

1           **TITLE I—CYBERSECURITY**  
2           **INFORMATION SHARING**

3 **SEC. 101. SHORT TITLE.**

4           This title may be cited as the “Cybersecurity Infor-  
5 mation Sharing Act of 2015”.

6 **SEC. 102. DEFINITIONS.**

7           In this title:

8           (1) **AGENCY.**—The term “agency” has the  
9 meaning given the term in section 3502 of title 44,  
10 United States Code.

11           (2) **ANTITRUST LAWS.**—The term “antitrust  
12 laws”—

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

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

19           (C) includes any State law that has the  
20 same intent and effect as the laws under sub-  
21 paragraphs (A) and (B).

22           (3) **APPROPRIATE FEDERAL ENTITIES.**—The  
23 term “appropriate Federal entities” means the fol-  
24 lowing:

25           (A) The Department of Commerce.

1 (B) The Department of Defense.

2 (C) The Department of Energy.

3 (D) The Department of Homeland Secu-  
4 rity.

5 (E) The Department of Justice.

6 (F) The Department of the Treasury.

7 (G) The Office of the Director of National  
8 Intelligence.

9 (4) CYBERSECURITY PURPOSE.—The term “cy-  
10 bersecurity purpose” means the purpose of pro-  
11 tecting an information system or information that is  
12 stored on, processed by, or transiting an information  
13 system from a cybersecurity threat or security vul-  
14 nerability.

15 (5) CYBERSECURITY THREAT.—

16 (A) IN GENERAL.—Except as provided in  
17 subparagraph (B), the term “cybersecurity  
18 threat” means an action, not protected by the  
19 First Amendment to the Constitution of the  
20 United States, on or through an information  
21 system that may result in an unauthorized ef-  
22 fort to adversely impact the security, avail-  
23 ability, confidentiality, or integrity of an infor-  
24 mation system or information that is stored on,

1 processed by, or transiting an information sys-  
2 tem.

3 (B) EXCLUSION.—The term “cybersecurity  
4 threat” does not include any action that solely  
5 involves a violation of a consumer term of serv-  
6 ice or a consumer licensing agreement.

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

10 (A) malicious reconnaissance, including  
11 anomalous patterns of communications that ap-  
12 pear to be transmitted for the purpose of gath-  
13 ering technical information related to a cyberse-  
14 curity threat or security vulnerability;

15 (B) a method of defeating a security con-  
16 trol or exploitation of a security vulnerability;

17 (C) a security vulnerability, including  
18 anomalous activity that appears to indicate the  
19 existence of a security vulnerability;

20 (D) a method of causing a user with legiti-  
21 mate access to an information system or infor-  
22 mation that is stored on, processed by, or  
23 transiting an information system to unwittingly  
24 enable the defeat of a security control or exploi-  
25 tation of a security vulnerability;

1 (E) malicious cyber command and control;

2 (F) the actual or potential harm caused by  
3 an incident, including a description of the infor-  
4 mation exfiltrated as a result of a particular cy-  
5 bersecurity threat;

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

9 (H) any combination thereof.

10 (7) DEFENSIVE MEASURE.—

11 (A) IN GENERAL.—Except as provided in  
12 subparagraph (B), the term “defensive meas-  
13 ure” means an action, device, procedure, signa-  
14 ture, technique, or other measure applied to an  
15 information system or information that is  
16 stored on, processed by, or transiting an infor-  
17 mation system that detects, prevents, or miti-  
18 gates a known or suspected cybersecurity threat  
19 or security vulnerability.

20 (B) EXCLUSION.—The term “defensive  
21 measure” does not include a measure that de-  
22 stroys, renders unusable, provides unauthorized  
23 access to, or substantially harms an information  
24 system or data on an information system not  
25 belonging to—

1 (i) the private entity operating the  
2 measure; or

3 (ii) another entity or Federal entity  
4 that is authorized to provide consent and  
5 has provided consent to that private entity  
6 for operation of such measure.

7 (8) ENTITY.—

8 (A) IN GENERAL.—Except as otherwise  
9 provided in this paragraph, the term “entity”  
10 means any private entity, non-Federal govern-  
11 ment agency or department, or State, tribal, or  
12 local government (including a political subdivi-  
13 sion, department, or component thereof).

14 (B) INCLUSIONS.—The term “entity” in-  
15 cludes a government agency or department of  
16 the District of Columbia, the Commonwealth of  
17 Puerto Rico, the Virgin Islands, Guam, Amer-  
18 ican Samoa, the Northern Mariana Islands, and  
19 any other territory or possession of the United  
20 States.

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

1           (9) FEDERAL ENTITY.—The term “Federal en-  
2           tity” means a department or agency of the United  
3           States or any component of such department or  
4           agency.

5           (10) INFORMATION SYSTEM.—The term “infor-  
6           mation system”—

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

9                   (B) includes industrial control systems,  
10                  such as supervisory control and data acquisition  
11                  systems, distributed control systems, and pro-  
12                  grammable logic controllers.

13           (11) LOCAL GOVERNMENT.—The term “local  
14           government” means any borough, city, county, par-  
15           ish, town, township, village, or other political sub-  
16           division of a State.

17           (12) MALICIOUS CYBER COMMAND AND CON-  
18           TROL.—The term “malicious cyber command and  
19           control” means a method for unauthorized remote  
20           identification of, access to, or use of, an information  
21           system or information that is stored on, processed  
22           by, or transiting an information system.

23           (13) MALICIOUS RECONNAISSANCE.—The term  
24           “malicious reconnaissance” means a method for ac-  
25           tively probing or passively monitoring an information

1 system for the purpose of discerning security  
2 vulnerabilities of the information system, if such  
3 method is associated with a known or suspected cy-  
4 bersecurity threat.

5 (14) MONITOR.—The term “monitor” means to  
6 acquire, identify, or scan, or to possess, information  
7 that is stored on, processed by, or transiting an in-  
8 formation system.

9 (15) PRIVATE ENTITY.—

10 (A) IN GENERAL.—Except as otherwise  
11 provided in this paragraph, the term “private  
12 entity” means any person or private group, or-  
13 ganization, proprietorship, partnership, trust,  
14 cooperative, corporation, or other commercial or  
15 nonprofit entity, including an officer, employee,  
16 or agent thereof.

17 (B) INCLUSION.—The term “private enti-  
18 ty” includes a State, tribal, or local government  
19 performing electric or other utility services.

