

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.

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 “Cybersecurity Informa-
5 tion Sharing Act of 2012”.

6 **SEC. 2. AFFIRMATIVE AUTHORITY TO MONITOR AND DE-**
7 **FEND AGAINST CYBERSECURITY THREATS.**

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

1 Act of 1978 (50 U.S.C. 1801 et seq.), and the Commu-
2 nications Act of 1934 (47 U.S.C. 151 et seq.), any private
3 entity may—

4 (1) monitor its information systems and infor-
5 mation that is stored on, processed by, or transiting
6 such information systems for cybersecurity threats;

7 (2) monitor a third party's information systems
8 and information that is stored on, processed by, or
9 transiting such information systems for cybersecu-
10 rity threats, if the third party lawfully authorizes
11 such monitoring;

12 (3) operate countermeasures on its information
13 systems to protect its information systems and infor-
14 mation that is stored on, processed by, or transiting
15 such information systems; and

16 (4) operate countermeasures on a third party's
17 information systems to protect the third party's in-
18 formation systems and information that is stored on,
19 processed by, or transiting such information sys-
20 tems, if the third party lawfully authorizes such
21 countermeasures.

1 **SEC. 3. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
2 **THREAT INDICATORS AMONG PRIVATE ENTI-**
3 **TIES.**

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

8 (b) **USE AND PROTECTION OF INFORMATION.**—A pri-
9 vate entity disclosing or receiving cybersecurity threat in-
10 dicators pursuant to subsection (a)—

11 (1) shall make reasonable efforts to safeguard
12 communications, records, system traffic, or other in-
13 formation that can be used to identify specific per-
14 sons from unauthorized access or acquisition;

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

21 (3) may not use the cybersecurity threat indica-
22 tors to gain an unfair competitive advantage to the
23 detriment of the entity that authorized such sharing;
24 and

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

1 of protecting an information system or information
2 that is stored on, processed by, or transiting an in-
3 formation system from cybersecurity threats or miti-
4 gating such threats.

5 **SEC. 4. CYBERSECURITY EXCHANGES.**

6 (a) DESIGNATION OF CYBERSECURITY EX-
7 CHANGES.—The Secretary of Homeland Security, in con-
8 sultation with the Director of National Intelligence, the
9 Attorney General, and the Secretary of Defense, shall es-
10 tablish—

11 (1) a process for designating appropriate Fed-
12 eral entities, such as 1 or more Federal cybersecu-
13 rity centers, and non-Federal entities as cybersecu-
14 rity exchanges;

15 (2) procedures to facilitate and encourage the
16 sharing of classified and unclassified cybersecurity
17 threat indicators with designated cybersecurity ex-
18 changes and other appropriate Federal entities and
19 non-Federal entities; and

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

23 (b) PURPOSE.—The purpose of a cybersecurity ex-
24 change is to efficiently receive and distribute cybersecurity
25 threat indicators as provided in this Act.

1 (c) REQUIREMENT FOR A LEAD FEDERAL CYBERSE-
2 CURITY EXCHANGE.—

3 (1) IN GENERAL.—The Secretary of Homeland
4 Security, in consultation with the Director of Na-
5 tional Intelligence, the Attorney General, and the
6 Secretary of Defense, shall designate a Federal enti-
7 ty as the lead cybersecurity exchange to serve as the
8 focal point within the Federal Government for cyber-
9 security information sharing among Federal entities
10 and with non-Federal entities.

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

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

15 (B) facilitate information sharing, inter-
16 action, and collaboration among and between—

17 (i) Federal entities;

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

20 (iii) private entities;

21 (iv) academia;

22 (v) international partners, in consulta-
23 tion with the Secretary of State; and

24 (vi) other cybersecurity exchanges;

1 (C) disseminate timely and actionable cy-
2 bersecurity threat, vulnerability, mitigation, and
3 warning information, including alerts,
4 advisories, indicators, signatures, and mitiga-
5 tion and response measures, to improve the se-
6 curity and protection of information systems;

7 (D) coordinate with other Federal and
8 non-Federal entities, as appropriate, to inte-
9 grate information from Federal and non-Fed-
10 eral entities, including Federal cybersecurity
11 centers, non-Federal network or security oper-
12 ation centers, other cybersecurity exchanges,
13 and non-Federal entities that disclose cyberse-
14 curity threat indicators under section 5(a) to
15 provide situational awareness of the United
16 States information security posture and foster
17 information security collaboration among infor-
18 mation system owners and operators;

