

AMENDMENT NO. _____ Calendar No. _____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—114th Cong., 1st Sess.

S. 754

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

Referred to the Committee on _____ and
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended
to be proposed by _____

Viz:

1 Strike all after the enacting clause and insert the fol-
2 lowing:

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 cy-
bersecurity threats.

Sec. 5. Sharing of cyber threat indicators and defensive measures with the Fed-
eral 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 amendment.

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.

23 (D) The Department of Homeland Secu-
24 rity.

1 (E) The Department of Justice.

2 (F) The Department of the Treasury.

3 (G) The Office of the Director of National
4 Intelligence.

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

11 (5) CYBERSECURITY THREAT.—

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

23 (B) EXCLUSION.—The term “cybersecurity
24 threat” does not include any action that solely

1 involves a violation of a consumer term of serv-
2 ice or a consumer licensing agreement.

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

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

11 (B) a method of defeating a security con-
12 trol or exploitation of a security vulnerability;

13 (C) a security vulnerability, including
14 anomalous activity that appears to indicate the
15 existence of a security vulnerability;

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

22 (E) malicious cyber command and control;

23 (F) the actual or potential harm caused by
24 an incident, including a description of the infor-

1 mation exfiltrated as a result of a particular cy-
2 bersecurity threat;

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

6 (H) any combination thereof.

7 (7) DEFENSIVE MEASURE.—

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

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

23 (i) the private entity operating the
24 measure; or

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

5 (8) ENTITY.—

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

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

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

23 (9) FEDERAL ENTITY.—The term “Federal en-
24 tity” means a department or agency of the United

1 States or any component of such department or
2 agency.

3 (10) INFORMATION SYSTEM.—The term “infor-
4 mation system”—

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

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

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

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

21 (13) MALICIOUS RECONNAISSANCE.—The term
22 “malicious reconnaissance” means a method for ac-
23 tively probing or passively monitoring an information
24 system for the purpose of discerning security
25 vulnerabilities of the information system, if such

1 method is associated with a known or suspected cy-
2 bersecurity threat.

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

7 (15) PRIVATE ENTITY.—

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

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

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

22 (16) SECURITY CONTROL.—The term “security
23 control” means the management, operational, and
24 technical controls used to protect against an unau-
25 thorized effort to adversely affect the confidentiality,

1 integrity, and availability of an information system
2 or its information.

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

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

11 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**
12 **ERNMENT.**

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

21 (1) the timely sharing of classified cyber threat
22 indicators in the possession of the Federal Govern-
23 ment with cleared representatives of relevant enti-
24 ties;

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

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

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

14 (b) DEVELOPMENT OF PROCEDURES.—

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

17 (A) ensure the Federal Government has
18 and maintains the capability to share cyber
19 threat indicators in real time consistent with
20 the protection of classified information;

21 (B) incorporate, to the greatest extent
22 practicable, existing processes and existing roles
23 and responsibilities of Federal and non-Federal
24 entities for information sharing by the Federal

1 Government, including sector specific informa-
2 tion sharing and analysis centers;

3 (C) include procedures for notifying enti-
4 ties that have received a cyber threat indicator
5 from a Federal entity under this Act that is
6 known or determined to be in error or in con-
7 travention of the requirements of this Act or
8 another provision of Federal law or policy of
9 such error or contravention;

10 (D) include requirements for Federal enti-
11 ties sharing cyber threat indicators or defensive
12 measures to implement and utilize security con-
13 trols to protect against unauthorized access to
14 or acquisition of such cyber threat indicators or
15 defensive measures; and

16 (E) include procedures that require a Fed-
17 eral entity, prior to the sharing of a cyber
18 threat indicator—

19 (i) to review such cyber threat indi-
20 cator to assess whether such cyber threat
21 indicator contains any information that
22 such Federal entity knows at the time of
23 sharing to be personal information or in-
24 formation that identifies a specific person

1 not directly related to a cybersecurity
2 threat and remove such information; or

3 (ii) to implement and utilize a tech-
4 nical capability configured to remove any
5 personal information or information that
6 identifies a specific person not directly re-
7 lated to a cybersecurity threat.