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

24 (16) SECURITY CONTROL.—The term “security  
25 control” means the management, operational, and

1 technical controls used to protect against an unau-  
2 thorized effort to adversely affect the confidentiality,  
3 integrity, and availability of an information system  
4 or its information.

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

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

13 **SEC. 103. SHARING OF INFORMATION BY THE FEDERAL**  
14 **GOVERNMENT.**

15 (a) IN GENERAL.—Consistent with the protection of  
16 classified information, intelligence sources and methods,  
17 and privacy and civil liberties, the Director of National  
18 Intelligence, the Secretary of Homeland Security, the Sec-  
19 retary of Defense, and the Attorney General, in consulta-  
20 tion with the heads of the appropriate Federal entities,  
21 shall develop and promulgate procedures to facilitate and  
22 promote—

23 (1) the timely sharing of classified cyber threat  
24 indicators in the possession of the Federal Govern-

1 ment with cleared representatives of relevant enti-  
2 ties;

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

7 (3) the sharing with relevant entities, or the  
8 public if appropriate, of unclassified, including con-  
9 trolled unclassified, cyber threat indicators in the  
10 possession of the Federal Government;

11 (4) the sharing with entities, if appropriate, of  
12 information in the possession of the Federal Govern-  
13 ment about cybersecurity threats to such entities to  
14 prevent or mitigate adverse effects from such cyber-  
15 security threats; and

16 (5) the periodic sharing, through publication  
17 and targeted outreach, of cybersecurity best prac-  
18 tices that are developed based on ongoing analysis of  
19 cyber threat indicators and information in possession  
20 of the Federal Government, with attention to acces-  
21 sibility and implementation challenges faced by small  
22 business concerns (as defined in section 3 of the  
23 Small Business Act (15 U.S.C. 632)).

24 (b) DEVELOPMENT OF PROCEDURES.—

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

3           (A) ensure the Federal Government has  
4 and maintains the capability to share cyber  
5 threat indicators in real time consistent with  
6 the protection of classified information;

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

13           (C) include procedures for notifying, in a  
14 timely manner, entities that have received a  
15 cyber threat indicator from a Federal entity  
16 under this title that is known or determined to  
17 be in error or in contravention of the require-  
18 ments of this title or another provision of Fed-  
19 eral law or policy of such error or contraven-  
20 tion;

21           (D) include requirements for Federal enti-  
22 ties sharing cyber threat indicators or defensive  
23 measures to implement and utilize security con-  
24 trols to protect against unauthorized access to

1 or acquisition of such cyber threat indicators or  
2 defensive measures;

3 (E) include procedures that require a Fed-  
4 eral entity, prior to the sharing of a cyber  
5 threat indicator—

6 (i) to review such cyber threat indi-  
7 cator to assess whether such cyber threat  
8 indicator contains any information that  
9 such Federal entity knows at the time of  
10 sharing to be personal information or in-  
11 formation that identifies a specific person  
12 not directly related to a cybersecurity  
13 threat and remove such information; or

14 (ii) to implement and utilize a tech-  
15 nical capability configured to remove any  
16 personal information or information that  
17 identifies a specific person not directly re-  
18 lated to a cybersecurity threat; and

19 (F) include procedures for notifying, in a  
20 timely manner, any United States person whose  
21 personal information is known or determined to  
22 have been shared by a Federal entity in viola-  
23 tion of this Act.

24 (2) COORDINATION.—In developing the proce-  
25 dures required under this section, the Director of

1 National Intelligence, the Secretary of Homeland Se-  
2 curity, the Secretary of Defense, and the Attorney  
3 General shall coordinate with appropriate Federal  
4 entities, including the Small Business Administra-  
5 tion and the National Laboratories (as defined in  
6 section 2 of the Energy Policy Act of 2005 (42  
7 U.S.C. 15801)), to ensure that effective protocols  
8 are implemented that will facilitate and promote the  
9 sharing of cyber threat indicators by the Federal  
10 Government in a timely manner.

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

16 **SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
17 **ANALYZING, AND MITIGATING CYBERSECU-**  
18 **RITY THREATS.**

19 (a) AUTHORIZATION FOR MONITORING.—

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

23 (A) an information system of such private  
24 entity;

1 (B) an information system of another enti-  
2 ty, upon the authorization and written consent  
3 of such other entity;

4 (C) an information system of a Federal en-  
5 tity, upon the authorization and written consent  
6 of an authorized representative of the Federal  
7 entity; and

8 (D) information that is stored on, proc-  
9 essed by, or transiting an information system  
10 monitored by the private entity under this para-  
11 graph.

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

14 (A) to authorize the monitoring of an in-  
15 formation system, or the use of any information  
16 obtained through such monitoring, other than  
17 as provided in this title; or

18 (B) to limit otherwise lawful activity.

19 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE  
20 MEASURES.—

21 (1) IN GENERAL.—Notwithstanding any other  
22 provision of law, a private entity may, for cybersecu-  
23 rity purposes, operate a defensive measure that is  
24 applied to—

1 (A) an information system of such private  
2 entity in order to protect the rights or property  
3 of the private entity;

4 (B) an information system of another enti-  
5 ty upon written consent of such entity for oper-  
6 ation of such defensive measure to protect the  
7 rights or property of such entity; and

8 (C) an information system of a Federal en-  
9 tity upon written consent of an authorized rep-  
10 resentative of such Federal entity for operation  
11 of such defensive measure to protect the rights  
12 or property of the Federal Government.

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

15 (A) to authorize the use of a defensive  
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 DEFENSIVE MEAS-  
21 URES.—

22 (1) IN GENERAL.—Except as provided in para-  
23 graph (2) and notwithstanding any other provision  
24 of law, an entity may, for a cybersecurity purpose  
25 and consistent with the protection of classified infor-

1 mation, share with, or receive from, any other entity  
2 or the Federal Government a cyber threat indicator  
3 or defensive measure.

4 (2) **LAWFUL RESTRICTION.**—An entity receiving  
5 a cyber threat indicator or defensive measure from  
6 another entity or Federal entity shall comply with  
7 otherwise lawful restrictions placed on the sharing or  
8 use of such cyber threat indicator or defensive meas-  
9 ure by the sharing entity or Federal entity.

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

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

15 (B) to limit otherwise lawful activity.

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

17 (1) **SECURITY OF INFORMATION.**—An entity  
18 monitoring an information system, operating a de-  
19 fensive measure, or providing or receiving a cyber  
20 threat indicator or defensive measure under this sec-  
21 tion shall implement and utilize a security control to  
22 protect against unauthorized access to or acquisition  
23 of such cyber threat indicator or defensive measure.