19 (E) conduct, in consultation with private
20 entities and relevant Federal and other govern-
21 mental entities, regular assessments of existing
22 and proposed information sharing models to
23 eliminate bureaucratic obstacles to information
24 sharing and identify best practices for such
25 sharing; and

1 (F) coordinate with other Federal entities,
2 as appropriate, to compile and analyze informa-
3 tion about risks and incidents that threaten in-
4 formation systems, including information volun-
5 tarily submitted in accordance with section 5(a)
6 or otherwise in accordance with applicable laws.

7 (3) SCHEDULE FOR DESIGNATION.—

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

13 (B) INTERIM DESIGNATION.—The Na-
14 tional Cybersecurity and Communications Inte-
15 gration Center of the Department of Homeland
16 Security shall serve as the interim lead cyberse-
17 curity exchange until the initial designation is
18 made pursuant to subparagraph (A).

19 (d) ADDITIONAL FEDERAL CYBERSECURITY EX-
20 CHANGES.—In accordance with the process and proce-
21 dures established in subsection (a), the Secretary of
22 Homeland Security, in consultation with the Director of
23 National Intelligence, the Attorney General, and the Sec-
24 retary of Defense, may designate additional existing Fed-
25 eral entities as cybersecurity exchanges, if such cybersecu-

1 rity exchanges are subject to the requirements for use, re-
2 tention, and disclosure of information by a cybersecurity
3 exchange under section 5(b) and the special requirements
4 for Federal entities under section 5(g).

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

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

13 (A) The net effect that an additional cy-
14 bersecurity exchange would have on the overall
15 cybersecurity of the United States.

16 (B) Whether such designation could sub-
17 stantially improve such overall cybersecurity by
18 serving as a hub for receiving and sharing cy-
19 bersecurity threat indicators, including the ca-
20 pacity of the non-Federal entity for performing
21 those functions.

22 (C) The capacity of such non-Federal enti-
23 ty to safeguard cybersecurity threat indicators
24 from unauthorized disclosure and use.

1 (D) The adequacy of the policies and pro-
2 cedures of such non-Federal entity to protect
3 personally identifiable information from unau-
4 thorized disclosure and use.

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

8 (2) REGULATIONS.—The Secretary of Home-
9 land Security may promulgate regulations as may be
10 necessary to carry out this subsection.

11 (f) CONSTRUCTION WITH OTHER AUTHORITIES.—
12 Nothing in this section may be construed to alter the au-
13 thorities of a Federal cybersecurity center, unless such cy-
14 bersecurity center is acting in its capacity as a designated
15 cybersecurity exchange.

16 (g) NO NEW BUREAUCRACIES.—Nothing in this sec-
17 tion may be construed to authorize additional layers of
18 Federal bureaucracy for the receipt and disclosure of cy-
19 bersecurity threat indicators.

20 (h) REPORT ON DESIGNATION OF CYBERSECURITY
21 EXCHANGES.—Not later than 90 days after the date the
22 Secretary of Homeland Security designates the initial cy-
23 bersecurity exchange under this section, the Secretary of
24 Homeland Security, the Director of National Intelligence,

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

3 (1) describes the processes established to des-
4 ignate cybersecurity exchanges under subsection (a);

5 (2) summarizes the policies and procedures es-
6 tablished under section 5(g); and

7 (3) if none of the cybersecurity exchanges are
8 non-Federal entities, provides recommendations con-
9 cerning the advisability of designating non-Federal
10 entities as cybersecurity exchanges.

11 **SEC. 5. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
12 **THREAT INDICATORS TO A CYBERSECURITY**
13 **EXCHANGE.**

14 (a) **AUTHORITY TO DISCLOSE.**—Notwithstanding
15 any other provision of law, a non-Federal entity may dis-
16 close lawfully obtained cybersecurity threat indicators to
17 a cybersecurity exchange.

18 (b) **USE, RETENTION, AND DISCLOSURE OF INFOR-**
19 **MATION BY A CYBERSECURITY EXCHANGE.**—Except as
20 provided in subsection (g), a cybersecurity exchange may
21 only use, retain, or further disclose information provided
22 pursuant to subsection (a) in order to protect information
23 systems from cybersecurity threats or mitigate cybersecu-
24 rity threats.