8 (2) COORDINATION.—In developing the proce-
9 dures required under this section, the Director of
10 National Intelligence, the Secretary of Homeland Se-
11 curity, the Secretary of Defense, and the Attorney
12 General shall coordinate with appropriate Federal
13 entities, including the National Laboratories (as de-
14 fined in section 2 of the Energy Policy Act of 2005
15 (42 U.S.C. 15801)), to ensure that effective proto-
16 cols are implemented that will facilitate and promote
17 the sharing of cyber threat indicators by the Federal
18 Government in a timely manner.

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

1 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
2 **ANALYZING, AND MITIGATING CYBERSECU-**
3 **RITY THREATS.**

4 (a) AUTHORIZATION FOR MONITORING.—

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

8 (A) an information system of such private
9 entity;

10 (B) an information system of another enti-
11 ty, upon the authorization and written consent
12 of such other entity;

13 (C) an information system of a Federal en-
14 tity, upon the authorization and written consent
15 of an authorized representative of the Federal
16 entity; and

17 (D) information that is stored on, proc-
18 essed by, or transiting an information system
19 monitored by the private entity under this para-
20 graph.

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

23 (A) to authorize the monitoring of an in-
24 formation system, or the use of any information
25 obtained through such monitoring, other than
26 as provided in this Act; or

1 (B) to limit otherwise lawful activity.

2 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE
3 MEASURES.—

4 (1) IN GENERAL.—Notwithstanding any other
5 provision of law, a private entity may, for cybersecu-
6 rity purposes, operate a defensive measure that is
7 applied to—

8 (A) an information system of such private
9 entity in order to protect the rights or property
10 of the private entity;

11 (B) an information system of another enti-
12 ty upon written consent of such entity for oper-
13 ation of such defensive measure to protect the
14 rights or property of such entity; and

15 (C) an information system of a Federal en-
16 tity upon written consent of an authorized rep-
17 resentative of such Federal entity for operation
18 of such defensive measure to protect the rights
19 or property of the Federal Government.

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

22 (A) to authorize the use of a defensive
23 measure other than as provided in this sub-
24 section; or

25 (B) to limit otherwise lawful activity.

1 (c) AUTHORIZATION FOR SHARING OR RECEIVING
2 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-
3 URES.—

4 (1) IN GENERAL.—Except as provided in para-
5 graph (2) and notwithstanding any other provision
6 of law, an entity may, for a cybersecurity purpose
7 and consistent with the protection of classified infor-
8 mation, share with, or receive from, any other entity
9 or the Federal Government a cyber threat indicator
10 or defensive measure.

11 (2) LAWFUL RESTRICTION.—An entity receiving
12 a cyber threat indicator or defensive measure from
13 another entity or Federal entity shall comply with
14 otherwise lawful restrictions placed on the sharing or
15 use of such cyber threat indicator or defensive meas-
16 ure by the sharing entity or Federal entity.

17 (3) CONSTRUCTION.—Nothing in this sub-
18 section shall be construed—

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

22 (B) to limit otherwise lawful activity.

23 (d) PROTECTION AND USE OF INFORMATION.—

24 (1) SECURITY OF INFORMATION.—An entity
25 monitoring an information system, operating a de-

1 fensive measure, or providing or receiving a cyber
2 threat indicator or defensive measure under this sec-
3 tion shall implement and utilize a security control to
4 protect against unauthorized access to or acquisition
5 of such cyber threat indicator or defensive measure.

6 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
7 TION.—An entity sharing a cyber threat indicator
8 pursuant to this Act shall, prior to such sharing—

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

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

23 (3) USE OF CYBER THREAT INDICATORS AND
24 DEFENSIVE MEASURES BY ENTITIES.—

1 (A) IN GENERAL.—Consistent with this
2 Act, a cyber threat indicator or defensive meas-
3 ure shared or received under this section may,
4 for cybersecurity purposes—

5 (i) be used by an entity to monitor or
6 operate a defensive measure that is applied
7 to—

8 (I) an information system of the
9 entity; or

10 (II) an information system of an-
11 other entity or a Federal entity upon
12 the written consent of that other enti-
13 ty or that Federal entity; and

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

16 (I) an otherwise lawful restriction
17 placed by the sharing entity or Fed-
18 eral entity on such cyber threat indi-
19 cator or defensive measure; or

20 (II) an otherwise applicable pro-
21 vision of law.