1           (2) REMOVAL OF CERTAIN PERSONAL INFORMA-  
2           TION.—An entity sharing a cyber threat indicator  
3           pursuant to this title shall, prior to such sharing—

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

11                   (B) implement and utilize a technical capa-  
12                   bility configured to remove any information  
13                   contained within such indicator that the entity  
14                   knows at the time of sharing to be personal in-  
15                   formation or information that identifies a spe-  
16                   cific person not directly related to a cybersecu-  
17                   rity threat.

18           (3) USE OF CYBER THREAT INDICATORS AND  
19           DEFENSIVE MEASURES BY ENTITIES.—

20                   (A) IN GENERAL.—Consistent with this  
21                   title, a cyber threat indicator or defensive meas-  
22                   ure shared or received under this section may,  
23                   for cybersecurity purposes—

1 (i) be used by an entity to monitor or  
2 operate a defensive measure that is applied  
3 to—

4 (I) an information system of the  
5 entity; or

6 (II) an information system of an-  
7 other entity or a Federal entity upon  
8 the written consent of that other enti-  
9 ty or that Federal entity; and

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

12 (I) an otherwise lawful restriction  
13 placed by the sharing entity or Fed-  
14 eral entity on such cyber threat indi-  
15 cator or defensive measure; or

16 (II) an otherwise applicable pro-  
17 vision of law.

18 (B) CONSTRUCTION.—Nothing in this  
19 paragraph shall be construed to authorize the  
20 use of a cyber threat indicator or defensive  
21 measure other than as provided in this section.

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

24 (A) LAW ENFORCEMENT USE.—

1 (i) PRIOR WRITTEN CONSENT.—Ex-  
2 cept as provided in clause (ii), a cyber  
3 threat indicator shared with a State, tribal,  
4 or local government under this section  
5 may, with the prior written consent of the  
6 entity sharing such indicator, be used by a  
7 State, tribal, or local government for the  
8 purpose of preventing, investigating, or  
9 prosecuting any of the offenses described  
10 in section 105(d)(5)(A)(vi).

11 (ii) ORAL CONSENT.—If exigent cir-  
12 cumstances prevent obtaining written con-  
13 sent under clause (i), such consent may be  
14 provided orally with subsequent docu-  
15 mentation of the consent.

16 (B) EXEMPTION FROM DISCLOSURE.—A  
17 cyber threat indicator shared with a State, trib-  
18 al, or local government under this section shall  
19 be—

20 (i) deemed voluntarily shared informa-  
21 tion; and

22 (ii) exempt from disclosure under any  
23 State, tribal, or local law requiring disclo-  
24 sure of information or records.

1 (C) STATE, TRIBAL, AND LOCAL REGU-  
2 LATORY AUTHORITY.—

3 (i) IN GENERAL.—Except as provided  
4 in clause (ii), a cyber threat indicator or  
5 defensive measure shared with a State,  
6 tribal, or local government under this title  
7 shall not be directly used by any State,  
8 tribal, or local government to regulate, in-  
9 cluding an enforcement action, the lawful  
10 activity of any entity, including an activity  
11 relating to monitoring, operating a defen-  
12 sive measure, or sharing of a cyber threat  
13 indicator.

14 (ii) REGULATORY AUTHORITY SPE-  
15 CIFICALLY RELATING TO PREVENTION OR  
16 MITIGATION OF CYBERSECURITY  
17 THREATS.—A cyber threat indicator or de-  
18 fensive measure shared as described in  
19 clause (i) may, consistent with a State,  
20 tribal, or local government regulatory au-  
21 thority specifically relating to the preven-  
22 tion or mitigation of cybersecurity threats  
23 to information systems, inform the devel-  
24 opment or implementation of a regulation  
25 relating to such information systems.

1 (e) ANTITRUST EXEMPTION.—

2 (1) IN GENERAL.—Except as provided in sec-  
3 tion 108(e), it shall not be considered a violation of  
4 any provision of antitrust laws for 2 or more private  
5 entities to exchange or provide a cyber threat indi-  
6 cator, or assistance relating to the prevention, inves-  
7 tigation, or mitigation of a cybersecurity threat, for  
8 cybersecurity purposes under this title.

9 (2) APPLICABILITY.—Paragraph (1) shall apply  
10 only to information that is exchanged or assistance  
11 provided in order to assist with—

12 (A) facilitating the prevention, investiga-  
13 tion, or mitigation of a cybersecurity threat to  
14 an information system or information that is  
15 stored on, processed by, or transiting an infor-  
16 mation system; or

17 (B) communicating or disclosing a cyber  
18 threat indicator to help prevent, investigate, or  
19 mitigate the effect of a cybersecurity threat to  
20 an information system or information that is  
21 stored on, processed by, or transiting an infor-  
22 mation system.

23 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber  
24 threat indicator with an entity under this title shall not

1 create a right or benefit to similar information by such  
2 entity or any other entity.

3 **SEC. 105. SHARING OF CYBER THREAT INDICATORS AND**  
4 **DEFENSIVE MEASURES WITH THE FEDERAL**  
5 **GOVERNMENT.**

6 (a) REQUIREMENT FOR POLICIES AND PROCE-  
7 DURES.—

8 (1) INTERIM POLICIES AND PROCEDURES.—Not  
9 later than 60 days after the date of the enactment  
10 of this Act, the Attorney General and the Secretary  
11 of Homeland Security shall, in coordination with the  
12 heads of the appropriate Federal entities, develop  
13 and submit to Congress interim policies and proce-  
14 dures relating to the receipt of cyber threat indica-  
15 tors and defensive measures by the Federal Govern-  
16 ment.

17 (2) FINAL POLICIES AND PROCEDURES.—Not  
18 later than 180 days after the date of the enactment  
19 of this Act, the Attorney General and the Secretary  
20 of Homeland Security shall, in coordination with the  
21 heads of the appropriate Federal entities, promul-  
22 gate final policies and procedures relating to the re-  
23 ceipt of cyber threat indicators and defensive meas-  
24 ures by the Federal Government.

