PRACTICES FOR PRIVATE INFORMA-
21 TION SHARING AND ANALYSIS ORGANIZATIONS.—

22 The Secretary, in consultation with the Secretary of
23 Commerce, the Attorney General, the Director of the
24 Office of Management and Budget, and the heads of

1 sector-specific agencies and other appropriate Fed-
2 eral agencies, shall—

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

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

11 “(c) FEDERAL CYBER THREAT INDICATOR SHAR-
12 ING.—

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

19 “(2) SHARING WITH NON-FEDERAL ENTI-
20 TIES.—

21 “(A) IN GENERAL.—To protect informa-
22 tion systems or information that is stored on,
23 processed by, or transiting an information sys-
24 tem from cyber threats, the Secretary shall co-
25 ordinate Federal efforts to ensure that useful

1 classified and unclassified cyber threat indica-
2 tors are shared in a timely manner with non-
3 Federal entities.

4 “(B) REPORT.—

5 “(i) IN GENERAL.—Not later than 1
6 year after the date of enactment of this
7 section, and every year thereafter for 2
8 years, the Secretary, in consultation with
9 the Attorney General, the Director of the
10 Office of Management and Budget, the Di-
11 rector of National Intelligence, the Sec-
12 retary of Defense, and the heads of sector-
13 specific agencies and other appropriate
14 Federal agencies, shall submit to Congress
15 a report including—

16 “(I) a review of all Federal ef-
17 forts to share classified and unclassi-
18 fied cyber threat indicators to protect
19 information systems from cyber
20 threats, including summaries of the
21 nature of those efforts and the quan-
22 tities of information shared;

23 “(II) challenges to the appro-
24 priate sharing of cyber threat indica-
25 tors; and

1 “(III) recommendations to en-
2 hance the appropriate sharing of
3 cyber threat indicators.

4 “(ii) FORM OF REPORT.—Each report
5 submitted under clause (i) shall be in un-
6 classified form, but may include a classi-
7 fied annex.

8 “(3) SHARING AMONG FEDERAL ENTITIES.—

9 “(A) IN GENERAL.—The Secretary, in con-
10 sultation with the heads of appropriate agen-
11 cies, shall coordinate and establish procedures
12 for the sharing of cyber threat indicators
13 among Federal agencies, with appropriate con-
14 sideration of privacy and civil liberties and
15 agency equities.

16 “(B) SHARING BY THE CENTER.—The
17 Secretary, in consultation with the Attorney
18 General, the Director of the Office of Manage-
19 ment and Budget, the Director of National In-
20 telligence, the Secretary of Defense, and the
21 heads of sector-specific agencies and other ap-
22 propriate Federal agencies, shall ensure that
23 cyber threat indicators received and disclosed
24 by the Center under paragraph (1) are shared

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

3 “(4) REAL TIME SHARING.—

4 “(A) IN GENERAL.—The Secretary, in co-
5 ordination with the Director of the National In-
6 stitute for Standards and Technology, and con-
7 sistent with the Cybersecurity Enhancement
8 Act of 2014 (Public Law 113–274; 128 Stat.
9 2971), shall develop a program that supports
10 and rapidly advances the development, adop-
11 tion, and implementation of automated mecha-
12 nisms for the real time sharing of cyber threat
13 indicators.

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

19 “(d) LIMITATION OF LIABILITY.—

20 “(1) LIABILITY FOR DISCLOSURE OF CYBER
21 THREAT INDICATORS.—

22 “(A) IN GENERAL.—A civil or criminal ac-
23 tion may not be filed or maintained in a Fed-
24 eral or State court against an entity for the vol-
25 untary disclosure or receipt under this section

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

4 “(i) the Center; or

5 “(ii) a private Information Sharing
6 and Analysis Organization, if the organiza-
7 tion maintains a publicly-available self-cer-
8 tification that the organization has adopted
9 the best practices identified or developed
10 under subsection (b)(4).

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

15 “(2) PROTECTION FROM PUBLIC DISCLO-
16 SURE.—

17 “(A) IN GENERAL.—A cyber threat indi-
18 cator that is submitted by a non-Federal entity
19 to the Center shall be exempt from disclosure
20 under—

21 “(i) section 552(b)(3) of title 5,
22 United States Code;

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

1 “(iii) any State law otherwise requir-
2 ing disclosure.

3 “(B) APPLICATION OF SECTION 214.—

4 “(i) IN GENERAL.—Except as pro-
5 vided under clause (ii), a cyber threat indi-
6 cator that is submitted by a non-Federal
7 entity to the Center shall be treated in the
8 same manner as voluntarily submitted crit-
9 ical infrastructure information is treated
10 under section 214.

11 “(ii) EXCEPTION.—For purposes of
12 clause (i), the requirements under sub-
13 section (a)(2) (regarding an express state-
14 ment) and subsection (e)(2)(A) (regarding
15 acknowledgment of receipt) of section 214
16 shall not apply.

