

114TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

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

---

IN THE SENATE OF THE UNITED STATES

Mr. BURR introduced the following bill; which was read twice and referred to the Committee on \_\_\_\_\_

---

## A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, 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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Cybersecurity Information Sharing Act of 2015”.

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Sharing of information by the Federal Government.

Sec. 4. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

- Sec. 5. Sharing of cyber threat indicators and countermeasures with the Federal Government.
- Sec. 6. Protection from liability.
- Sec. 7. Oversight of Government activities.
- Sec. 8. Construction and preemption.
- Sec. 9. Report on cybersecurity threats.
- Sec. 10. Conforming amendments.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) AGENCY.—The term “agency” has the  
4 meaning given the term in section 3502 of title 44,  
5 United States Code.

6 (2) ANTITRUST LAWS.—The term “antitrust  
7 laws”—

8 (A) has the meaning given the term in sec-  
9 tion 1 of the Clayton Act (15 U.S.C. 12);

10 (B) includes section 5 of the Federal  
11 Trade Commission Act (15 U.S.C. 45) to the  
12 extent that section 5 of that Act applies to un-  
13 fair methods of competition; and

14 (C) includes any State law that has the  
15 same intent and effect as the laws under sub-  
16 paragraphs (A) and (B).

17 (3) APPROPRIATE FEDERAL ENTITIES.—The  
18 term “appropriate Federal entities” means the fol-  
19 lowing:

20 (A) The Department of Commerce.

21 (B) The Department of Defense.

22 (C) The Department of Energy.

1 (D) The Department of Homeland Secu-  
2 rity.

3 (E) The Department of Justice.

4 (F) The Department of the Treasury.

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

7 (4) COUNTERMEASURE.—The term “counter-  
8 measure” means an action, device, procedure, tech-  
9 nique, or other measure applied to an information  
10 system or information that is stored on, processed  
11 by, or transiting an information system that pre-  
12 vents or mitigates a known or suspected cybersecu-  
13 rity threat or security vulnerability.

14 (5) CYBERSECURITY PURPOSE.—The term “cy-  
15 bersecurity purpose” means the purpose of pro-  
16 tecting an information system or information that is  
17 stored on, processed by, or transiting an information  
18 system from a cybersecurity threat or security vul-  
19 nerability.

20 (6) CYBERSECURITY THREAT.—

21 (A) IN GENERAL.—Except as provided in  
22 subparagraph (B), the term “cybersecurity  
23 threat” means an action, not protected by the  
24 First Amendment to the Constitution of the  
25 United States, on or through an information

1 system that may result in an unauthorized ef-  
2 fort to adversely impact the security, avail-  
3 ability, confidentiality, or integrity of an infor-  
4 mation system or information that is stored on,  
5 processed by, or transiting an information sys-  
6 tem.

7 (B) EXCLUSION.—The term “cybersecurity  
8 threat” does not include any action that—

9 (i) solely involves a violation of a con-  
10 sumer term of service or a consumer li-  
11 censing agreement; and

12 (ii) does not otherwise constitute un-  
13 authorized access.

14 (7) CYBER THREAT INDICATOR.—The term  
15 “cyber threat indicator” means information that is  
16 necessary to describe or identify—

17 (A) malicious reconnaissance, including  
18 anomalous patterns of communications that ap-  
19 pear to be transmitted for the purpose of gath-  
20 ering technical information related to a cyberse-  
21 curity threat or security vulnerability;

22 (B) a method of defeating a security con-  
23 trol or exploitation of a security vulnerability;

1 (C) a security vulnerability, including  
2 anomalous activity that appears to indicate the  
3 existence of a security vulnerability;

4 (D) a method of causing a user with legiti-  
5 mate access to an information system or infor-  
6 mation that is stored on, processed by, or  
7 transiting an information system to unwittingly  
8 enable the defeat of a security control or exploi-  
9 tation of a security vulnerability;

10 (E) malicious cyber command and control;

11 (F) the actual or potential harm caused by  
12 an incident, including information exfiltrated  
13 when it is necessary in order to describe a cy-  
14 bersecurity threat;

15 (G) any other attribute of a cybersecurity  
16 threat, if disclosure of such attribute is not oth-  
17 erwise prohibited by law; or

18 (H) any combination thereof.

19 (8) ENTITY.—

20 (A) IN GENERAL.—Except as otherwise  
21 provided in this paragraph, the term “entity”  
22 means any private entity, non-Federal govern-  
23 ment agency or department, or State, tribal, or  
24 local government (including a political subdivi-  
25 sion, department, or component thereof).

1           (B) INCLUSIONS.—The term “entity” in-  
2           cludes a government agency or department of  
3           the District of Columbia, the Commonwealth of  
4           Puerto Rico, the Virgin Islands, Guam, Amer-  
5           ican Samoa, the Northern Mariana Islands, and  
6           any other territory or possession of the United  
7           States.

8           (C) EXCLUSION.—The term “entity” does  
9           not include a foreign power as defined in sec-  
10          tion 101 of the Foreign Intelligence Surveil-  
11          lance Act of 1978 (50 U.S.C. 1801).

12          (9) FEDERAL ENTITY.—The term “Federal en-  
13          tity” means a department or agency of the United  
14          States or any component of such department or  
15          agency.

16          (10) INFORMATION SYSTEM.—The term “infor-  
17          mation system”—

18                 (A) has the meaning given the term in sec-  
19                 tion 3502 of title 44, United States Code; and

20                 (B) includes industrial control systems,  
21                 such as supervisory control and data acquisition  
22                 systems, distributed control systems, and pro-  
23                 grammable logic controllers.

24          (11) LOCAL GOVERNMENT.—The term “local  
25          government” means any borough, city, county, par-

1 ish, town, township, village, or other political sub-  
2 division of a State.

3 (12) MALICIOUS CYBER COMMAND AND CON-  
4 TROL.—The term “malicious cyber command and  
5 control” means a method for unauthorized remote  
6 identification of, access to, or use of, an information  
7 system or information that is stored on, processed  
8 by, or transiting an information system.

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

16 (14) MONITOR.—The term “monitor” means to  
17 obtain, identify, or otherwise possess information  
18 that is stored on, processed by, or transiting an in-  
19 formation system.