1           (3) REQUIREMENTS CONCERNING POLICIES AND  
2 PROCEDURES.—Consistent with the guidelines re-  
3 quired by subsection (b), the policies and procedures  
4 developed and promulgated under this subsection  
5 shall—

6           (A) ensure that cyber threat indicators  
7 shared with the Federal Government by any en-  
8 tity pursuant to section 104(c) through the  
9 real-time process described in subsection (c) of  
10 this section—

11           (i) are shared in an automated man-  
12 ner with all of the appropriate Federal en-  
13 tities;

14           (ii) are only subject to a delay, modi-  
15 fication, or other action due to controls es-  
16 tablished for such real-time process that  
17 could impede real-time receipt by all of the  
18 appropriate Federal entities when the  
19 delay, modification, or other action is due  
20 to controls—

21           (I) agreed upon unanimously by  
22 all of the heads of the appropriate  
23 Federal entities;

24           (II) carried out before any of the  
25 appropriate Federal entities retains or

1 uses the cyber threat indicators or de-  
2 fensive measures; and

3 (III) uniformly applied such that  
4 each of the appropriate Federal enti-  
5 ties is subject to the same delay,  
6 modification, or other action; and

7 (iii) may be provided to other Federal  
8 entities;

9 (B) ensure that cyber threat indicators  
10 shared with the Federal Government by any en-  
11 tity pursuant to section 104 in a manner other  
12 than the real time process described in sub-  
13 section (c) of this section—

14 (i) are shared as quickly as operation-  
15 ally practicable with all of the appropriate  
16 Federal entities;

17 (ii) are not subject to any unnecessary  
18 delay, interference, or any other action  
19 that could impede receipt by all of the ap-  
20 propriate Federal entities; and

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

23 (C) consistent with this title, any other ap-  
24 plicable provisions of law, and the fair informa-  
25 tion practice principles set forth in appendix A

1 of the document entitled “National Strategy for  
2 Trusted Identities in Cyberspace” and pub-  
3 lished by the President in April, 2011, govern  
4 the retention, use, and dissemination by the  
5 Federal Government of cyber threat indicators  
6 shared with the Federal Government under this  
7 title, including the extent, if any, to which such  
8 cyber threat indicators may be used by the Fed-  
9 eral Government; and

10 (D) ensure there are—

11 (i) audit capabilities; and

12 (ii) appropriate sanctions in place for  
13 officers, employees, or agents of a Federal  
14 entity who knowingly and willfully conduct  
15 activities under this title in an unauthor-  
16 ized manner.

17 (4) GUIDELINES FOR ENTITIES SHARING CYBER  
18 THREAT INDICATORS WITH FEDERAL GOVERN-  
19 MENT.—

20 (A) IN GENERAL.—Not later than 60 days  
21 after the date of the enactment of this Act, the  
22 Attorney General and the Secretary of Home-  
23 land Security shall develop and make publicly  
24 available guidance to assist entities and pro-

1           mote sharing of cyber threat indicators with  
2           Federal entities under this title.

3           (B) CONTENTS.—The guidelines developed  
4           and made publicly available under subpara-  
5           graph (A) shall include guidance on the fol-  
6           lowing:

7                   (i) Identification of types of informa-  
8                   tion that would qualify as a cyber threat  
9                   indicator under this title that would be un-  
10                  likely to include personal information or in-  
11                  formation that identifies a specific person  
12                  not directly related to a cyber security  
13                  threat.

14                  (ii) Identification of types of informa-  
15                  tion protected under otherwise applicable  
16                  privacy laws that are unlikely to be directly  
17                  related to a cybersecurity threat.

18                  (iii) Such other matters as the Attor-  
19                  ney General and the Secretary of Home-  
20                  land Security consider appropriate for enti-  
21                  ties sharing cyber threat indicators with  
22                  Federal entities under this title.

23           (b) PRIVACY AND CIVIL LIBERTIES.—

24                   (1) GUIDELINES OF ATTORNEY GENERAL.—Not  
25           later than 60 days after the date of the enactment

1 of this Act, the Attorney General shall, in coordina-  
2 tion with heads of the appropriate Federal entities  
3 and in consultation with officers designated under  
4 section 1062 of the National Security Intelligence  
5 Reform Act of 2004 (42 U.S.C. 2000ee–1), develop,  
6 submit to Congress, and make available to the public  
7 interim guidelines relating to privacy and civil lib-  
8 erties which shall govern the receipt, retention, use,  
9 and dissemination of cyber threat indicators by a  
10 Federal entity obtained in connection with activities  
11 authorized in this title.

12 (2) FINAL GUIDELINES.—

13 (A) IN GENERAL.—Not later than 180  
14 days after the date of the enactment of this  
15 Act, the Attorney General shall, in coordination  
16 with heads of the appropriate Federal entities  
17 and in consultation with officers designated  
18 under section 1062 of the National Security In-  
19 telligence Reform Act of 2004 (42 U.S.C.  
20 2000ee–1) and such private entities with indus-  
21 try expertise as the Attorney General considers  
22 relevant, promulgate final guidelines relating to  
23 privacy and civil liberties which shall govern the  
24 receipt, retention, use, and dissemination of  
25 cyber threat indicators by a Federal entity ob-

1           tained in connection with activities authorized  
2           in this title.

3           (B) PERIODIC REVIEW.—The Attorney  
4           General shall, in coordination with heads of the  
5           appropriate Federal entities and in consultation  
6           with officers and private entities described in  
7           subparagraph (A), periodically, but not less fre-  
8           quently than once every two years, review the  
9           guidelines promulgated under subparagraph  
10          (A).

11          (3) CONTENT.—The guidelines required by  
12          paragraphs (1) and (2) shall, consistent with the  
13          need to protect information systems from cybersecu-  
14          rity threats and mitigate cybersecurity threats—

15                 (A) limit the effect on privacy and civil lib-  
16                 erties of activities by the Federal Government  
17                 under this title;

18                 (B) limit the receipt, retention, use, and  
19                 dissemination of cyber threat indicators con-  
20                 taining personal information or information  
21                 that identifies specific persons, including by es-  
22                 tablishing—

23                         (i) a process for the timely destruction  
24                         of such information that is known not to

1           be directly related to uses authorized under  
2           this title; and

3           (ii) specific limitations on the length  
4           of any period in which a cyber threat indi-  
5           cator may be retained;

6           (C) include requirements to safeguard  
7           cyber threat indicators containing personal in-  
8           formation or information that identifies specific  
9           persons from unauthorized access or acquisi-  
10          tion, including appropriate sanctions for activi-  
11          ties by officers, employees, or agents of the  
12          Federal Government in contravention of such  
13          guidelines;

14          (D) include procedures for notifying enti-  
15          ties and Federal entities if information received  
16          pursuant to this section is known or determined  
17          by a Federal entity receiving such information  
18          not to constitute a cyber threat indicator;

19          (E) protect the confidentiality of cyber  
20          threat indicators containing personal informa-  
21          tion or information that identifies specific per-  
22          sons to the greatest extent practicable and re-  
23          quire recipients to be informed that such indica-  
24          tors may only be used for purposes authorized  
25          under this title; and

1           (F) include steps that may be needed so  
2           that dissemination of cyber threat indicators is  
3           consistent with the protection of classified and  
4           other sensitive national security information.