1 (c) USE AND PROTECTION OF INFORMATION RE-
2 CEIVED FROM A CYBERSECURITY EXCHANGE.—A non-
3 Federal entity receiving cybersecurity threat indicators
4 from a cybersecurity exchange—

5 (1) shall make reasonable efforts to safeguard
6 communications, records, system traffic, or other in-
7 formation that can be used to identify specific per-
8 sons from unauthorized access or acquisition;

9 (2) shall comply with any lawful restrictions
10 placed on the disclosure or use of cybersecurity
11 threat indicators by the cybersecurity exchange or a
12 third party, if the cybersecurity exchange received
13 such information from the third party, including, if
14 requested, the removal of information that can be
15 used to identify specific persons from such indica-
16 tors;

17 (3) may not use the cybersecurity threat indica-
18 tors to gain an unfair competitive advantage to the
19 detriment of the third party that authorized such
20 sharing; and

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

1 formation system from cybersecurity threats or miti-
2 gating such threats.

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

7 (1) exempt from disclosure under section
8 552(b)(3) of title 5, United States Code, or any
9 comparable State law; and

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

13 (e) EXEMPTION FROM EX PARTE LIMITATIONS.—
14 Any cybersecurity threat indicator disclosed by a non-Fed-
15 eral entity to a cybersecurity exchange pursuant to sub-
16 section (a) shall not be subject to the rules of any govern-
17 mental entity or judicial doctrine regarding ex parte com-
18 munications with a decisionmaking official.

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

1 (g) SPECIAL REQUIREMENTS FOR FEDERAL ENTI-
2 TIES.—

3 (1) PERMITTED DISCLOSURES.—Notwith-
4 standing any other provision of law and consistent
5 with the requirements of this subsection, a Federal
6 entity that lawfully intercepts, acquires, or otherwise
7 obtains or possesses any communication, record, or
8 other information from its electronic communica-
9 tions system, may disclose that communication,
10 record, or other information if—

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

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

16 (ii) mitigating cybersecurity threats
17 to—

18 (I) another component, officer,
19 employee, or agent of such Federal
20 entity with cybersecurity responsibil-
21 ities;

22 (II) any cybersecurity exchange;
23 or

24 (III) a private entity that is act-
25 ing as a provider of electronic commu-

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

4 (B) the recipient of the communication,
5 record, or other information has agreed to com-
6 ply with such Federal entity’s lawful require-
7 ments regarding the protection and further dis-
8 closure of such information, except to the ex-
9 tent such requirements are inconsistent with
10 the policies and procedures developed by the
11 Secretary of Homeland Security and approved
12 by the Attorney General under paragraph (4).

13 (2) DISCLOSURE TO LAW ENFORCEMENT.—A
14 cybersecurity exchange that is a Federal entity may
15 disclose cybersecurity threat indicators received pur-
16 suant to subsection (a) to a law enforcement entity
17 if—

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

21 (B) the disclosure is permitted under the
22 procedures developed by the Secretary and ap-
23 proved by the Attorney General under para-
24 graph (4).

1 (3) FURTHER DISCLOSURE AND USE OF INFOR-
2 MATION BY A FEDERAL ENTITY.—

3 (A) AUTHORITY TO RECEIVE CYBERSECU-
4 RITY THREAT INDICATORS.—A Federal entity
5 that is not a cybersecurity exchange may re-
6 ceive cybersecurity threat indicators from a cy-
7 bersecurity exchange pursuant to section 4, but
8 shall only use or retain such cybersecurity
9 threat indicators in a manner that is consistent
10 with this subsection in order—

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

14 (ii) to disclose such cybersecurity
15 threat indicators to law enforcement pur-
16 suant to paragraph (2).

17 (B) AUTHORITY TO USE CYBERSECURITY
18 THREAT INDICATORS.—A Federal entity that is
19 not a cybersecurity exchange shall ensure, by
20 written agreement, that if disclosing cybersecu-
21 rity threat indicators to a non-Federal entity
22 under this section, such non-Federal entity
23 shall use or retain such cybersecurity threat in-
24 dicators in a manner that is consistent with the
25 requirements in—

1 (i) section 3(b) on the use and protec-
2 tion of information; and

3 (ii) paragraph (2) of this subsection.