20 (15) PRIVATE ENTITY.—

21 (A) IN GENERAL.—Except as otherwise  
22 provided in this paragraph, the term “private  
23 entity” means any person or private group, or-  
24 ganization, proprietorship, partnership, trust,  
25 cooperative, corporation, or other commercial or

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

3 (B) INCLUSION.—The term “private enti-  
4 ty” includes a State, tribal, or local government  
5 performing electric utility services.

6 (C) EXCLUSION.—The term “private enti-  
7 ty” does not include a foreign power as defined  
8 in section 101 of the Foreign Intelligence Sur-  
9 veillance Act of 1978 (50 U.S.C. 1801).

10 (16) SECURITY CONTROL.—The term “security  
11 control” means the management, operational, and  
12 technical controls used to protect the confidentiality,  
13 integrity, and availability of an information system  
14 or its information.

15 (17) SECURITY VULNERABILITY.—The term  
16 “security vulnerability” means any attribute of hard-  
17 ware, software, process, or procedure that could en-  
18 able or facilitate the defeat of a security control.

19 (18) TRIBAL.—The term “tribal” has the  
20 meaning given the term “Indian tribe” in section 4  
21 of the Indian Self-Determination and Education As-  
22 sistance Act (25 U.S.C. 450b).

1 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**  
2 **ERNMENT.**

3 (a) IN GENERAL.—Consistent with the protection of  
4 intelligence sources and methods and the protection of pri-  
5 vacy and civil liberties, the Director of National Intel-  
6 ligence, the Secretary of Homeland Security, the Secretary  
7 of Defense, and the Attorney General, in consultation with  
8 the heads of the appropriate Federal entities, shall develop  
9 and promulgate procedures to facilitate and promote—

10 (1) the timely sharing of classified cyber threat  
11 indicators in the possession of the Federal Govern-  
12 ment with cleared representatives of relevant enti-  
13 ties;

14 (2) the timely sharing with relevant entities of  
15 cyber threat indicators or information in the posses-  
16 sion of the Federal Government that may be declas-  
17 sified and shared at an unclassified level; and

18 (3) the sharing with relevant entities, or the  
19 public if appropriate, of unclassified, including con-  
20 trolled unclassified, cyber threat indicators in the  
21 possession of the Federal Government.

22 (b) DEVELOPMENT OF PROCEDURES.—

23 (1) IN GENERAL.—The procedures developed  
24 and promulgated under subsection (a) shall—

25 (A) ensure the Federal Government has  
26 and maintains the capability to share cyber

1 threat indicators in real time consistent with  
2 the protection of classified information;

3 (B) incorporate, to the greatest extent  
4 practicable, existing processes and existing roles  
5 and responsibilities of Federal and non-Federal  
6 entities for information sharing by the Federal  
7 Government, including sector specific informa-  
8 tion sharing and analysis centers; and

9 (C) include procedures for notifying enti-  
10 ties that have received a cyber threat indicator  
11 from a Federal entity that is known or deter-  
12 mined to be in error or in contravention of the  
13 requirements of this Act or another provision of  
14 Federal law or policy of such error or con-  
15 travention.

16 (2) COORDINATION.—In developing the proce-  
17 dures required under this section, the Director of  
18 National Intelligence, the Secretary of Homeland Se-  
19 curity, the Secretary of Defense, and the Attorney  
20 General shall coordinate with appropriate Federal  
21 entities, including the National Laboratories (as de-  
22 fined in section 2 of the Energy Policy Act of 2005  
23 (42 U.S.C. 15801)), to ensure that effective proto-  
24 cols are implemented that will facilitate and promote

1 the sharing of cyber threat indicators by the Federal  
2 Government in a timely manner.

3 (c) SUBMITTAL TO CONGRESS.—Not later than 60  
4 days after the date of the enactment of this Act, the Direc-  
5 tor of National Intelligence, in consultation with the heads  
6 of the appropriate Federal entities, shall submit to Con-  
7 gress the procedures required by subsection (a).

8 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
9 **ANALYZING, AND MITIGATING CYBERSECU-**  
10 **RITY THREATS.**

11 (a) AUTHORIZATION FOR MONITORING.—

12 (1) IN GENERAL.—Notwithstanding any other  
13 provision of law, a private entity may, for cybersecu-  
14 rity purposes, monitor—

15 (A) an information system of such private  
16 entity;

17 (B) an information system of another enti-  
18 ty, upon written consent of such other entity;

19 (C) an information system of a Federal en-  
20 tity, upon written consent of an authorized rep-  
21 resentative of the Federal entity; and

22 (D) information that is stored on, proc-  
23 essed by, or transiting an information system  
24 monitored by the private entity under this para-  
25 graph.

1           (2) CONSTRUCTION.—Nothing in this sub-  
2 section shall be construed—

3           (A) to authorize the monitoring of an in-  
4 formation system, or the use of any information  
5 obtained through such monitoring, other than  
6 as provided in this Act; or

7           (B) to limit otherwise lawful activity.

8           (b) AUTHORIZATION FOR OPERATION OF COUNTER-  
9 MEASURES.—

10           (1) IN GENERAL.—Except as provided in para-  
11 graph (2) and notwithstanding any other provision  
12 of law, a private entity may, for cybersecurity pur-  
13 poses, operate a countermeasure that is applied to—

14           (A) an information system of such private  
15 entity in order to protect the rights or property  
16 of the private entity;

17           (B) an information system of another enti-  
18 ty upon written consent of such entity for oper-  
19 ation of such countermeasure to protect the  
20 rights or property of such entity; and

21           (C) an information system of a Federal en-  
22 tity upon written consent of an authorized rep-  
23 resentative of such Federal entity for operation  
24 of such countermeasure to protect the rights or  
25 property of the Federal Government.

1           (2) LIMITATION.—The authority provided in  
2 paragraph (1) does not include operation of any  
3 countermeasure that is designed or deployed in a  
4 manner that will intentionally destroy, disable, or  
5 substantially harm an information system not be-  
6 longing to—

7           (A) the private entity operating such coun-  
8 termeasure; or

9           (B) another entity or Federal entity that  
10 has provided consent to that private entity for  
11 operation of such countermeasure in accordance  
12 with this subsection.