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

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

13                (A) shall accept from any entity in real  
14                time cyber threat indicators and defensive  
15                measures, pursuant to this section;

16                (B) shall, upon submittal of the certifi-  
17                cation under paragraph (2) that such capability  
18                and process fully and effectively operates as de-  
19                scribed in such paragraph, be the process by  
20                which the Federal Government receives cyber  
21                threat indicators and defensive measures under  
22                this title that are shared by a private entity  
23                with the Federal Government through electronic  
24                mail or media, an interactive form on an Inter-

1 net website, or a real time, automated process  
2 between information systems except—

3 (i) consistent with section 104, com-  
4 munications between a Federal entity and  
5 a private entity regarding a previously  
6 shared cyber threat indicator to describe  
7 the relevant cybersecurity threat or develop  
8 a defensive measure based on such cyber  
9 threat indicator; and

10 (ii) communications by a regulated en-  
11 tity with such entity's Federal regulatory  
12 authority regarding a cybersecurity threat;

13 (C) ensures that all of the appropriate  
14 Federal entities receive in an automated man-  
15 ner such cyber threat indicators shared through  
16 the real-time process within the Department of  
17 Homeland Security;

18 (D) is in compliance with the policies, pro-  
19 cedures, and guidelines required by this section;  
20 and

21 (E) does not limit or prohibit otherwise  
22 lawful disclosures of communications, records,  
23 or other information, including—

1 (i) reporting of known or suspected  
2 criminal activity, by an entity to any other  
3 entity or a Federal entity;

4 (ii) voluntary or legally compelled par-  
5 ticipation in a Federal investigation; and

6 (iii) providing cyber threat indicators  
7 or defensive measures as part of a statu-  
8 tory or authorized contractual requirement.

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

16 (A) as the process by which the Federal  
17 Government receives from any entity a cyber  
18 threat indicator or defensive measure under this  
19 title; and

20 (B) in accordance with the policies, proce-  
21 dures, and guidelines developed under this sec-  
22 tion.

23 (3) PUBLIC NOTICE AND ACCESS.—The Sec-  
24 retary of Homeland Security shall ensure there is  
25 public notice of, and access to, the capability and

1 process developed and implemented under paragraph  
2 (1) so that—

3 (A) any entity may share cyber threat indi-  
4 cators and defensive measures through such  
5 process with the Federal Government; and

6 (B) all of the appropriate Federal entities  
7 receive such cyber threat indicators and defen-  
8 sive measures in real time with receipt through  
9 the process within the Department of Home-  
10 land Security.

11 (4) OTHER FEDERAL ENTITIES.—The process  
12 developed and implemented under paragraph (1)  
13 shall ensure that other Federal entities receive in a  
14 timely manner any cyber threat indicators and de-  
15 fensive measures shared with the Federal Govern-  
16 ment through such process.

17 (5) REPORT ON DEVELOPMENT AND IMPLE-  
18 MENTATION.—

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

1 of such capability and process and the public  
2 notice of, and access to, such process.

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

7 (d) INFORMATION SHARED WITH OR PROVIDED TO  
8 THE FEDERAL GOVERNMENT.—

9 (1) NO WAIVER OF PRIVILEGE OR PROTEC-  
10 TION.—The provision of cyber threat indicators and  
11 defensive measures to the Federal Government  
12 under this title shall not constitute a waiver of any  
13 applicable privilege or protection provided by law, in-  
14 cluding trade secret protection.

15 (2) PROPRIETARY INFORMATION.—Consistent  
16 with section 104(c)(2), a cyber threat indicator or  
17 defensive measure provided by an entity to the Fed-  
18 eral Government under this title shall be considered  
19 the commercial, financial, and proprietary informa-  
20 tion of such entity when so designated by the origi-  
21 nating entity or a third party acting in accordance  
22 with the written authorization of the originating en-  
23 tity.

1           (3) EXEMPTION FROM DISCLOSURE.—Cyber  
2 threat indicators and defensive measures provided to  
3 the Federal Government under this title shall be—

4           (A) deemed voluntarily shared information  
5 and exempt from disclosure under section 552  
6 of title 5, United States Code, and any State,  
7 tribal, or local law requiring disclosure of infor-  
8 mation or records; and

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

14           (4) EX PARTE COMMUNICATIONS.—The provi-  
15 sion of a cyber threat indicator or defensive measure  
16 to the Federal Government under this title shall not  
17 be subject to a rule of any Federal agency or depart-  
18 ment or any judicial doctrine regarding ex parte  
19 communications with a decision-making official.

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

21           (A) AUTHORIZED ACTIVITIES.—Cyber  
22 threat indicators and defensive measures pro-  
23 vided to the Federal Government under this  
24 title may be disclosed to, retained by, and used  
25 by, consistent with otherwise applicable provi-

1 sions of Federal law, any Federal agency or de-  
2 partment, component, officer, employee, or  
3 agent of the Federal Government solely for—

4 (i) a cybersecurity purpose;

5 (ii) the purpose of identifying a cyber-  
6 security threat, including the source of  
7 such cybersecurity threat, or a security  
8 vulnerability;

9 (iii) the purpose of identifying a cy-  
10 bersecurity threat involving the use of an  
11 information system by a foreign adversary  
12 or terrorist;

13 (iv) the purpose of responding to, or  
14 otherwise preventing or mitigating, an im-  
15minent threat of death, serious bodily  
16harm, or serious economic harm, including  
17a terrorist act or a use of a weapon of  
18mass destruction;

19 (v) the purpose of responding to, or  
20 otherwise preventing or mitigating, a seri-  
21ous threat to a minor, including sexual ex-  
22ploitation and threats to physical safety; or

23 (vi) the purpose of preventing, inves-  
24tigating, disrupting, or prosecuting an of-  
25fense arising out of a threat described in

1 clause (iv) or any of the offenses listed  
2 in—

3 (I) sections 1028 through 1030  
4 of title 18, United States Code (relat-  
5 ing to fraud and identity theft);

6 (II) chapter 37 of such title (re-  
7 lating to espionage and censorship);  
8 and

9 (III) chapter 90 of such title (re-  
10 lating to protection of trade secrets).

