

.....
(Original Signature of Member)

114TH CONGRESS
1ST SESSION

H. R.

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

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

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

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

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Protecting Cyber Networks Act”.

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. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.
- Sec. 3. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.
- Sec. 4. Sharing of cyber threat indicators and defensive measures with appropriate Federal entities other than the Department of Defense or the National Security Agency.
- Sec. 5. Federal Government liability for violations of privacy or civil liberties.
- Sec. 6. Protection from liability.
- Sec. 7. Oversight of Government activities.
- Sec. 8. Report on cybersecurity threats.
- Sec. 9. Construction and preemption.
- Sec. 10. Conforming amendments.
- Sec. 11. Definitions.

1 **SEC. 2. SHARING OF CYBER THREAT INDICATORS AND DE-**
2 **FENSIVE MEASURES BY THE FEDERAL GOV-**
3 **ERNMENT WITH NON-FEDERAL ENTITIES.**

4 (a) IN GENERAL.—Title I of the National Security
5 Act of 1947 (50 U.S.C. 3021 et seq.) is amended by in-
6 serting after section 110 (50 U.S.C. 3045) the following
7 new section:

8 **“SEC. 111. SHARING OF CYBER THREAT INDICATORS AND**
9 **DEFENSIVE MEASURES BY THE FEDERAL**
10 **GOVERNMENT WITH NON-FEDERAL ENTITIES.**

11 **“(a) SHARING BY THE FEDERAL GOVERNMENT.—**

12 **“(1) IN GENERAL.—**Consistent with the protec-
13 tion of classified information, intelligence sources
14 and methods, and privacy and civil liberties, the Di-
15 rector of National Intelligence, in consultation with
16 the heads of the other appropriate Federal entities
17 and the National Laboratories (as defined in section
18 2 of the Energy Policy Act of 2005 (42 U.S.C.

1 15801)), shall develop and promulgate procedures to
2 facilitate and promote—

3 “(A) the timely sharing of classified cyber
4 threat indicators in the possession of the Fed-
5 eral Government with representatives of rel-
6 evant non-Federal entities with appropriate se-
7 curity clearances;

8 “(B) the timely sharing with relevant non-
9 Federal entities of cyber threat indicators or in-
10 formation in the possession of the Federal Gov-
11 ernment that may be declassified and shared at
12 an unclassified level; and

13 “(C) the sharing with non-Federal entities,
14 if appropriate, of information in the possession
15 of the Federal Government about imminent or
16 ongoing cybersecurity threats to such entities to
17 prevent or mitigate adverse impacts from such
18 cybersecurity threats.

19 “(2) DEVELOPMENT OF PROCEDURES.—The
20 procedures developed and promulgated under para-
21 graph (1) shall—

22 “(A) ensure the Federal Government has
23 and maintains the capability to share cyber
24 threat indicators in real time consistent with
25 the protection of classified information;

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

7 “(C) include procedures for notifying non-
8 Federal entities that have received a cyber
9 threat indicator from a Federal entity in ac-
10 cordance with this Act that is known or deter-
11 mined to be in error or in contravention of the
12 requirements of this section, the Protecting
13 Cyber Networks Act, or the amendments made
14 by such Act or another provision of Federal law
15 or policy of such error or contravention;

16 “(D) include requirements for Federal en-
17 tities receiving a cyber threat indicator or de-
18 fensive measure to implement appropriate secu-
19 rity controls to protect against unauthorized ac-
20 cess to, or acquisition of, such cyber threat in-
21 dicator or defensive measure; and

22 “(E) include procedures that require Fed-
23 eral entities, prior to the sharing of a cyber
24 threat indicator, to—

1 “(i) review such cyber threat indicator
2 to assess whether such cyber threat indi-
3 cator, in contravention of the requirement
4 under section 3(d)(2) of the Protecting
5 Cyber Networks Act, contains any infor-
6 mation that such Federal entity knows at
7 the time of sharing to be personal informa-
8 tion of, or information identifying, a spe-
9 cific person not directly related to a
10 cybersecurity threat and remove such in-
11 formation; or

12 “(ii) implement a technical capability
13 configured to remove or exclude any per-
14 sonal information of, or information identi-
15 fying, a specific person not directly related
16 to a cybersecurity threat.

17 “(b) DEFINITIONS.—In this section, the terms ‘ap-
18 propriate Federal entities’, ‘cyber threat indicator’, ‘defen-
19 sive measure’, ‘Federal entity’, and ‘non-Federal entity’
20 have the meaning given such terms in section 11 of the
21 Protecting Cyber Networks Act.”.