13           (3) CONSTRUCTION.—Nothing in this sub-  
14 section shall be construed—

15           (A) to authorize the use of a counter-  
16 measure other than as provided in this sub-  
17 section; or

18           (B) to limit otherwise lawful activity.

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

21           (1) IN GENERAL.—Except as provided in para-  
22 graph (2) and notwithstanding any other provision  
23 of law, an entity may, for the purposes permitted  
24 under this Act and consistent with the protection of  
25 classified information, share with, or receive from,

1 any other entity or the Federal Government a cyber  
2 threat indicator or countermeasure.

3 (2) **LAWFUL RESTRICTION.**—An entity receiving  
4 a cyber threat indicator or countermeasure from an-  
5 other entity or Federal entity shall comply with oth-  
6 erwise lawful restrictions placed on the sharing or  
7 use of such cyber threat indicator or countermeasure  
8 by the sharing entity or Federal entity.

9 (3) **CONSTRUCTION.**—Nothing in this sub-  
10 section shall be construed—

11 (A) to authorize the sharing or receiving of  
12 a cyber threat indicator or countermeasure  
13 other than as provided in this subsection; or

14 (B) to limit otherwise lawful activity.

15 (d) **PROTECTION AND USE OF INFORMATION.**—

16 (1) **SECURITY OF INFORMATION.**—An entity  
17 monitoring an information system, operating a coun-  
18 termeasure, or providing or receiving a cyber threat  
19 indicator or countermeasure under this section shall  
20 implement and utilize a security control to protect  
21 against unauthorized access to or acquisition of such  
22 cyber threat indicator or countermeasure.

23 (2) **REMOVAL OF CERTAIN PERSONAL INFORMA-**  
24 **TION.**—An entity sharing a cyber threat indicator  
25 pursuant to this Act shall, prior to such sharing—

1 (A) review such cyber threat indicator to  
2 assess whether such cyber threat indicator con-  
3 tains any information that the entity knows at  
4 the time of sharing to be personal information  
5 of or identifying a specific person not directly  
6 related to a cybersecurity threat and remove  
7 such information; or

8 (B) implement and utilize a technical capa-  
9 bility to remove any information contained  
10 within such indicator that the entity knows at  
11 the time of sharing to be personal information  
12 of or identifying a specific person not directly  
13 related to a cybersecurity threat.

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

16 (A) IN GENERAL.—Consistent with this  
17 Act, a cyber threat indicator or countermeasure  
18 shared or received under this section may, for  
19 cybersecurity purposes—

20 (i) be used by an entity to monitor or  
21 operate a countermeasure on—

22 (I) an information system of the  
23 entity; or

24 (II) an information system of an-  
25 other entity or a Federal entity upon

1 the written consent of that other enti-  
2 ty or that Federal entity; and

3 (ii) be otherwise used, retained, and  
4 further shared by an entity subject to—

5 (I) an otherwise lawful restriction  
6 placed by the sharing entity or Fed-  
7 eral entity on such cyber threat indi-  
8 cator or countermeasure; or

9 (II) an otherwise applicable pro-  
10 vision of law.

11 (B) CONSTRUCTION.—Nothing in this  
12 paragraph shall be construed to authorize the  
13 use of a cyber threat indicator or counter-  
14 measure other than as provided in this section.

15 (4) USE OF CYBER THREAT INDICATORS BY  
16 STATE, TRIBAL, OR LOCAL GOVERNMENT.—

17 (A) LAW ENFORCEMENT USE.—

18 (i) PRIOR WRITTEN CONSENT.—Ex-  
19 cept as provided in clause (ii), a cyber  
20 threat indicator shared with a State, tribal,  
21 or local government under this section  
22 may, with the prior written consent of the  
23 entity sharing such indicator, be used by a  
24 State, tribal, or local government for the  
25 purpose of preventing, investigating, or

1 prosecuting any of the offenses described  
2 in section 5(d)(5)(A)(vi).

3 (ii) ORAL CONSENT.—If exigent cir-  
4 cumstances prevent obtaining written con-  
5 sent under clause (i), such consent may be  
6 provided orally with subsequent docu-  
7 mentation of the consent.

8 (B) EXEMPTION FROM DISCLOSURE.—A  
9 cyber threat indicator shared with a State, trib-  
10 al, or local government under this section shall  
11 be—

12 (i) deemed voluntarily shared informa-  
13 tion; and

14 (ii) exempt from disclosure under any  
15 State, tribal, or local law requiring disclo-  
16 sure of information or records.

17 (C) STATE, TRIBAL, AND LOCAL REGU-  
18 LATORY AUTHORITY.—

19 (i) AUTHORIZATION.—A cyber threat  
20 indicator shared with a State, tribal, or  
21 local government under this section may,  
22 consistent with State regulatory authority  
23 specifically relating to the prevention or  
24 mitigation of cybersecurity threats to infor-  
25 mation systems, inform the development or

1 implementation of a regulation relating to  
2 such information systems.

3 (ii) LIMITATION.—A cyber threat indi-  
4 cator shared as described in clause (i) shall  
5 not otherwise be directly used by any  
6 State, tribal, or local government to regu-  
7 late a lawful activity of an entity.

8 (e) ANTITRUST EXEMPTION.—

9 (1) IN GENERAL.—Except as provided in sec-  
10 tion 8(e), it shall not be considered a violation of  
11 any provision of antitrust laws for 2 or more private  
12 entities to exchange or provide a cyber threat indi-  
13 cator, or assistance relating to the prevention, inves-  
14 tigation, or mitigation of a cybersecurity threat, for  
15 cybersecurity purposes under this Act.

16 (2) APPLICABILITY.—Paragraph (1) shall apply  
17 only to information that is exchanged or assistance  
18 provided in order to assist with—

19 (A) facilitating the prevention, investiga-  
20 tion, or mitigation of a cybersecurity threat to  
21 an information system or information that is  
22 stored on, processed by, or transiting an infor-  
23 mation system; or

24 (B) communicating or disclosing a cyber  
25 threat indicator to help prevent, investigate, or

1 mitigate the effect of a cybersecurity threat to  
2 an information system or information that is  
3 stored on, processed by, or transiting an infor-  
4 mation system.