11 (B) PROHIBITED ACTIVITIES.—Cyber  
12 threat indicators and defensive measures pro-  
13 vided to the Federal Government under this  
14 title shall not be disclosed to, retained by, or  
15 used by any Federal agency or department for  
16 any use not permitted under subparagraph (A).

17 (C) PRIVACY AND CIVIL LIBERTIES.—  
18 Cyber threat indicators and defensive measures  
19 provided to the Federal Government under this  
20 title shall be retained, used, and disseminated  
21 by the Federal Government—

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

1 (ii) in a manner that protects from  
2 unauthorized use or disclosure any cyber  
3 threat indicators that may contain personal  
4 information or information that identifies  
5 specific persons; and

6 (iii) in a manner that protects the  
7 confidentiality of cyber threat indicators  
8 containing personal information or infor-  
9 mation that identifies a specific person.

10 (D) FEDERAL REGULATORY AUTHORITY.—

11 (i) IN GENERAL.—Except as provided  
12 in clause (ii), cyber threat indicators and  
13 defensive measures provided to the Federal  
14 Government under this title shall not be  
15 directly used by any Federal, State, tribal,  
16 or local government to regulate, including  
17 an enforcement action, the lawful activities  
18 of any entity, including activities relating  
19 to monitoring, operating defensive meas-  
20 ures, or sharing cyber threat indicators.

21 (ii) EXCEPTIONS.—

22 (I) REGULATORY AUTHORITY  
23 SPECIFICALLY RELATING TO PREVEN-  
24 TION OR MITIGATION OF CYBERSECU-  
25 RITY THREATS.—Cyber threat indica-

1           tors and defensive measures provided  
2           to the Federal Government under this  
3           title may, consistent with Federal or  
4           State regulatory authority specifically  
5           relating to the prevention or mitiga-  
6           tion of cybersecurity threats to infor-  
7           mation systems, inform the develop-  
8           ment or implementation of regulations  
9           relating to such information systems.

10                           (II) PROCEDURES DEVELOPED  
11                           AND IMPLEMENTED UNDER THIS  
12                           TITLE.—Clause (i) shall not apply to  
13                           procedures developed and imple-  
14                           mented under this title.

15 **SEC. 106. PROTECTION FROM LIABILITY.**

16           (a) MONITORING OF INFORMATION SYSTEMS.—No  
17           cause of action shall lie or be maintained in any court  
18           against any private entity, and such action shall be  
19           promptly dismissed, for the monitoring of information sys-  
20           tems and information under section 104(a) that is con-  
21           ducted in accordance with this title.

22           (b) SHARING OR RECEIPT OF CYBER THREAT INDI-  
23           CATORS.—No cause of action shall lie or be maintained  
24           in any court against any entity, and such action shall be  
25           promptly dismissed, for the sharing or receipt of cyber

1 threat indicators or defensive measures under section  
2 104(c) if—

3           (1) such sharing or receipt is conducted in ac-  
4 cordance with this title; and

5           (2) in a case in which a cyber threat indicator  
6 or defensive measure is shared with the Federal  
7 Government, the cyber threat indicator or defensive  
8 measure is shared in a manner that is consistent  
9 with section 105(c)(1)(B) and the sharing or receipt,  
10 as the case may be, occurs after the earlier of—

11                   (A) the date on which the interim policies  
12 and procedures are submitted to Congress  
13 under section 105(a)(1) and guidelines are sub-  
14 mitted to Congress under section 105(b)(1); or

15                   (B) the date that is 60 days after the date  
16 of the enactment of this Act.

17       (c) CONSTRUCTION.—Nothing in this section shall be  
18 construed—

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

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

1 **SEC. 107. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

2 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

3 (1) IN GENERAL.—Not later than 1 year after  
4 the date of the enactment of this Act, and not less  
5 frequently than once every 2 years thereafter, the  
6 heads of the appropriate Federal entities shall joint-  
7 ly submit and the Inspector General of the Depart-  
8 ment of Homeland Security, the Inspector General  
9 of the Intelligence Community, the Inspector Gen-  
10 eral of the Department of Justice, the Inspector  
11 General of the Department of Defense, and the In-  
12 spector General of the Department of Energy, in  
13 consultation with the Council of Inspectors General  
14 on Financial Oversight, shall jointly submit to Con-  
15 gress a detailed report concerning the implementa-  
16 tion of this title during—

17 (A) in the case of the first report sub-  
18 mitted under this paragraph, the most recent 1-  
19 year period; and

20 (B) in the case of any subsequent report  
21 submitted under this paragraph, the most re-  
22 cent 2-year period.

23 (2) CONTENTS.—Each report submitted under  
24 paragraph (1) shall include, for the period covered  
25 by the report, the following:

1           (A) An assessment of the sufficiency of the  
2 policies, procedures, and guidelines required by  
3 section 105 in ensuring that cyber threat indi-  
4 cators are shared effectively and responsibly  
5 within the Federal Government.

6           (B) An evaluation of the effectiveness of  
7 real-time information sharing through the capa-  
8 bility and process developed under section  
9 105(c), including any impediments to such real-  
10 time sharing.

11           (C) An assessment of the sufficiency of the  
12 procedures developed under section 103 in en-  
13 suring that cyber threat indicators in the pos-  
14 session of the Federal Government are shared  
15 in a timely and adequate manner with appro-  
16 priate entities, or, if appropriate, are made pub-  
17 licly available.

18           (D) An assessment of whether cyber threat  
19 indicators have been properly classified and an  
20 accounting of the number of security clearances  
21 authorized by the Federal Government for the  
22 purposes of this title.

23           (E) A review of the type of cyber threat in-  
24 dicators shared with the appropriate Federal  
25 entities under this title, including the following:

1 (i) The number of cyber threat indica-  
2 tors received through the capability and  
3 process developed under section 105(c).

4 (ii) The number of times that infor-  
5 mation shared under this title was used by  
6 a Federal entity to prosecute an offense  
7 consistent with section 105(d)(5)(A).

8 (iii) The degree to which such infor-  
9 mation may affect the privacy and civil lib-  
10 erties of specific persons.