17 “(3) LIMITATION OF REGULATORY ENFORCE-
18 MENT ACTIONS.—

19 “(A) IN GENERAL.—A Federal entity may
20 not use a cyber threat indicator received under
21 this section as evidence in a regulatory enforce-
22 ment action against an entity that disclosed the
23 cyber threat indicator to the Federal Govern-
24 ment under subsection (c).

1 “(B) EXCEPTION.—Nothing in subpara-
2 graph (A) shall be construed to prevent a Fed-
3 eral entity from using a cyber threat indicator
4 received through lawful means other than under
5 this section as evidence in a regulatory enforce-
6 ment action, even if the Federal entity also re-
7 ceives the cyber threat indicator under this sec-
8 tion.

9 “(4) RULE OF CONSTRUCTION.—Nothing in
10 this section shall be construed to prohibit or other-
11 wise limit an Information Sharing and Analysis Or-
12 ganization, information sharing and analysis center,
13 or other non-Federal entity from self-certifying
14 under paragraph (1)(A)(ii) that the entity has
15 adopted the best practices identified or developed
16 under subsection (b)(4).

17 “(e) PRIVACY PROTECTIONS.—

18 “(1) POLICIES AND PROCEDURES.—

19 “(A) IN GENERAL.—The Secretary, in con-
20 sultation with the Attorney General, the Chief
21 Privacy Officer of the Department, the Chief
22 Privacy and Civil Liberties Officer of the De-
23 partment of Justice, the Secretary of Com-
24 merce, the Director of National Intelligence, the
25 Secretary of Defense, the Director of the Office

1 of Management and Budget, the heads of sec-
2 tor-specific agencies and other appropriate
3 agencies, and the Privacy and Civil Liberties
4 Oversight Board, shall develop and periodically
5 review policies and procedures governing the re-
6 ceipt, retention, use, and disclosure of a cyber
7 threat indicator obtained by a Federal entity
8 under this section.

9 “(B) REQUIREMENTS.—The policies and
10 procedures developed under subparagraph (A)
11 shall—

12 “(i) reasonably limit the acquisition,
13 interception, retention, use, and disclosure
14 of a cyber threat indicator that is reason-
15 ably likely to identify specific persons, in-
16 cluding by establishing a process—

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

21 “(II) to anonymize and safeguard
22 information received and disclosed
23 that may be used to identify specific
24 persons unrelated to a cyber threat;

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

6 “(iii) for cyber threat indicators re-
7 ceived by the Center under subsection
8 (c)(1), establish publicly available guide-
9 lines that authorize law enforcement use of
10 a cyber threat indicator received by a Fed-
11 eral entity under subsection (c) only to in-
12 vestigate, prosecute, disrupt, or otherwise
13 respond to—

14 “(I) a computer crime;

15 “(II) a threat of death or serious
16 bodily harm;

17 “(III) a serious threat to a
18 minor, including sexual exploitation
19 and threats to physical safety; or

20 “(IV) an attempt or conspiracy
21 to commit an offense described in sub-
22 clause (I), (II), or (III);

23 “(iv) preserve the confidentiality of
24 disclosed proprietary information to the
25 greatest extent practicable, and require re-

1 recipients of such information to be informed
2 that the cyber threat indicator disclosed
3 may only be used for the purposes author-
4 ized under this section; and

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

11 “(2) OVERSIGHT BY FEDERAL ENTITIES.—The
12 head of each Federal entity that receives or discloses
13 a cyber threat indicator under this section shall es-
14 tablish a program to monitor and oversee compliance
15 with the policies and procedures developed under
16 paragraph (1)(A).

17 “(3) PUBLICATION.—The policies and proce-
18 dures developed under paragraph (1)(A) shall—

19 “(A) be provided to the appropriate con-
20 gressional committees; and

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

25 “(4) REPORTS.—

1 “(A) ANNUAL REPORT ON PRIVACY AND
2 CIVIL LIBERTIES.—The Chief Privacy Officer of
3 the Department and the Chief Privacy and Civil
4 Liberties Officer of the Department of Justice,
5 in consultation with the privacy and civil lib-
6 erties officers of other appropriate Federal
7 agencies, shall submit to Congress an annual
8 report assessing the privacy and civil liberties
9 impact of the governmental activities conducted
10 under this section.