5 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber  
6 threat indicator with an entity under this Act shall not  
7 create a right or benefit to similar information by such  
8 entity or any other entity.

9 **SEC. 5. SHARING OF CYBER THREAT INDICATORS AND**  
10 **COUNTERMEASURES WITH THE FEDERAL**  
11 **GOVERNMENT.**

12 (a) REQUIREMENT FOR POLICIES AND PROCE-  
13 DURES.—

14 (1) INTERIM POLICIES AND PROCEDURES.—Not  
15 later than 60 days after the date of the enactment  
16 of this Act, the Attorney General, in coordination  
17 with the heads of the appropriate Federal entities,  
18 shall develop, and submit to Congress, interim poli-  
19 cies and procedures relating to the receipt of cyber  
20 threat indicators and countermeasures by the Fed-  
21 eral Government.

22 (2) FINAL POLICIES AND PROCEDURES.—Not  
23 later than 180 days after the date of the enactment  
24 of this Act, the Attorney General shall, in coordina-  
25 tion with the heads of the appropriate Federal enti-

1 ties, promulgate final policies and procedures relat-  
2 ing to the receipt of cyber threat indicators and  
3 countermeasures by the Federal Government.

4 (3) REQUIREMENTS CONCERNING POLICIES AND  
5 PROCEDURES.—Consistent with the guidelines devel-  
6 oped under subsection (b), the policies and proce-  
7 dures developed and promulgated under this sub-  
8 section shall—

9 (A) ensure that cyber threat indicators  
10 shared with the Federal Government by any en-  
11 tity pursuant to section 4 that are received  
12 through the process described in subsection  
13 (c)—

14 (i) are shared in real time with such  
15 receipt with all of the appropriate Federal  
16 entities;

17 (ii) are not subject to any delay, inter-  
18 ference, or any other action that could im-  
19 pede real-time receipt by all of the appro-  
20 priate Federal entities; and

21 (iii) may be provided to other Federal  
22 entities;

23 (B) ensure that cyber threat indicators  
24 shared with the Federal Government by any en-

1           tity pursuant to section 4 in a manner other  
2           than the process described in subsection (c)—

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

5                   (ii) are not subject to any unnecessary  
6                   delay, interference, or any other action  
7                   that could impede receipt by all of the ap-  
8                   propriate Federal entities; and

9                   (iii) may be provided to other Federal  
10                  entities;

11                (C) consistent with this Act, any other ap-  
12                plicable provisions of law, and the fair informa-  
13                tion practice principles set forth in appendix A  
14                of the document entitled “National Strategy for  
15                Trusted Identities in Cyberspace” and pub-  
16                lished by the President in April, 2011, govern  
17                the retention, use, and dissemination by the  
18                Federal Government of cyber threat indicators  
19                shared with the Federal Government under this  
20                Act, including the extent, if any, to which such  
21                cyber threat indicators may be used by the Fed-  
22                eral Government; and

23                (D) ensure there is—

24                   (i) an audit capability; and

1                   (ii) appropriate sanctions in place for  
2                   officers, employees, or agents of a Federal  
3                   entity who knowingly and willfully conduct  
4                   activities under this Act in an unauthor-  
5                   ized manner.

6           (b) PRIVACY AND CIVIL LIBERTIES.—

7                   (1) GUIDELINES OF ATTORNEY GENERAL.—The  
8           Attorney General shall, in coordination with the  
9           heads of the appropriate Federal agencies and in  
10          consultation with officers designated under section  
11          1062 of the National Security Intelligence Reform  
12          Act of 2004 (42 U.S.C. 2000ee–1), develop and peri-  
13          odically review guidelines relating to privacy and  
14          civil liberties which shall govern the receipt, reten-  
15          tion, use, and dissemination of cyber threat indica-  
16          tors by a Federal entity obtained in connection with  
17          activities authorized in this Act.

18                   (2) CONTENT.—The guidelines developed and  
19          reviewed under paragraph (1) shall, consistent with  
20          the need to protect information systems from cyber-  
21          security threats and mitigate cybersecurity threats—

22                           (A) limit the impact on privacy and civil  
23                   liberties of activities by the Federal Government  
24                   under this Act;

1 (B) limit the receipt, retention, use, and  
2 dissemination of cyber threat indicators con-  
3 taining personal information of or identifying  
4 specific persons, including by establishing—

5 (i) a process for the timely destruction  
6 of information that is known not to be di-  
7 rectly related to uses authorized under this  
8 Act; and

9 (ii) specific limitations on the length  
10 of any period in which a cyber threat indi-  
11 cator may be retained;

12 (C) include requirements to safeguard  
13 cyber threat indicators containing personal in-  
14 formation of or identifying specific persons  
15 from unauthorized access or acquisition, includ-  
16 ing appropriate sanctions for activities by offi-  
17 cers, employees, or agents of the Federal Gov-  
18 ernment in contravention of such guidelines;

19 (D) include procedures for notifying enti-  
20 ties and Federal entities if information received  
21 pursuant to this section that is known or deter-  
22 mined by a Federal entity receiving such infor-  
23 mation not to constitute a cyber threat indi-  
24 cator; and

1           (E) protect the confidentiality of cyber  
2           threat indicators containing personal informa-  
3           tion of or identifying specific persons to the  
4           greatest extent practicable and require recipi-  
5           ents to be informed that such indicators may  
6           only be used for purposes authorized under this  
7           Act.