4 (4) PRIVACY AND CIVIL LIBERTIES.—

5 (A) REQUIREMENT FOR POLICIES AND
6 PROCEDURES.—In consultation with privacy
7 and civil liberties experts, the Director of Na-
8 tional Intelligence, and the Secretary of De-
9 fense, the Secretary of Homeland Security shall
10 develop and periodically review policies and pro-
11 cedures governing the receipt, retention, use,
12 and disclosure of cybersecurity threat indicators
13 by a Federal entity obtained in connection with
14 activities authorized in this Act. Such policies
15 and procedures shall—

16 (i) minimize the impact on privacy
17 and civil liberties, consistent with the need
18 to protect information systems from cyber-
19 security threats and mitigate cybersecurity
20 threats;

21 (ii) reasonably limit the receipt, reten-
22 tion, use and disclosure of cybersecurity
23 threat indicators associated with specific
24 persons consistent with the need to carry
25 out the responsibilities of this Act, includ-

1 ing establishing a process for the timely
2 destruction of cybersecurity threat indica-
3 tors that are received pursuant to this sec-
4 tion that do not reasonably appear to be
5 related to protecting information systems
6 from cybersecurity threats and mitigating
7 cybersecurity threats, unless such indica-
8 tors appear to pertain to a crime which
9 has been, is being, or is about to be com-
10 mitted;

11 (iii) include requirements to safeguard
12 cybersecurity threat indicators that can be
13 used to identify specific persons from un-
14 authorized access or acquisition; and

15 (iv) protect the confidentiality of cy-
16 bersecurity threat indicators associated
17 with specific persons to the greatest extent
18 practicable and require recipients to be in-
19 formed that such indicators may only be
20 used for protecting information systems
21 against cybersecurity threats, mitigating
22 against cybersecurity threats, or disclosed
23 to law enforcement pursuant to paragraph
24 (2).

1 (B) ADOPTION OF POLICIES AND PROCE-
2 DURES.—The head of an agency responsible for
3 a Federal entity designated as a cybersecurity
4 exchange under section 4 shall adopt and com-
5 ply with the policies and procedures developed
6 under this paragraph.

7 (C) REVIEW BY THE ATTORNEY GEN-
8 ERAL.—Not later than 1 year after the date of
9 the enactment of this Act, the policies and pro-
10 cedures developed under this subsection shall be
11 reviewed and approved by the Attorney General.

12 (D) PROVISION TO CONGRESS.—The poli-
13 cies and procedures issued under this Act and
14 any amendments to such policies and proce-
15 dures shall be provided to Congress.

16 (5) OVERSIGHT.—

17 (A) REQUIREMENT FOR OVERSIGHT.—The
18 Secretary of Homeland Security and the Attor-
19 ney General shall establish a mandatory pro-
20 gram to monitor and oversee compliance with
21 the policies and procedures issued under this
22 subsection.

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

1 (i) comply with the policies and proce-
2 dures developed by the Secretary of Home-
3 land Security and approved by the Attor-
4 nery General under paragraph (4);

5 (ii) promptly notify the Attorney Gen-
6 eral of significant violations of such poli-
7 cies and procedures; and

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

11 (C) ANNUAL REPORT.—On an annual
12 basis, the Chief Privacy and Civil Liberties Of-
13 ficer of the Department of Justice and the De-
14 partment of Homeland Security, in consultation
15 with the most senior privacy and civil liberties
16 officer or officers of any appropriate agencies,
17 shall jointly submit to Congress a report assess-
18 ing the privacy and civil liberties impact of the
19 governmental activities conducted pursuant to
20 this Act.

21 (6) PRIVACY AND CIVIL LIBERTIES OVERSIGHT
22 BOARD REPORT.—Not later than two years after the
23 date of the enactment of this Act, the Privacy and
24 Civil Liberties Oversight Board shall submit to Con-
25 gress and the President a report providing—

1 (A) an assessment of the privacy and civil
2 liberties impact of the activities carried out by
3 the Federal entities under this Act; and

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

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

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

13 (B) in a manner inconsistent with the dis-
14 charge of the responsibilities of such govern-
15 mental entities; or

16 (C) in contravention of the requirements,
17 policies and procedures required by this sub-
18 section.