11 (iv) A quantitative and qualitative as-  
12 sessment of the effect of the sharing of  
13 such cyber threat indicators with the Fed-  
14 eral Government on privacy and civil lib-  
15 erties of specific persons, including the  
16 number of notices that were issued with re-  
17 spect to a failure to remove personal infor-  
18 mation or information that identified a  
19 specific person not directly related to a cy-  
20 bersecurity threat in accordance with the  
21 procedures required by section  
22 105(b)(3)(D).

23 (v) The adequacy of any steps taken  
24 by the Federal Government to reduce such  
25 effect.

1 (F) A review of actions taken by the Fed-  
2 eral Government based on cyber threat indica-  
3 tors shared with the Federal Government under  
4 this title, including the appropriateness of any  
5 subsequent use or dissemination of such cyber  
6 threat indicators by a Federal entity under sec-  
7 tion 105.

8 (G) A description of any significant viola-  
9 tions of the requirements of this title by the  
10 Federal Government.

11 (H) A summary of the number and type of  
12 entities that received classified cyber threat in-  
13 dicators from the Federal Government under  
14 this title and an evaluation of the risks and  
15 benefits of sharing such cyber threat indicators.

16 (3) RECOMMENDATIONS.—Each report sub-  
17 mitted under paragraph (1) may include rec-  
18 ommendations for improvements or modifications to  
19 the authorities and processes under this title.

20 (4) FORM OF REPORT.—Each report required  
21 by paragraph (1) shall be submitted in unclassified  
22 form, but may include a classified annex.

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

24 (1) BIENNIAL REPORT FROM PRIVACY AND  
25 CIVIL LIBERTIES OVERSIGHT BOARD.—Not later

1 than 2 years after the date of the enactment of this  
2 Act and not less frequently than once every 2 years  
3 thereafter, the Privacy and Civil Liberties Oversight  
4 Board shall submit to Congress and the President a  
5 report providing—

6 (A) an assessment of the effect on privacy  
7 and civil liberties by the type of activities car-  
8 ried out under this title; and

9 (B) an assessment of the sufficiency of the  
10 policies, procedures, and guidelines established  
11 pursuant to section 105 in addressing concerns  
12 relating to privacy and civil liberties.

13 (2) BIENNIAL REPORT OF INSPECTORS GEN-  
14 ERAL.—

15 (A) IN GENERAL.—Not later than 2 years  
16 after the date of the enactment of this Act and  
17 not less frequently than once every 2 years  
18 thereafter, the Inspector General of the Depart-  
19 ment of Homeland Security, the Inspector Gen-  
20 eral of the Intelligence Community, the Inspec-  
21 tor General of the Department of Justice, the  
22 Inspector General of the Department of De-  
23 fense, and the Inspector General of the Depart-  
24 ment of Energy shall, in consultation with the  
25 Council of Inspectors General on Financial

1 Oversight, jointly submit to Congress a report  
2 on the receipt, use, and dissemination of cyber  
3 threat indicators and defensive measures that  
4 have been shared with Federal entities under  
5 this title.

6 (B) CONTENTS.—Each report submitted  
7 under subparagraph (A) shall include the fol-  
8 lowing:

9 (i) A review of the types of cyber  
10 threat indicators shared with Federal enti-  
11 ties.

12 (ii) A review of the actions taken by  
13 Federal entities as a result of the receipt  
14 of such cyber threat indicators.

15 (iii) A list of Federal entities receiving  
16 such cyber threat indicators.

17 (iv) A review of the sharing of such  
18 cyber threat indicators among Federal en-  
19 tities to identify inappropriate barriers to  
20 sharing information.

21 (3) RECOMMENDATIONS.—Each report sub-  
22 mitted under this subsection may include such rec-  
23 ommendations as the Privacy and Civil Liberties  
24 Oversight Board, with respect to a report submitted  
25 under paragraph (1), or the Inspectors General re-

1       ferred to in paragraph (2)(A), with respect to a re-  
2       port submitted under paragraph (2), may have for  
3       improvements or modifications to the authorities  
4       under this title.

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

8       **SEC. 108. CONSTRUCTION AND PREEMPTION.**

9       (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in  
10      this title shall be construed—

11           (1) to limit or prohibit otherwise lawful disclo-  
12      sures of communications, records, or other informa-  
13      tion, including reporting of known or suspected  
14      criminal activity, by an entity to any other entity or  
15      the Federal Government under this title; or

16           (2) to limit or prohibit otherwise lawful use of  
17      such disclosures by any Federal entity, even when  
18      such otherwise lawful disclosures duplicate or rep-  
19      licate disclosures made under this title.

20      (b) WHISTLE BLOWER PROTECTIONS.—Nothing in  
21      this title shall be construed to prohibit or limit the disclo-  
22      sure of information protected under section 2302(b)(8) of  
23      title 5, United States Code (governing disclosures of ille-  
24      gality, waste, fraud, abuse, or public health or safety  
25      threats), section 7211 of title 5, United States Code (gov-

1 erning disclosures to Congress), section 1034 of title 10,  
2 United States Code (governing disclosure to Congress by  
3 members of the military), section 1104 of the National  
4 Security Act of 1947 (50 U.S.C. 3234) (governing disclo-  
5 sure by employees of elements of the intelligence commu-  
6 nity), or any similar provision of Federal or State law.

7 (c) PROTECTION OF SOURCES AND METHODS.—

8 Nothing in this title shall be construed—

9 (1) as creating any immunity against, or other-  
10 wise affecting, any action brought by the Federal  
11 Government, or any agency or department thereof,  
12 to enforce any law, executive order, or procedure  
13 governing the appropriate handling, disclosure, or  
14 use of classified information;

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

17 (3) to modify the authority of a department or  
18 agency of the Federal Government to protect classi-  
19 fied information and sources and methods and the  
20 national security of the United States.

21 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in  
22 this title shall be construed to affect any requirement  
23 under any other provision of law for an entity to provide  
24 information to the Federal Government.

1 (e) PROHIBITED CONDUCT.—Nothing in this title  
2 shall be construed to permit price-fixing, allocating a mar-  
3 ket between competitors, monopolizing or attempting to  
4 monopolize a market, boycotting, or exchanges of price or  
5 cost information, customer lists, or information regarding  
6 future competitive planning.

7 (f) INFORMATION SHARING RELATIONSHIPS.—Noth-  
8 ing in this title shall be construed—

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

11 (2) to prohibit a new information sharing rela-  
12 tionship;

13 (3) to require a new information sharing rela-  
14 tionship between any entity and another entity or a  
15 Federal entity; or

16 (4) to require the use of the capability and  
17 process within the Department of Homeland Secu-  
18 rity developed under section 105(c).