22 (B) CONSTRUCTION.—Nothing in this
23 paragraph shall be construed to authorize the
24 use of a cyber threat indicator or defensive
25 measure other than as provided in this section.

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

3 (A) LAW ENFORCEMENT USE.—

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

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

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

23 (i) deemed voluntarily shared informa-
24 tion; and

1 (ii) exempt from disclosure under any
2 State, tribal, or local law requiring disclo-
3 sure of information or records.

4 (C) STATE, TRIBAL, AND LOCAL REGU-
5 LATORY AUTHORITY.—

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

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

1 to information systems, inform the devel-
2 opment or implementation of a regulation
3 relating to such information systems.

4 (e) ANTITRUST EXEMPTION.—

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

12 (2) APPLICABILITY.—Paragraph (1) shall apply
13 only to information that is exchanged or assistance
14 provided in order to assist with—

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

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

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

5 **SEC. 5. SHARING OF CYBER THREAT INDICATORS AND DE-**
6 **FENSIVE MEASURES WITH THE FEDERAL**
7 **GOVERNMENT.**

8 (a) REQUIREMENT FOR POLICIES AND PROCE-
9 DURES.—

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

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

1 receipt of cyber threat indicators and defensive meas-
2 ures by the Federal Government.

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

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

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

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

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

22 (B) ensure that cyber threat indicators
23 shared with the Federal Government by any en-
24 tity pursuant to section 4 in a manner other

1 than the real time process described in sub-
2 section (c) of this section—

3 (i) are shared as quickly as operation-
4 ally practicable with all of the appropriate
5 Federal entities;

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

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

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

24 (D) ensure there is—

25 (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 (4) GUIDELINES FOR ENTITIES SHARING CYBER
7 THREAT INDICATORS WITH FEDERAL GOVERN-
8 MENT.—

9 (A) IN GENERAL.—Not later than 60 days
10 after the date of the enactment of this Act, the
11 Attorney General and the Secretary of Home-
12 land Security shall develop and make publicly
13 available guidance to assist entities and pro-
14 mote sharing of cyber threat indicators with
15 Federal entities under this Act.

16 (B) CONTENTS.—The guidelines developed
17 and made publicly available under subpara-
18 graph (A) shall include guidance on the fol-
19 lowing:

20 (i) Identification of types of informa-
21 tion that would qualify as a cyber threat
22 indicator under this Act that would be un-
23 likely to include personal information or in-
24 formation that identifies a specific person

1 not directly related to a cyber security
2 threat.

3 (ii) Identification of types of informa-
4 tion protected under otherwise applicable
5 privacy laws that are unlikely to be directly
6 related to a cybersecurity threat.

7 (iii) Such other matters as the Attor-
8 ney General and the Secretary of Home-
9 land Security consider appropriate for enti-
10 ties sharing cyber threat indicators with
11 Federal entities under this Act.

12 (b) PRIVACY AND CIVIL LIBERTIES.—

13 (1) GUIDELINES OF ATTORNEY GENERAL.—Not
14 later than 60 days after the date of the enactment
15 of this Act, the Attorney General shall, in coordina-
16 tion with heads of the appropriate Federal entities
17 and in consultation with officers designated under
18 section 1062 of the National Security Intelligence
19 Reform Act of 2004 (42 U.S.C. 2000ee–1), develop,
20 submit to Congress, and make available to the public
21 interim guidelines relating to privacy and civil lib-
22 erties which shall govern the receipt, retention, use,
23 and dissemination of cyber threat indicators by a
24 Federal entity obtained in connection with activities
25 authorized in this Act.

1 (2) FINAL GUIDELINES.—

2 (A) IN GENERAL.—Not later than 180
3 days after the date of the enactment of this
4 Act, the Attorney General shall, in coordination
5 with heads of the appropriate Federal entities
6 and in consultation with officers designated
7 under section 1062 of the National Security In-
8 telligence Reform Act of 2004 (42 U.S.C.
9 2000ee–1) and such private entities with indus-
10 try expertise as the Attorney General considers
11 relevant, promulgate final guidelines relating to
12 privacy and civil liberties which shall govern the
13 receipt, retention, use, and dissemination of
14 cyber threat indicators by a Federal entity ob-
15 tained in connection with activities authorized
16 in this Act.