19 **SEC. 6. SHARING OF CLASSIFIED CYBERSECURITY THREAT**
20 **INDICATORS.**

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

25 (1) shared with certified entities;

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

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

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

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

15 (1) grant a security clearance on a temporary
16 or permanent basis to an employee of a certified en-
17 tity;

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

21 (3) expedite the security clearance process for
22 such an employee or entity, if appropriate, in a man-
23 ner consistent with the need to protect the national
24 security of the United States.

1 (c) DISTRIBUTION OF PROCEDURES AND GUIDE-
2 LINES.—Following the establishment of the procedures
3 under section 4(a)(2) and the issuance of the guidelines
4 under subsection (b), the Secretary of Homeland Security
5 and the Director of National Intelligence shall expedi-
6 tiously distribute such procedures and guidelines to—

7 (1) appropriate governmental entities and pri-
8 vate entities;

9 (2) the Committee on Armed Services, the
10 Committee on Commerce, Science, and Transpor-
11 tation, the Committee on Homeland Security and
12 Governmental Affairs, the Committee on the Judici-
13 ary, and the Select Committee on Intelligence of the
14 Senate; and

15 (3) the Committee on Armed Services, the
16 Committee on Energy and Commerce, the Com-
17 mittee on Homeland Security, the Committee on the
18 Judiciary, and the Permanent Select Committee on
19 Intelligence of the House of Representatives.

20 **SEC. 7. LIMITATION ON LIABILITY AND GOOD FAITH DE-**
21 **FENSE FOR CYBERSECURITY ACTIVITIES.**

22 (a) IN GENERAL.—No civil or criminal cause of ac-
23 tion shall lie or be maintained in any Federal or State
24 court against any entity, and any such action shall be dis-
25 missed promptly, based on—

1 (1) the cybersecurity monitoring activities au-
2 thorized by paragraph (1) or (2) of section 2; or

3 (2) the voluntary disclosure of a lawfully ob-
4 tained cybersecurity threat indicator—

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

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

9 (C) to a private entity or governmental en-
10 tity that provides or manages critical infra-
11 structure (as that term is used in section 1016
12 of the Critical Infrastructures Protection Act of
13 2001 (42 U.S.C. 5195c)); or

14 (D) to any other private entity under sec-
15 tion 3(a), if the cybersecurity threat indicator is
16 also disclosed within a reasonable time to a cy-
17 bersecurity exchange.

18 (b) GOOD FAITH DEFENSE.—If a civil or criminal
19 cause of action is not barred under subsection (a), good
20 faith reliance that this Act permitted the conduct com-
21 plained of is a complete defense against any civil or crimi-
22 nal action brought under this Act or any other law.

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

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

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

11 (1) the Attorney General determines that dis-
12 closure of a cybersecurity threat indicator would im-
13 pede a civil or criminal investigation and submits a
14 written request to delay notification for up to 30
15 days, except that the Attorney General may, by a
16 subsequent written request, revoke such delay or ex-
17 tend the period of time set forth in the original re-
18 quest made under this paragraph if further delay is
19 necessary; or

20 (2) the Secretary of Homeland Security, the At-
21 torney General, or the Director of National Intel-
22 ligence determines that disclosure of a cybersecurity
23 threat indicator would threaten national or home-
24 land security and submits a written request to delay
25 notification, except that the Secretary, the Attorney

1 General, or the Director may, by a subsequent writ-
2 ten request, revoke such delay or extend the period
3 of time set forth in the original request made under
4 this paragraph if further delay is necessary.

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

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

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

19 (h) DEFENSE FOR BREACH OF CONTRACT.—Compli-
20 ance with lawful restrictions placed on the disclosure or
21 use of cybersecurity threat indicators is a complete defense
22 to any tort or breach of contract claim originating in a
23 failure to disclose cybersecurity threat indicators to a third
24 party.