8           (c) CAPABILITY AND PROCESS WITHIN THE DEPART-  
9           MENT OF HOMELAND SECURITY.—

10           (1) IN GENERAL.—Not later than 90 days after  
11           the date of the enactment of this Act, the Secretary  
12           of Homeland Security, in coordination with the  
13           heads of the appropriate Federal entities, shall de-  
14           velop and implement a capability and process within  
15           the Department of Homeland Security that—

16           (A) shall accept from any entity in real  
17           time cyber threat indicators and counter-  
18           measures, pursuant to this section;

19           (B) shall, upon submittal of the certifi-  
20           cation under paragraph (2) that such capability  
21           and process fully and effectively operates as de-  
22           scribed in such paragraph, be the process by  
23           which the Federal Government receives cyber  
24           threat indicators and countermeasures under  
25           this Act that are shared by a private entity with

1 the Federal Government through electronic mail  
2 or media, an interactive form on an Internet  
3 website, or a real time, automated process be-  
4 tween information systems except—

5 (i) communications between a Federal  
6 entity and a private entity regarding a pre-  
7 viously shared cyber threat indicator;

8 (ii) voluntary or legally compelled par-  
9 ticipation in an open Federal investigation;

10 (iii) communications by a regulated  
11 entity with such entity's Federal regulatory  
12 authority regarding a cybersecurity threat;  
13 and

14 (iv) cyber threat indicators or counter-  
15 measures shared with a Federal entity as  
16 part of a contractual or statutory require-  
17 ment;

18 (C) ensures that all of the appropriate  
19 Federal entities receive such cyber threat indi-  
20 cators in real time with receipt through the  
21 process within the Department of Homeland  
22 Security;

23 (D) is in compliance with the policies, pro-  
24 cedures, and guidelines required by this section;  
25 and

1 (E) does not limit or prohibit otherwise  
2 lawful disclosures of communications, records,  
3 or other information, including reporting of  
4 known or suspect criminal activity, by an entity  
5 to any other entity or a Federal entity.

6 (2) CERTIFICATION.—Not later than 10 days  
7 prior to the implementation of the capability and  
8 process required by paragraph (1), the Secretary of  
9 Homeland Security shall, in consultation with the  
10 heads of the appropriate Federal entities, certify to  
11 Congress whether such capability and process fully  
12 and effectively operates—

13 (A) as the process by which the Federal  
14 Government receives from any entity a cyber  
15 threat indicator or countermeasure under this  
16 Act; and

17 (B) in accordance with the policies, proce-  
18 dures, and guidelines developed under this sec-  
19 tion.

20 (3) PUBLIC NOTICE AND ACCESS.—The Sec-  
21 retary of Homeland Security shall ensure there is  
22 public notice of, and access to, the capability and  
23 process developed and implemented under paragraph  
24 (1) so that—

1 (A) any entity may share cyber threat indi-  
2 cators and countermeasures through such proc-  
3 ess with the Federal Government; and

4 (B) all of the appropriate Federal entities  
5 receive such cyber threat indicators and coun-  
6 termeasures in real time with receipt through  
7 the process within the Department of Home-  
8 land Security.

9 (4) OTHER FEDERAL ENTITIES.—The process  
10 developed and implemented under paragraph (1)  
11 shall ensure that other Federal entities receive in a  
12 timely manner any cyber threat indicators and coun-  
13 termeasures shared with the Federal Government  
14 through such process.

15 (5) REPORT ON DEVELOPMENT AND IMPLE-  
16 MENTATION.—

17 (A) IN GENERAL.—Not later than 60 days  
18 after the date of the enactment of this Act, the  
19 Secretary of Homeland Security shall submit to  
20 Congress a report on the development and im-  
21 plementation of the capability and process re-  
22 quired by paragraph (1), including a description  
23 of such capability and process and the public  
24 notice of, and access to, such process.

1 (B) CLASSIFIED ANNEX.—The report re-  
2 quired by subparagraph (A) shall be submitted  
3 in unclassified form, but may include a classi-  
4 fied annex.

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

7 (1) NO WAIVER OF PRIVILEGE OR PROTEC-  
8 TION.—The provision of cyber threat indicators and  
9 countermeasures to the Federal Government under  
10 this Act shall not constitute a waiver of any applica-  
11 ble privilege or protection provided by law, including  
12 trade secret protection.

13 (2) PROPRIETARY INFORMATION.—A cyber  
14 threat indicator or countermeasure provided by an  
15 entity to the Federal Government under this Act  
16 shall be considered the commercial, financial, and  
17 proprietary information of such entity when so des-  
18 ignated by such entity.

19 (3) EXEMPTION FROM DISCLOSURE.—Cyber  
20 threat indicators and countermeasures provided to  
21 the Federal Government under this Act shall be—

22 (A) deemed voluntarily shared information  
23 and exempt from disclosure under section 552  
24 of title 5, United States Code, and any State,

1 tribal, or local law requiring disclosure of infor-  
2 mation or records; and

3 (B) withheld, without discretion, from the  
4 public under section 552(b)(3)(B) of title 5,  
5 United States Code, and any State, tribal, or  
6 local provision of law requiring disclosure of in-  
7 formation or records.

8 (4) EX PARTE COMMUNICATIONS.—The provi-  
9 sion of a cyber threat indicator or countermeasure to  
10 the Federal Government under this Act shall not be  
11 subject to a rule of any Federal agency or depart-  
12 ment or any judicial doctrine regarding ex parte  
13 communications with a decisionmaking official.

14 (5) DISCLOSURE, RETENTION, AND USE.—

15 (A) AUTHORIZED ACTIVITIES.—Cyber  
16 threat indicators and countermeasures provided  
17 to the Federal Government under this Act may  
18 be disclosed to, retained by, and used by, con-  
19 sistent with otherwise applicable provisions of  
20 Federal law, any Federal agency or department,  
21 component, officer, employee, or agent of the  
22 Federal Government solely for—

23 (i) a cybersecurity purpose;

24 (ii) the purpose of identifying a cyber-  
25 security threat, including the source of

1 such cybersecurity threat, or a security  
2 vulnerability;

3 (iii) the purpose of responding to, or  
4 otherwise preventing or mitigating, an im-  
5minent threat of death or serious bodily  
6harm;

7 (iv) the purpose of responding to, or  
8 otherwise preventing or mitigating, a ter-  
9rorist act or the development or use of  
10weapons of mass destruction;

11 (v) the purpose of responding to, or  
12 otherwise preventing or mitigating, a seri-  
13ous threat to a minor, including sexual ex-  
14ploitation and threats to physical safety; or

15 (vi) the purpose of preventing, inves-  
16tigating, or prosecuting an offense arising  
17out of a threat described in clause (iii), an  
18offense arising out of an act, development,  
19or use described in clause (iv), or any of  
20the offenses listed in—

21 (I) section 3559(c)(2)(F) of title  
2218, United States Code (relating to  
23serious violent felonies);

1 (II) sections 1028 through 1030  
2 of such title (relating to fraud and  
3 identity theft);

4 (III) chapter 37 of such title (re-  
5 lating to espionage and censorship);  
6 and

7 (IV) chapter 90 of such title (re-  
8 lating to protection of trade secrets).