11 “(B) ADDITIONAL REPORT.—

12 “(i) IN GENERAL.—Not later than 2
13 years after the date of enactment of this
14 section, and every year thereafter for 2
15 years, the Secretary, the Director of Na-
16 tional Intelligence, the Attorney General,
17 and the Secretary of Defense shall jointly
18 submit to Congress a report that—

19 “(I) describes the extent to which
20 the authorities provided under this
21 section have enabled the Federal Gov-
22 ernment and the private sector to
23 mitigate cyber threats;

24 “(II) discloses any significant
25 acts of noncompliance by a non-Fed-

1 eral entity with this section, with spe-
2 cial emphasis on privacy and civil lib-
3 erties, and any measures taken by the
4 Federal Government to uncover such
5 noncompliance;

6 “(III) describes in general terms
7 the nature and quantity of informa-
8 tion disclosed and received by govern-
9 mental entities and private entities
10 under this section;

11 “(IV) describes the uses by Fed-
12 eral agencies of information received
13 under this section, including the gen-
14 eral quantity of information being
15 used for each purpose; and

16 “(V) identifies the emergence of
17 new threats or technologies that chal-
18 lenge the adequacy of this section, in-
19 cluding the definitions, authorities,
20 and requirements of this section, for
21 keeping pace with the threat.

22 “(ii) FORM OF REPORT.—Each report
23 submitted under clause (i) shall be sub-
24 mitted in unclassified form, but may in-
25 clude a classified annex.

1 “(f) CONSTRUCTION AND FEDERAL PREEMPTION.—

2 “(1) CONSTRUCTION.—Nothing in this section
3 may be construed—

4 “(A) except as provided in subsection
5 (d)(2), to limit any law or regulation that re-
6 quires the disclosure, receipt, or retention of in-
7 formation;

8 “(B) to limit the authority of an entity to
9 share information concerning potential criminal
10 activity or investigations with law enforcement
11 entities;

12 “(C) to limit or prohibit otherwise lawful
13 disclosures of information by a private entity to
14 any governmental or private entity not con-
15 ducted under this section;

16 “(D) to allow the otherwise unauthorized
17 disclosure by a private entity of information or
18 material that has been determined by the Fed-
19 eral Government pursuant to an Executive
20 order, statute, or regulation to require protec-
21 tion against unauthorized disclosure for reasons
22 of national defense or foreign relations of the
23 United States, including—

1 “(i) any restricted data, as defined in
2 section 11(y) of the Atomic Energy Act of
3 1954 (42 U.S.C. 2014(y));

4 “(ii) information related to intel-
5 ligence sources and methods; and

6 “(iii) information that is specifically
7 subject to a court order or a certification,
8 directive, or other authority precluding
9 such disclosure;

10 “(E) to authorize or limit liability for ac-
11 tions that would—

12 “(i) violate the Report and Order of
13 the Federal Communications Commission
14 with regard to Preserving the Open Inter-
15 net; Broadband Industry Practices (GN
16 Docket No. 09–191, WC Docket No. 07–
17 52) (adopted December 21, 2010) or any
18 successor Report or Order thereto; or

19 “(ii) modify or alter the obligations of
20 private entities under Report or Order de-
21 scribed in clause (i); or

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

1 tomer lists, or information regarding future
2 competitive planning.

3 “(2) FEDERAL PREEMPTION.—This section su-
4 persedes any law or requirement of a State or polit-
5 ical subdivision of a State that restricts or otherwise
6 expressly regulates the retention, use, or disclosure
7 of a cyber threat indicator by a private entity.

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

12 “(4) NO CREATION OF A RIGHT TO INFORMA-
13 TION.—The provision of information to a non-Fed-
14 eral entity under this section does not create a right
15 or benefit to similar information by any other non-
16 Federal entity.

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

21 “(6) PROHIBITION ON REQUIREMENT TO PRO-
22 VIDE INFORMATION TO THE FEDERAL GOVERN-
23 MENT.—Nothing in this section shall be construed to
24 authorize a Federal entity—

1 “(A) to require a non-Federal entity to
2 share information with the Federal Govern-
3 ment;

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

8 “(C) to condition the award of any Federal
9 grant, contract or purchase on the provision of
10 a cyber threat indicator to a Federal entity, if
11 the provision of the cyber threat indicator does
12 not reasonably relate to the protection of the in-
13 formation system of the Federal entity or infor-
14 mation, goods, or services covered by the
15 award.”.

16 (b) TECHNICAL AND CONFORMING AMENDMENT.—
17 The table of contents in section 1(b) of the Homeland Se-
18 curity Act of 2002 (6 U.S.C. 101 note) is amended by
19 inserting after the item relating to section 228 the fol-
20 lowing:

 “Sec. 229. Cyber threat sharing.”.

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

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

1 (2) the table of contents in section 1(b) of the
2 Homeland Security Act of 2002 (6 U.S.C. 101 note)
3 is amended by striking the item relating to section
4 229.

5 **SEC. 3. SENSE OF CONGRESS.**

6 It is the sense of Congress that the statement issued
7 by the Department of Justice and the Federal Trade Com-
8 mission on April 10, 2014 entitled “Antitrust Policy
9 Statement On Sharing Of Cybersecurity Information”
10 provides protections against antitrust concerns for the le-
11 gitimate sharing of cyber threat indicators (as defined in
12 section 229 of the Homeland Security Act of 2002 (as
13 added by section 2)).

○