1 **SEC. 8. CONSTRUCTION AND FEDERAL PREEMPTION.**

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

4 (1) to permit the unauthorized disclosure of—

5 (A) information that has been determined
6 by the Federal Government pursuant to an Ex-
7 ecutive order or statute to require protection
8 against unauthorized disclosure for reasons of
9 national defense or foreign relations;

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

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

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

19 (2) to limit or prohibit otherwise lawful disclo-
20 sures of communications, records, or information by
21 a private entity to a cybersecurity exchange or any
22 other governmental or private entity not conducted
23 under this Act;

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

1 information systems, including lawfully obtained cyberse-
2 curity threat indicators;

3 (4) to authorize or prohibit any law enforce-
4 ment, homeland security, or intelligence activities
5 not otherwise authorized or prohibited under another
6 provision of law;

7 (5) to permit price-fixing, allocating a market
8 between competitors, monopolizing or attempting to
9 monopolize a market, boycotting, or exchanges of
10 price or cost information, customer lists, or informa-
11 tion regarding future competitive planning; or

12 (6) to prevent a governmental entity from using
13 information not acquired through a cybersecurity ex-
14 change for regulatory purposes.

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

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

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

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

7 (e) PROHIBITION ON REQUIREMENT TO PROVIDE IN-
8 FORMATION TO THE FEDERAL GOVERNMENT.—Nothing
9 in this Act may be construed to permit a Federal entity—

10 (1) to require a non-Federal entity to share in-
11 formation with the Federal Government; or

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

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

21 (g) DECLASSIFICATION AND SHARING OF INFORMA-
22 TION.—Consistent with the exemptions from public disclo-
23 sure of section 5(d), the Director of National Intelligence,
24 in consultation with the Secretary of Homeland Security,
25 shall facilitate the declassification and sharing of informa-

1 tion in the possession of a Federal entity that is related
2 to cybersecurity threats, as the Director deems appro-
3 priate.

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

9 (1) describes the extent to which the authorities
10 conferred by this Act have enabled the Federal Gov-
11 ernment and the private sector to mitigate cyberse-
12 curity threats;

13 (2) discloses any significant acts of noncompli-
14 ance by a non-Federal entity with this Act, with spe-
15 cial emphasis on privacy and civil liberties, and any
16 measures taken by the Federal Government to un-
17 cover such noncompliance;

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

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

1 (i) REQUIREMENT FOR ANNUAL REPORT.—On an
2 annual basis, the Director of National Intelligence shall
3 provide a report to the Select Committee on Intelligence
4 of the Senate and the Permanent Select Committee on In-
5 telligence of the House of Representatives on the imple-
6 mentation of section 6 of this Act. Such report, which shall
7 be submitted in a classified and in an unclassified form,
8 shall include a list of private entities that receive classified
9 cybersecurity threat indicators under this Act, except that
10 the unclassified report shall not contain information that
11 may be used to identify specific private entities unless
12 such private entities consent to such identification.

13 **SEC. 9. DEFINITIONS.**

14 In this Act:

15 (1) CERTIFIED ENTITY.—The term “certified
16 entity” means a protected entity, a self-protected en-
17 tity, or a provider of cybersecurity services that—

18 (A) possesses or is eligible to obtain a se-
19 curity clearance, as determined by the Director
20 of National Intelligence; and

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

1 (2) COUNTERMEASURE.—The term “counter-
2 measure” means automated or manual actions with
3 defensive intent to modify or block data packets as-
4 sociated with electronic or wire communications,
5 internet traffic, program code, or other system traf-
6 fic transiting to or from or stored on an information
7 system for the purpose of protecting the information
8 system from cybersecurity threats, conducted on an
9 information system owned or operated by or on be-
10 half of the party to be protected or operated by a
11 private entity acting as a provider of electronic com-
12 munication services, remote computing services, or
13 cybersecurity services to the party to be protected.

14 (3) CYBERSECURITY EXCHANGE.—The term
15 “cybersecurity exchange” means any governmental
16 entity or private entity designated by the Secretary
17 of Homeland Security, in consultation with the Di-
18 rector of National Intelligence, the Attorney Gen-
19 eral, and the Secretary of Defense, to receive and
20 distribute cybersecurity threat indicators under sec-
21 tion 4(a).

22 (4) CYBERSECURITY SERVICES.—The term “cy-
23 bersecurity services” means products, goods, or serv-
24 ices intended to detect, mitigate, or prevent cyberse-
25 curity threats.

1 (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.