17 (B) PERIODIC REVIEW.—The Attorney
18 General shall, in coordination with heads of the
19 appropriate Federal entities and in consultation
20 with officers and private entities described in
21 subparagraph (A), periodically, but not less fre-
22 quently than once every two years, review the
23 guidelines promulgated under subparagraph
24 (A).

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

5 (A) limit the impact on privacy and civil
6 liberties of activities by the Federal Government
7 under this Act;

8 (B) limit the receipt, retention, use, and
9 dissemination of cyber threat indicators con-
10 taining personal information or information
11 that identifies specific persons, including by es-
12 tablishing—

13 (i) a process for the timely destruction
14 of such information that is known not to
15 be directly related to uses authorized under
16 this Act; and

17 (ii) specific limitations on the length
18 of any period in which a cyber threat indi-
19 cator may be retained;

20 (C) include requirements to safeguard
21 cyber threat indicators containing personal in-
22 formation or information that identifies specific
23 persons from unauthorized access or acquisi-
24 tion, including appropriate sanctions for activi-
25 ties by officers, employees, or agents of the

1 Federal Government in contravention of such
2 guidelines;

3 (D) include procedures for notifying enti-
4 ties and Federal entities if information received
5 pursuant to this section is known or determined
6 by a Federal entity receiving such information
7 not to constitute a cyber threat indicator;

8 (E) protect the confidentiality of cyber
9 threat indicators containing personal informa-
10 tion or information that identifies specific per-
11 sons to the greatest extent practicable and re-
12 quire recipients to be informed that such indica-
13 tors may only be used for purposes authorized
14 under this Act; and

15 (F) include steps that may be needed so
16 that dissemination of cyber threat indicators is
17 consistent with the protection of classified and
18 other sensitive national security information.

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

21 (1) IN GENERAL.—Not later than 90 days after
22 the date of the enactment of this Act, the Secretary
23 of Homeland Security, in coordination with the
24 heads of the appropriate Federal entities, shall de-

1 velop and implement a capability and process within
2 the Department of Homeland Security that—

3 (A) shall accept from any entity in real
4 time cyber threat indicators and defensive
5 measures, pursuant to this section;

6 (B) shall, upon submittal of the certifi-
7 cation under paragraph (2) that such capability
8 and process fully and effectively operates as de-
9 scribed in such paragraph, be the process by
10 which the Federal Government receives cyber
11 threat indicators and defensive measures under
12 this Act that are shared by a private entity with
13 the Federal Government through electronic mail
14 or media, an interactive form on an Internet
15 website, or a real time, automated process be-
16 tween information systems except—

17 (i) consistent with section 4, commu-
18 nications between a Federal entity and a
19 private entity regarding a previously
20 shared cyber threat indicator to describe
21 the relevant cybersecurity threat or develop
22 a defensive measure based on such cyber
23 threat indicator; and

1 (ii) communications by a regulated en-
2 tity with such entity's Federal regulatory
3 authority regarding a cybersecurity threat;

4 (C) ensures that all of the appropriate
5 Federal entities receive in an automated man-
6 ner such cyber threat indicators shared through
7 the real-time process within the Department of
8 Homeland Security;

9 (D) is in compliance with the policies, pro-
10 cedures, and guidelines required by this section;
11 and

12 (E) does not limit or prohibit otherwise
13 lawful disclosures of communications, records,
14 or other information, including—

15 (i) reporting of known or suspected
16 criminal activity, by an entity to any other
17 entity or a Federal entity;

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

20 (iii) providing cyber threat indicators
21 or defensive measures as part of a statu-
22 tory or authorized contractual requirement.

23 (2) CERTIFICATION.—Not later than 10 days
24 prior to the implementation of the capability and
25 process required by paragraph (1), the Secretary of

1 Homeland Security shall, in consultation with the
2 heads of the appropriate Federal entities, certify to
3 Congress whether such capability and process fully
4 and effectively operates—

5 (A) as the process by which the Federal
6 Government receives from any entity a cyber
7 threat indicator or defensive measure under this
8 Act; and

9 (B) in accordance with the policies, proce-
10 dures, and guidelines developed under this sec-
11 tion.