9 (B) PROHIBITED ACTIVITIES.—Cyber  
10 threat indicators and countermeasures provided  
11 to the Federal Government under this Act shall  
12 not be disclosed to, retained by, or used by any  
13 Federal agency or department for any use not  
14 permitted under subparagraph (A).

15 (C) PRIVACY AND CIVIL LIBERTIES.—  
16 Cyber threat indicators and countermeasures  
17 provided to the Federal Government under this  
18 Act shall be retained, used, and disseminated by  
19 the Federal Government—

20 (i) in accordance with the policies,  
21 procedures, and guidelines required by sub-  
22 sections (a) and (b);

23 (ii) in a manner that protects from  
24 unauthorized use or disclosure any cyber  
25 threat indicators that may contain personal

1 information of or identifying specific per-  
2 sons; and

3 (iii) in a manner that protects the  
4 confidentiality of cyber threat indicators  
5 containing information of, or that identi-  
6 fies, a specific person.

7 (D) FEDERAL REGULATORY AUTHORITY.—

8 (i) IN GENERAL.—Except as provided  
9 in clause (ii), cyber threat indicators and  
10 countermeasures provided to the Federal  
11 Government under this Act shall not be di-  
12 rectly used by any Federal, State, tribal,  
13 or local government department or agency  
14 to regulate the lawful activities of any enti-  
15 ty, including activities relating to moni-  
16 toring, operation of countermeasures, or  
17 sharing of cyber threat indicators.

18 (ii) EXCEPTIONS.—

19 (I) REGULATORY AUTHORITY  
20 SPECIFICALLY RELATING TO PREVEN-  
21 TION OR MITIGATION OF CYBERSECU-  
22 RITY THREATS.—Cyber threat indica-  
23 tors and countermeasures provided to  
24 the Federal Government under this  
25 Act may, consistent with Federal or

1 State regulatory authority specifically  
2 relating to the prevention or mitiga-  
3 tion of cybersecurity threats to infor-  
4 mation systems, inform the develop-  
5 ment or implementation of regulations  
6 relating to such information systems.

7 (II) PROCEDURES DEVELOPED  
8 AND IMPLEMENTED UNDER THIS  
9 ACT.—Clause (i) shall not apply to  
10 procedures developed and imple-  
11 mented under this Act.

12 **SEC. 6. PROTECTION FROM LIABILITY.**

13 (a) MONITORING OF INFORMATION SYSTEMS.—No  
14 cause of action shall lie or be maintained in any court  
15 against any private entity, and such action shall be  
16 promptly dismissed, for the monitoring of information sys-  
17 tems and information under subsection (a) of section 4  
18 that is conducted in accordance with this Act.

19 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-  
20 CATORS.—No cause of action shall lie or be maintained  
21 in any court against any entity, and such action shall be  
22 promptly dismissed, for the sharing or receipt of cyber  
23 threat indicators or countermeasures under section 4(c)  
24 if—

1 (1) such sharing or receipt is conducted in ac-  
2 cordance with this Act; and

3 (2) in a case in which a cyber threat indicator  
4 or countermeasure is shared with the Federal Gov-  
5 ernment, the cyber threat indicator or counter-  
6 measure is shared in a manner that is consistent  
7 with section 5(c) and the sharing or receipt, as the  
8 case may be, occurs after the earlier of—

9 (A) the date on which the interim policies  
10 and procedures are submitted to Congress  
11 under section 5(a)(1); or

12 (B) the date that is 60 days after the date  
13 of the enactment of this Act.

14 (c) CONSTRUCTION.—Nothing in this section shall be  
15 construed—

16 (1) to require dismissal of a cause of action  
17 against an entity that has engaged in gross neg-  
18 ligence or willful misconduct in the course of con-  
19 ducting activities authorized by this Act; or

20 (2) to undermine or limit the availability of oth-  
21 erwise applicable common law or statutory defenses.

22 **SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

23 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

24 (1) IN GENERAL.—Not later than 1 year after  
25 the date of the enactment of this Act, and not less

1 frequently than once every 2 years thereafter, the  
2 heads of the appropriate Federal entities shall joint-  
3 ly submit to Congress a detailed report concerning  
4 the implementation of this Act.

5 (2) CONTENTS.—Each report submitted under  
6 paragraph (1) shall include the following:

7 (A) An assessment of the sufficiency of the  
8 policies, procedures, and guidelines required by  
9 section 5 in ensuring that cyber threat indica-  
10 tors are shared effectively and responsibly with-  
11 in the Federal Government.

12 (B) An evaluation of the effectiveness of  
13 real-time information sharing through the capa-  
14 bility and process developed under section 5(c),  
15 including any impediments to such real-time  
16 sharing.

17 (C) An assessment of the sufficiency of the  
18 procedures developed under section 3 in ensur-  
19 ing that cyber threat indicators in the posses-  
20 sion of the Federal Government are shared in  
21 a timely and adequate manner with appropriate  
22 entities, or, if appropriate, are made publicly  
23 available.

24 (D) An assessment of whether cyber threat  
25 indicators have been properly classified and an

1 accounting of the number of security clearances  
2 authorized by the Federal Government for the  
3 purposes of this Act.

4 (E) A review of the type of cyber threat in-  
5 dicators shared with the Federal Government  
6 under this Act, including the following:

7 (i) The degree to which such informa-  
8 tion may impact the privacy and civil lib-  
9 erties of specific persons.

10 (ii) A quantitative and qualitative as-  
11 sessment of the impact of the sharing of  
12 such cyber threat indicators with the Fed-  
13 eral Government on privacy and civil lib-  
14 erties of specific persons.

15 (iii) The adequacy of any steps taken  
16 by the Federal Government to reduce such  
17 impact.

18 (F) A review of actions taken by the Fed-  
19 eral Government based on cyber threat indica-  
20 tors shared with the Federal Government under  
21 this Act, including the appropriateness of any  
22 subsequent use or dissemination of such cyber  
23 threat indicators by a Federal entity under sec-  
24 tion 5.