8 (6) CYBERSECURITY THREAT INDICATOR.—The term “cybersecurity threat indicator” means information—

11 (A) that may be indicative of or describe—

12 (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;

17 (ii) a method of defeating a technical control;

19 (iii) a technical vulnerability;

20 (iv) a method of defeating an operational control;

22 (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

1 unwittingly enable the defeat of a technical
2 control or an operational control;

3 (vi) malicious cyber command and
4 control;

5 (vii) the actual or potential harm
6 caused by an incident, including informa-
7 tion exfiltrated as a result of subverting a
8 technical control when it is necessary in
9 order to identify or describe a cybersecu-
10 rity threat;

11 (viii) any other attribute of a cyberse-
12 curity threat, if disclosure of such attribute
13 is not otherwise prohibited by law; or

14 (ix) any combination thereof; and

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

19 (7) FEDERAL CYBERSECURITY CENTER.—The
20 term “Federal cybersecurity center” means the De-
21 partment of Defense Cyber Crime Center, the Intel-
22 ligence Community Incident Response Center, the
23 United States Cyber Command Joint Operations
24 Center, the National Cyber Investigative Joint Task
25 Force, the National Security Agency/Central Secu-

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

4 (8) FEDERAL ENTITY.—The term “Federal en-
5 tity” means an agency or department of the United
6 States, or any component, officer, employee, or
7 agent of such an agency or department.

8 (9) GOVERNMENTAL ENTITY.—The term “gov-
9 ernmental entity” means any Federal entity and
10 agency or department of a State, local, tribal, or ter-
11 ritorial government other than an educational insti-
12 tution, or any component, officer, employee, or agent
13 of such an agency or department.

14 (10) INFORMATION SYSTEM.—The term “infor-
15 mation system” means a discrete set of information
16 resources organized for the collection, processing,
17 maintenance, use, sharing, dissemination, or disposi-
18 tion of information, including communications with,
19 or commands to, specialized systems such as indus-
20 trial and process control systems, telephone switch-
21 ing and private branch exchange, and environmental
22 control systems.

23 (11) MALICIOUS CYBER COMMAND AND CON-
24 TROL.—The term “malicious cyber command and
25 control” means a method for remote identification

1 of, access to, or use of, an information system or in-
2 formation that is stored on, processed by, or
3 transiting an information system associated with a
4 known or suspected cybersecurity threat.

5 (12) MALICIOUS RECONNAISSANCE.—The term
6 “malicious reconnaissance” means a method for ac-
7 tively probing or passively monitoring an information
8 system for the purpose of discerning technical
9 vulnerabilities of the information system, if such
10 method is associated with a known or suspected cy-
11 bersecurity threat.

12 (13) MONITOR.—The term “monitor” means
13 the interception, acquisition, or collection of informa-
14 tion that is stored on, processed by, or transiting an
15 information system for the purpose of identifying cy-
16 bersecurity threats.

17 (14) NON-FEDERAL ENTITY.—The term “non-
18 Federal entity” means a private entity or a govern-
19 mental entity other than a Federal entity.

20 (15) OPERATIONAL CONTROL.—The term
21 “operational control” means a security control for
22 an information system that primarily is implemented
23 and executed by people.

24 (16) PRIVATE ENTITY.—The term “private en-
25 tity” has the meaning given the term “person” in

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

3 (17) PROTECT.—The term “protect” means ac-
4 tions undertaken to secure, defend, or reduce the
5 vulnerabilities of an information system, mitigate cy-
6 bersecurity threats, or otherwise enhance informa-
7 tion security or the resiliency of information systems
8 or assets.

9 (18) PROTECTED ENTITY.—The term “pro-
10 tected entity” means an entity, other than an indi-
11 vidual, that contracts with a provider of cybersecu-
12 rity services for goods or services to be used for cy-
13 bersecurity purposes.

14 (19) SELF-PROTECTED ENTITY.—The term
15 “self-protected entity” means an entity, other than
16 an individual, that provides cybersecurity services to
17 itself.

18 (20) TECHNICAL CONTROL.—The term “tech-
19 nical control” means a hardware or software restric-
20 tion on, or audit of, access or use of an information
21 system or information that is stored on, processed
22 by, or transiting an information system that is in-
23 tended to ensure the confidentiality, integrity, or
24 availability of that system.

1 (21) TECHNICAL VULNERABILITY.—The term
2 “technical vulnerability” means any attribute of
3 hardware or software that could enable or facilitate
4 the defeat of a technical control.

5 (22) THIRD PARTY.—The term “third party”
6 includes Federal entities and non-Federal entities.

○