12 (3) PUBLIC NOTICE AND ACCESS.—The Sec-
13 retary of Homeland Security shall ensure there is
14 public notice of, and access to, the capability and
15 process developed and implemented under paragraph
16 (1) so that—

17 (A) any entity may share cyber threat indi-
18 cators and defensive measures through such
19 process with the Federal Government; and

20 (B) all of the appropriate Federal entities
21 receive such cyber threat indicators and defen-
22 sive measures in real time with receipt through
23 the process within the Department of Home-
24 land Security.

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

7 (5) REPORT ON DEVELOPMENT AND IMPLE-
8 MENTATION.—

9 (A) IN GENERAL.—Not later than 60 days
10 after the date of the enactment of this Act, the
11 Secretary of Homeland Security shall submit to
12 Congress a report on the development and im-
13 plementation of the capability and process re-
14 quired by paragraph (1), including a description
15 of such capability and process and the public
16 notice of, and access to, such process.

17 (B) CLASSIFIED ANNEX.—The report re-
18 quired by subparagraph (A) shall be submitted
19 in unclassified form, but may include a classi-
20 fied annex.

21 (d) INFORMATION SHARED WITH OR PROVIDED TO
22 THE FEDERAL GOVERNMENT.—

23 (1) NO WAIVER OF PRIVILEGE OR PROTEC-
24 TION.—The provision of cyber threat indicators and
25 defensive measures to the Federal Government

1 under this Act shall not constitute a waiver of any
2 applicable privilege or protection provided by law, in-
3 cluding trade secret protection.

4 (2) PROPRIETARY INFORMATION.—Consistent
5 with section 4(e)(2), a cyber threat indicator or de-
6 fensive measure provided by an entity to the Federal
7 Government under this Act shall be considered the
8 commercial, financial, and proprietary information of
9 such entity when so designated by the originating
10 entity or a third party acting in accordance with the
11 written authorization of the originating entity.

12 (3) EXEMPTION FROM DISCLOSURE.—Cyber
13 threat indicators and defensive measures provided to
14 the Federal Government under this Act shall be—

15 (A) deemed voluntarily shared information
16 and exempt from disclosure under section 552
17 of title 5, United States Code, and any State,
18 tribal, or local law requiring disclosure of infor-
19 mation or records; and

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

1 (4) EX PARTE COMMUNICATIONS.—The provi-
2 sion of a cyber threat indicator or defensive measure
3 to the Federal Government under this Act shall not
4 be subject to a rule of any Federal agency or depart-
5 ment or any judicial doctrine regarding ex parte
6 communications with a decision-making official.

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

8 (A) AUTHORIZED ACTIVITIES.—Cyber
9 threat indicators and defensive measures pro-
10 vided to the Federal Government under this Act
11 may be disclosed to, retained by, and used by,
12 consistent with otherwise applicable provisions
13 of Federal law, any Federal agency or depart-
14 ment, component, officer, employee, or agent of
15 the Federal Government solely for—

16 (i) a cybersecurity purpose;

17 (ii) the purpose of identifying a cyber-
18 security threat, including the source of
19 such cybersecurity threat, or a security
20 vulnerability;

21 (iii) the purpose of identifying a cy-
22 bersecurity threat involving the use of an
23 information system by a foreign adversary
24 or terrorist;

1 (iv) the purpose of responding to, or
2 otherwise preventing or mitigating, an im-
3 minent threat of death, serious bodily
4 harm, or serious economic harm, including
5 a terrorist act or a use of a weapon of
6 mass destruction;

7 (v) the purpose of responding to, or
8 otherwise preventing or mitigating, a seri-
9 ous threat to a minor, including sexual ex-
10 ploitation and threats to physical safety; or

11 (vi) the purpose of preventing, inves-
12 tigating, disrupting, or prosecuting an of-
13 fense arising out of a threat described in
14 clause (iv) or any of the offenses listed
15 in—

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

19 (II) chapter 37 of such title (re-
20 lating to espionage and censorship);
21 and

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

24 (B) PROHIBITED ACTIVITIES.—Cyber
25 threat indicators and defensive measures pro-

1 vided to the Federal Government under this Act
2 shall not be disclosed to, retained by, or used
3 by any Federal agency or department for any
4 use not permitted under subparagraph (A).