1 (G) A description of any significant viola-  
2 tions of the requirements of this Act by the  
3 Federal Government.

4 (H) A classified summary of the number  
5 and type of entities that received classified  
6 cyber threat indicators from the Federal Gov-  
7 ernment under this Act and an evaluation of  
8 the risks and benefits of sharing such cyber  
9 threat indicators.

10 (3) RECOMMENDATIONS.—Each report sub-  
11 mitted under paragraph (1) may include such rec-  
12 ommendations as the heads of the appropriate Fed-  
13 eral entities may have for improvements or modifica-  
14 tions to the authorities and processes under this Act.

15 (4) FORM OF REPORT.—Each report required  
16 by paragraph (1) shall be submitted in unclassified  
17 form, but shall include a classified annex.

18 (b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

19 (1) BIENNIAL REPORT FROM PRIVACY AND  
20 CIVIL LIBERTIES OVERSIGHT BOARD.—Not later  
21 than 2 years after the date of the enactment of this  
22 Act and not less frequently than once every 2 years  
23 thereafter, the Privacy and Civil Liberties Oversight  
24 Board shall submit to Congress and the President a  
25 report providing—

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

4 (B) an assessment of the sufficiency of the  
5 policies, procedures, and guidelines established  
6 pursuant to section 5 in addressing privacy and  
7 civil liberties concerns.

8 (2) BIENNIAL REPORT OF INSPECTORS GEN-  
9 ERAL.—

10 (A) IN GENERAL.—Not later than 2 years  
11 after the date of the enactment of this Act and  
12 not less frequently than once every 2 years  
13 thereafter, the Inspector General of the Depart-  
14 ment of Homeland Security, the Inspector Gen-  
15 eral of the Intelligence Community, the Inspec-  
16 tor General of the Department of Justice, the  
17 Inspector General of the Department of De-  
18 fense shall, in consultation with the Council of  
19 Inspectors General on Financial Oversight,  
20 jointly submit to Congress a report on the re-  
21 ceipt, use, and dissemination of cyber threat in-  
22 dicators and countermeasures that have been  
23 shared with Federal entities under this Act.

1 (B) CONTENTS.—Each report submitted  
2 under subparagraph (A) shall include the fol-  
3 lowing:

4 (i) A review of the types of cyber  
5 threat indicators shared with Federal enti-  
6 ties.

7 (ii) A review of the actions taken by  
8 Federal entities as a result of the receipt  
9 of such cyber threat indicators.

10 (iii) A list of Federal entities receiving  
11 such cyber threat indicators.

12 (iv) A review of the sharing of such  
13 cyber threat indicators among Federal en-  
14 tities to identify inappropriate barriers to  
15 sharing information.

16 (3) RECOMMENDATIONS.—Each report sub-  
17 mitted under this subsection may include such rec-  
18 ommendations as the Privacy and Civil Liberties  
19 Oversight Board, with respect to a report submitted  
20 under paragraph (1), or the Inspectors General re-  
21 ferred to in paragraph (2)(A), with respect to a re-  
22 port submitted under paragraph (2), may have for  
23 improvements or modifications to the authorities  
24 under this Act.

1           (4) FORM.—Each report required under this  
2           subsection shall be submitted in unclassified form,  
3           but may include a classified annex.

4 **SEC. 8. CONSTRUCTION AND PREEMPTION.**

5           (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in  
6 this Act shall be construed to limit or prohibit otherwise  
7 lawful disclosures of communications, records, or other in-  
8 formation, including reporting of known or suspected  
9 criminal activity, by an entity to any other entity or the  
10 Federal Government under this Act.

11          (b) WHISTLE BLOWER PROTECTIONS.—Nothing in  
12 this Act shall be construed to prohibit or limit the dislo-  
13 sure of information protected under section 2302(b)(8) of  
14 title 5, United States Code (governing disclosures of ille-  
15 gality, waste, fraud, abuse, or public health or safety  
16 threats), section 7211 of title 5, United States Code (gov-  
17 erning disclosures to Congress), section 1034 of title 10,  
18 United States Code (governing disclosure to Congress by  
19 members of the military), section 1104 of the National  
20 Security Act of 1947 (50 U.S.C. 3234) (governing dislo-  
21 sure by employees of elements of the intelligence commu-  
22 nity), or any similar provision of Federal or State law.

23          (c) PROTECTION OF SOURCES AND METHODS.—  
24 Nothing in this Act shall be construed—

1           (1) as creating any immunity against, or other-  
2           wise affecting, any action brought by the Federal  
3           Government, or any agency or department thereof,  
4           to enforce any law, executive order, or procedure  
5           governing the appropriate handling, disclosure, or  
6           use of classified information;

7           (2) to affect the conduct of authorized law en-  
8           forcement or intelligence activities; or

9           (3) to modify the authority of a department or  
10          agency of the Federal Government to protect sources  
11          and methods and the national security of the United  
12          States.

13          (d) RELATIONSHIP TO OTHER LAWS.—Nothing in  
14          this Act shall be construed to affect any requirement  
15          under any other provision of law for an entity to provide  
16          information to the Federal Government.

17          (e) PROHIBITED CONDUCT.—Nothing in this Act  
18          shall be construed to permit price-fixing, allocating a mar-  
19          ket between competitors, monopolizing or attempting to  
20          monopolize a market, boycotting, or exchanges of price or  
21          cost information, customer lists, or information regarding  
22          future competitive planning.

23          (f) INFORMATION SHARING RELATIONSHIPS.—Noth-  
24          ing in this Act shall be construed—

1 (1) to limit or modify an existing information  
2 sharing relationship;

3 (2) to prohibit a new information sharing rela-  
4 tionship;

5 (3) to require a new information sharing rela-  
6 tionship between any entity and the Federal Govern-  
7 ment; or

8 (4) to require the use of the capability and  
9 process within the Department of Homeland Secu-  
10 rity developed under section 5(c).

11 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS  
12 AND RIGHTS.—Nothing in this Act shall be construed—

13 (1) to amend, repeal, or supersede any current  
14 or future contractual agreement, terms of service  
15 agreement, or other contractual relationship between  
16 any entities, or between any entity and a Federal en-  
17 tity; or

18 (2) to abrogate trade secret or intellectual prop-  
19 erty rights of any entity or Federal entity.