19 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS  
20 AND RIGHTS.—Nothing in this title shall be construed—

21 (1) to amend, repeal, or supersede any current  
22 or future contractual agreement, terms of service  
23 agreement, or other contractual relationship between  
24 any entities, or between any entity and a Federal en-  
25 tity; or

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

3           (h) ANTI-TASKING RESTRICTION.—Nothing in this  
4 title shall be construed to permit a Federal entity—

5           (1) to require an entity to provide information  
6           to a Federal entity or another entity;

7           (2) to condition the sharing of cyber threat in-  
8           dicators with an entity on such entity’s provision of  
9           cyber threat indicators to a Federal entity or an-  
10          other entity; or

11          (3) to condition the award of any Federal  
12          grant, contract, or purchase on the provision of a  
13          cyber threat indicator to a Federal entity or another  
14          entity.

15          (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-  
16          ing in this title shall be construed to subject any entity  
17          to liability for choosing not to engage in the voluntary ac-  
18          tivities authorized in this title.

19          (j) USE AND RETENTION OF INFORMATION.—Noth-  
20          ing in this title shall be construed to authorize, or to mod-  
21          ify any existing authority of, a department or agency of  
22          the Federal Government to retain or use any information  
23          shared under this title for any use other than permitted  
24          in this title.

25          (k) FEDERAL PREEMPTION.—

1           (1) IN GENERAL.—This title supersedes any  
2 statute or other provision of law of a State or polit-  
3 ical subdivision of a State that restricts or otherwise  
4 expressly regulates an activity authorized under this  
5 title.

6           (2) STATE LAW ENFORCEMENT.—Nothing in  
7 this title shall be construed to supersede any statute  
8 or other provision of law of a State or political sub-  
9 division of a State concerning the use of authorized  
10 law enforcement practices and procedures.

11          (l) REGULATORY AUTHORITY.—Nothing in this title  
12 shall be construed—

13           (1) to authorize the promulgation of any regu-  
14 lations not specifically authorized by this title;

15           (2) to establish or limit any regulatory author-  
16 ity not specifically established or limited under this  
17 title; or

18           (3) to authorize regulatory actions that would  
19 duplicate or conflict with regulatory requirements,  
20 mandatory standards, or related processes under an-  
21 other provision of Federal law.

22          (m) AUTHORITY OF SECRETARY OF DEFENSE TO  
23 RESPOND TO CYBER ATTACKS.—Nothing in this title  
24 shall be construed to limit the authority of the Secretary  
25 of Defense to develop, prepare, coordinate, or, when au-

1 thORIZED by the President to do so, conduct a military  
2 cyber operation in response to a malicious cyber activity  
3 carried out against the United States or a United States  
4 person by a foreign government or an organization spon-  
5 sored by a foreign government or a terrorist organization.

6 **SEC. 109. REPORT ON CYBERSECURITY THREATS.**

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

16 (b) **CONTENTS.**—The report required by subsection  
17 (a) shall include the following:

18 (1) An assessment of the current intelligence  
19 sharing and cooperation relationships of the United  
20 States with other countries regarding cybersecurity  
21 threats, including cyber attacks, theft, and data  
22 breaches, directed against the United States and  
23 which threaten the United States national security  
24 interests and economy and intellectual property, spe-  
25 cifically identifying the relative utility of such rela-

1        tionships, which elements of the intelligence commu-  
2        nity participate in such relationships, and whether  
3        and how such relationships could be improved.

4            (2) A list and an assessment of the countries  
5        and nonstate actors that are the primary threats of  
6        carrying out a cybersecurity threat, including a  
7        cyber attack, theft, or data breach, against the  
8        United States and which threaten the United States  
9        national security, economy, and intellectual property.

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

18           (4) An assessment of additional technologies or  
19        capabilities that would enhance the ability of the  
20        United States to prevent and to respond to cyberse-  
21        curity threats, including cyber attacks, theft, and  
22        data breaches.

23           (5) An assessment of any technologies or prac-  
24        tices utilized by the private sector that could be rap-

1 idly fielded to assist the intelligence community in  
2 preventing and responding to cybersecurity threats.

3 (c) ADDITIONAL REPORT.—At the time the report re-  
4 quired by subsection (a) is submitted, the Director of Na-  
5 tional Intelligence shall submit to the Committee on For-  
6 eign Relations of the Senate and the Committee on For-  
7 eign Affairs of the House of Representatives a report con-  
8 taining the information required by subsection (b)(2).

9 (d) FORM OF REPORT.—The report required by sub-  
10 section (a) shall be made available in classified and unclas-  
11 sified forms.

12 (e) INTELLIGENCE COMMUNITY DEFINED.—In this  
13 section, the term “intelligence community” has the mean-  
14 ing given that term in section 3 of the National Security  
15 Act of 1947 (50 U.S.C. 3003).

16 **SEC. 110. CONFORMING AMENDMENT.**

17 Section 941(c)(3) of the National Defense Authoriza-  
18 tion Act for Fiscal Year 2013 (Public Law 112–239; 10  
19 U.S.C. 2224 note) is amended by inserting at the end the  
20 following: “The Secretary may share such information  
21 with other Federal entities if such information consists of  
22 cyber threat indicators and defensive measures and such  
23 information is shared consistent with the policies and pro-  
24 cedures promulgated by the Attorney General and the Sec-

1 retary of Homeland Security under section 105 of the Cy-  
2 bersecurity Information Sharing Act of 2015.”.

3 **TITLE II—FEDERAL CYBERSECU-**  
4 **RITY ENHANCEMENT**

5 **SEC. 201. SHORT TITLE.**

6 This title may be cited as the “Federal Cybersecurity  
7 Enhancement Act of 2015”.

8 **SEC. 202. DEFINITIONS.**

9 In this title—

10 (1) the term “agency” has the meaning given  
11 the term in section 3502 of title 44, United States  
12 Code;

13 (2) the term “agency information system” has  
14 the meaning given the term in section 228 of the  
15 Homeland Security Act of 2002, as added by section  
16 203(a);

17 (3) the term “appropriate congressional com-  
18 mittees” means—

19 (A) the Committee on Homeland Security  
20 and Governmental Affairs of the Senate; and

21 (B) the Committee on Homeland Security  
22 of the House of Representatives;

23 (4) the terms “cybersecurity risk” and “infor-  
24 mation system” have the meanings given those