5 (C) PRIVACY AND CIVIL LIBERTIES.—
6 Cyber threat indicators and defensive measures
7 provided to the Federal Government under this
8 Act shall be retained, used, and disseminated by
9 the Federal Government—

10 (i) in accordance with the policies,
11 procedures, and guidelines required by sub-
12 sections (a) and (b);

13 (ii) in a manner that protects from
14 unauthorized use or disclosure any cyber
15 threat indicators that may contain personal
16 information or information that identifies
17 specific persons; and

18 (iii) in a manner that protects the
19 confidentiality of cyber threat indicators
20 containing personal information or infor-
21 mation that identifies a specific person.

22 (D) FEDERAL REGULATORY AUTHORITY.—

23 (i) IN GENERAL.—Except as provided
24 in clause (ii), cyber threat indicators and
25 defensive measures provided to the Federal

1 Government under this Act shall not be di-
2 rectly used by any Federal, State, tribal,
3 or local government to regulate, including
4 an enforcement action, the lawful activities
5 of any entity, including activities relating
6 to monitoring, operating defensive meas-
7 ures, or sharing cyber threat indicators.

8 (ii) EXCEPTIONS.—

9 (I) REGULATORY AUTHORITY
10 SPECIFICALLY RELATING TO PREVEN-
11 TION OR MITIGATION OF CYBERSECU-
12 RITY THREATS.—Cyber threat indica-
13 tors and defensive measures provided
14 to the Federal Government under this
15 Act may, consistent with Federal or
16 State regulatory authority specifically
17 relating to the prevention or mitiga-
18 tion of cybersecurity threats to infor-
19 mation systems, inform the develop-
20 ment or implementation of regulations
21 relating to such information systems.

22 (II) PROCEDURES DEVELOPED
23 AND IMPLEMENTED UNDER THIS
24 ACT.—Clause (i) shall not apply to

1 under section 5(a)(1) and guidelines are sub-
2 mitted to Congress under section 5(b)(1); or

3 (B) the date that is 60 days after the date
4 of the enactment of this Act.

5 (c) CONSTRUCTION.—Nothing in this section shall be
6 construed—

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

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

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

14 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

15 (1) IN GENERAL.—Not later than 1 year after
16 the date of the enactment of this Act, and not less
17 frequently than once every 2 years thereafter, the
18 heads of the appropriate Federal entities shall joint-
19 ly submit and the Inspector General of the Depart-
20 ment of Homeland Security, the Inspector General
21 of the Intelligence Community, the Inspector Gen-
22 eral of the Department of Justice, the Inspector
23 General of the Department of Defense, and the In-
24 spector General of the Department of Energy, in
25 consultation with the Council of Inspectors General

1 on Financial Oversight, shall jointly submit to Con-
2 gress a detailed report concerning the implementa-
3 tion of this Act.

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

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

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

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

23 (D) An assessment of whether cyber threat
24 indicators have been properly classified and an
25 accounting of the number of security clearances

1 authorized by the Federal Government for the
2 purposes of this Act.

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

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

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

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

17 (F) A review of actions taken by the Fed-
18 eral Government based on cyber threat indica-
19 tors shared with the Federal Government under
20 this Act, including the appropriateness of any
21 subsequent use or dissemination of such cyber
22 threat indicators by a Federal entity under sec-
23 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 summary of the number and type of
5 entities that received classified cyber threat in-
6 dicators from the Federal Government under
7 this Act and an evaluation of the risks and ben-
8 efits of sharing such cyber threat indicators.

9 (3) RECOMMENDATIONS.—Each report sub-
10 mitted under paragraph (1) may include rec-
11 ommendations for improvements or modifications to
12 the authorities and processes under this Act.

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

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

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

1 (A) an assessment of the effect on privacy
2 and civil liberties by the type of activities car-
3 ried 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 concerns re-
7 lating to privacy and civil liberties.