20 (h) ANTI-TASKING RESTRICTION.—Nothing in this  
21 Act shall be construed to permit the Federal Govern-  
22 ment—

23 (1) to require an entity to provide information  
24 to the Federal Government;

1           (2) to condition the sharing of cyber threat in-  
2           dicators with an entity on such entity's provision of  
3           cyber threat indicators to the Federal Government;  
4           or

5           (3) to condition the award of any Federal  
6           grant, contract, or purchase on the provision of a  
7           cyber threat indicator to a Federal entity.

8           (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-  
9           ing in this Act shall be construed to subject any entity  
10          to liability for choosing not to engage in the voluntary ac-  
11          tivities authorized in this Act.

12          (j) USE AND RETENTION OF INFORMATION.—Noth-  
13          ing in this Act shall be construed to authorize, or to mod-  
14          ify any existing authority of, a department or agency of  
15          the Federal Government to retain or use any information  
16          shared under this Act for any use other than permitted  
17          in this Act.

18          (k) FEDERAL PREEMPTION.—

19                (1) IN GENERAL.—This Act supersedes any  
20                statute or other provision of law of a State or polit-  
21                ical subdivision of a State that restricts or otherwise  
22                expressly regulates an activity authorized under this  
23                Act.

24                (2) STATE LAW ENFORCEMENT.—Nothing in  
25                this Act shall be construed to supersede any statute

1 or other provision of law of a State or political sub-  
2 division of a State concerning the use of authorized  
3 law enforcement practices and procedures.

4 (l) REGULATORY AUTHORITY.—Nothing in this Act  
5 shall be construed—

6 (1) to authorize the promulgation of any regu-  
7 lations not specifically authorized by this Act;

8 (2) to establish or limit any regulatory author-  
9 ity not specifically established or limited under this  
10 Act; or

11 (3) to authorize regulatory actions that would  
12 duplicate or conflict with regulatory requirements,  
13 mandatory standards, or related processes under an-  
14 other provision of Federal law.

15 (m) AUTHORITY OF SECRETARY OF DEFENSE TO  
16 RESPOND TO CYBER ATTACKS.—Nothing in this Act shall  
17 be construed to limit the authority of the Secretary of De-  
18 fense to develop, prepare, coordinate, or, when directed by  
19 the President to do so, conduct a military cyber operation  
20 in response to a cyber attack carried out against the  
21 United States or a United States person by a foreign gov-  
22 ernment or an organization sponsored by a foreign govern-  
23 ment.

1 **SEC. 9. REPORT ON CYBERSECURITY THREATS.**

2 (a) REPORT REQUIRED.—Not later than 180 days  
3 after the date of the enactment of this Act, the Director  
4 of National Intelligence, in coordination with the heads of  
5 other appropriate elements of the intelligence community,  
6 shall submit to the Select Committee on Intelligence of  
7 the Senate and the Permanent Select Committee on Intel-  
8 ligence of the House of Representatives a report on cyber-  
9 security threats, including cyber attacks, theft, and data  
10 breaches.

11 (b) CONTENTS.—The report required by subsection  
12 (a) shall include the following:

13 (1) An assessment of the current intelligence  
14 sharing and cooperation relationships of the United  
15 States with other countries regarding cybersecurity  
16 threats, including cyber attacks, theft, and data  
17 breaches, directed against the United States and  
18 which threaten the United States national security  
19 interests and economy and intellectual property, spe-  
20 cifically identifying the relative utility of such rela-  
21 tionships, which elements of the intelligence commu-  
22 nity participate in such relationships, and whether  
23 and how such relationships could be improved.

24 (2) A list and an assessment of the countries  
25 and nonstate actors that are the primary threats of  
26 carrying out a cybersecurity threat, including a

1 cyber attack, theft, or data breach, against the  
2 United States and which threaten the United States  
3 national security, economy, and intellectual property.

4 (3) A description of the extent to which the ca-  
5 pabilities of the United States Government to re-  
6 spond to or prevent cybersecurity threats, including  
7 cyber attacks, theft, or data breaches, directed  
8 against the United States private sector are de-  
9 graded by a delay in the prompt notification by pri-  
10 vate entities of such threats or cyber attacks, theft,  
11 and breaches.

12 (4) An assessment of additional technologies or  
13 capabilities that would enhance the ability of the  
14 United States to prevent and to respond to cyberse-  
15 curity threats, including cyber attacks, theft, and  
16 data breaches.

17 (5) An assessment of any technologies or prac-  
18 tices utilized by the private sector that could be rap-  
19 idly fielded to assist the intelligence community in  
20 preventing and responding to cybersecurity threats.

21 (c) FORM OF REPORT.—The report required by sub-  
22 section (a) shall be made available in classified and unclas-  
23 sified forms.

24 (d) INTELLIGENCE COMMUNITY DEFINED.—In this  
25 section, the term “intelligence community” has the mean-

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

3 **SEC. 10. CONFORMING AMENDMENTS.**

4 (a) PUBLIC INFORMATION.—Section 552(b) of title  
5 5, United States Code, is amended—

6 (1) in paragraph (8), by striking “or” at the  
7 end;

8 (2) in paragraph (9), by striking “wells.” and  
9 inserting “wells; or”; and

10 (3) by inserting after paragraph (9) the fol-  
11 lowing:

12 “(10) information shared with or provided to  
13 the Federal Government pursuant to the Cybersecu-  
14 rity Information Sharing Act of 2015.”.

15 (b) MODIFICATION OF LIMITATION ON DISSEMINA-  
16 TION OF CERTAIN INFORMATION CONCERNING PENETRA-  
17 TIONS OF DEFENSE CONTRACTOR NETWORKS.—Section  
18 941(e)(3) of the National Defense Authorization Act for  
19 Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224  
20 note) is amended by inserting at the end the following:  
21 “The Secretary may share such information with other  
22 Federal entities if such information consists of cyber  
23 threat indicators and countermeasures and such informa-  
24 tion is shared consistent with the policies and procedures

1 promulgated by the Attorney General under section 5 of  
2 the Cybersecurity Information Sharing Act of 2015.”.