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, and the Inspector General of the Depart-
19 ment of Energy shall, in consultation with the
20 Council of Inspectors General on Financial
21 Oversight, jointly submit to Congress a report
22 on the receipt, use, and dissemination of cyber
23 threat indicators and defensive measures that
24 have been shared with Federal entities under
25 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—

7 (1) to limit or prohibit otherwise lawful disclo-
8 sures of communications, records, or other informa-
9 tion, including reporting of known or suspected
10 criminal activity, by an entity to any other entity or
11 the Federal Government under this Act; or

12 (2) to limit or prohibit otherwise lawful use of
13 such disclosures by any Federal entity, even when
14 such otherwise lawful disclosures duplicate or rep-
15 licate disclosures made under this Act.

16 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in
17 this Act shall be construed to prohibit or limit the disclo-
18 sure of information protected under section 2302(b)(8) of
19 title 5, United States Code (governing disclosures of ille-
20 gality, waste, fraud, abuse, or public health or safety
21 threats), section 7211 of title 5, United States Code (gov-
22 erning disclosures to Congress), section 1034 of title 10,
23 United States Code (governing disclosure to Congress by
24 members of the military), section 1104 of the National
25 Security Act of 1947 (50 U.S.C. 3234) (governing disclo-

1 sure by employees of elements of the intelligence commu-
2 nity), or any similar provision of Federal or State law.

3 (c) PROTECTION OF SOURCES AND METHODS.—

4 Nothing in this Act shall be construed—

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

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

13 (3) to modify the authority of a department or
14 agency of the Federal Government to protect classi-
15 fied information and sources and methods and the
16 national security of the United States.

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

21 (e) PROHIBITED CONDUCT.—Nothing in this Act
22 shall be construed to permit price-fixing, allocating a mar-
23 ket between competitors, monopolizing or attempting to
24 monopolize a market, boycotting, or exchanges of price or

1 cost information, customer lists, or information regarding
2 future competitive planning.

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

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

7 (2) to prohibit a new information sharing rela-
8 tionship;

9 (3) to require a new information sharing rela-
10 tionship between any entity and the Federal Govern-
11 ment; or

12 (4) to require the use of the capability and
13 process within the Department of Homeland Secu-
14 rity developed under section 5(c).

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

17 (1) to amend, repeal, or supersede any current
18 or future contractual agreement, terms of service
19 agreement, or other contractual relationship between
20 any entities, or between any entity and a Federal en-
21 tity; or

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

1 (h) ANTI-TASKING RESTRICTION.—Nothing in this
2 Act shall be construed to permit the Federal Govern-
3 ment—

4 (1) to require an entity to provide information
5 to the Federal Government;

6 (2) to condition the sharing of cyber threat in-
7 dicators with an entity on such entity's provision of
8 cyber threat indicators to the Federal Government;
9 or

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

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

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

23 (k) FEDERAL PREEMPTION.—

24 (1) IN GENERAL.—This Act supersedes any
25 statute or other provision of law of a State or polit-

1 ical subdivision of a State that restricts or otherwise
2 expressly regulates an activity authorized under this
3 Act.

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

9 (1) REGULATORY AUTHORITY.—Nothing in this Act
10 shall be construed—

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

13 (2) to establish or limit any regulatory author-
14 ity not specifically established or limited under this
15 Act; or

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

20 (m) AUTHORITY OF SECRETARY OF DEFENSE TO
21 RESPOND TO CYBER ATTACKS.—Nothing in this Act shall
22 be construed to limit the authority of the Secretary of De-
23 fense to develop, prepare, coordinate, or, when authorized
24 by the President to do so, conduct a military cyber oper-
25 ation in response to a malicious cyber activity carried out

1 against the United States or a United States person by
2 a foreign government or an organization sponsored by a
3 foreign government or a terrorist organization.

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

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

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

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

1 nity participate in such relationships, and whether
2 and how such relationships could be improved.

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

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

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

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

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

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

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

14 **SEC. 10. CONFORMING AMENDMENT.**

15 Section 941(c)(3) of the National Defense Authoriza-
16 tion Act for Fiscal Year 2013 (Public Law 112–239; 10
17 U.S.C. 2224 note) is amended by inserting at the end the
18 following: “The Secretary may share such information
19 with other Federal entities if such information consists of
20 cyber threat indicators and defensive measures and such
21 information is shared consistent with the policies and pro-
22 cedures promulgated by the Attorney General under sec-
23 tion 5 of the Cybersecurity Information Sharing Act of
24 2015.”.