22 (b) SUBMITTAL TO CONGRESS.—Not later than 90
23 days after the date of the enactment of this Act, the Direc-
24 tor of National Intelligence, in consultation with the heads
25 of the other appropriate Federal entities, shall submit to

1 Congress the procedures required by section 111(a) of the
2 National Security Act of 1947, as inserted by subsection
3 (a) of this section.

4 (c) TABLE OF CONTENTS AMENDMENT.—The table
5 of contents in the first section of the National Security
6 Act of 1947 is amended by inserting after the item relat-
7 ing to section 110 the following new item:

“Sec. 111. Sharing of cyber threat indicators and defensive measures by the
Federal Government with non-Federal entities.”.

8 **SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
9 **ANALYZING, AND MITIGATING**
10 **CYBERSECURITY THREATS.**

11 (a) AUTHORIZATION FOR PRIVATE-SECTOR DEFEN-
12 SIVE MONITORING.—

13 (1) IN GENERAL.—Notwithstanding any other
14 provision of law, a private entity may, for a
15 cybersecurity purpose, monitor—

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

18 (B) an information system of a non-Fed-
19 eral entity or a Federal entity, upon the written
20 authorization of such non-Federal entity or
21 such Federal entity; and

22 (C) information that is stored on, proc-
23 essed by, or transiting an information system

1 monitored by the private entity under this para-
2 graph.

3 (2) CONSTRUCTION.—Nothing in this sub-
4 section shall be construed to—

5 (A) authorize the monitoring of an infor-
6 mation system, or the use of any information
7 obtained through such monitoring, other than
8 as provided in this Act;

9 (B) authorize the Federal Government to
10 conduct surveillance of any person; or

11 (C) limit otherwise lawful activity.

12 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE
13 MEASURES.—

14 (1) IN GENERAL.—Except as provided in para-
15 graph (2) and notwithstanding any other provision
16 of law, a private entity may, for a cybersecurity pur-
17 pose, operate a defensive measure that is applied
18 and limited to—

19 (A) an information system of such private
20 entity to protect the rights or property of the
21 private entity; and

22 (B) an information system of a non-Fed-
23 eral entity or a Federal entity upon written au-
24 thorization of such non-Federal entity or such
25 Federal entity for operation of such defensive

1 measure to protect the rights or property of
2 such private entity, such non-Federal entity, or
3 such Federal entity.

4 (2) LIMITATION.—The authority provided in
5 paragraph (1) does not include the intentional or
6 reckless operation of any defensive measure that is
7 designed or deployed to destroy, render unusable (in
8 whole or in part), substantially harm, or initiate a
9 new action, process, or procedure on an information
10 system or information stored on, processed by, or
11 transiting such information system not belonging
12 to—

13 (A) the private entity operating such de-
14 fensive measure; or

15 (B) a non-Federal entity or a Federal enti-
16 ty that has provided written authorization to
17 that private entity for operation of such defen-
18 sive measure in accordance with this subsection.

19 (3) CONSTRUCTION.—Nothing in this sub-
20 section shall be construed—

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

24 (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, a non-Federal entity may, for a cybersecurity
7 purpose and consistent with the requirement under
8 subsection (d)(2) to remove personal information of,
9 or information identifying, a specific person not di-
10 rectly related to a cybersecurity threat and the pro-
11 tection of classified information—

12 (A) share a cyber threat indicator or de-
13 fensive measure with any other non-Federal en-
14 tity or an appropriate Federal entity (other
15 than the Department of Defense or any compo-
16 nent of the Department, including the National
17 Security Agency); and

18 (B) receive a cyber threat indicator or de-
19 fensive measure from any other non-Federal en-
20 tity or an appropriate Federal entity.

21 (2) LAWFUL RESTRICTION.—A non-Federal en-
22 tity receiving a cyber threat indicator or defensive
23 measure from another non-Federal entity or a Fed-
24 eral entity shall comply with otherwise lawful restric-
25 tions placed on the sharing or use of such cyber

1 threat indicator or defensive measure by the sharing
2 non-Federal entity or Federal entity.

3 (3) CONSTRUCTION.—Nothing in this sub-
4 section shall be construed to—

5 (A) authorize the sharing or receiving of a
6 cyber threat indicator or defensive measure
7 other than as provided in this subsection;

8 (B) authorize the sharing or receiving of
9 classified information by or with any person not
10 authorized to access such classified information;

11 (C) prohibit any Federal entity from en-
12 gaging in formal or informal technical discus-
13 sion regarding cyber threat indicators or defen-
14 sive measures with a non-Federal entity or from
15 providing technical assistance to address
16 vulnerabilities or mitigate threats at the request
17 of such an entity;

18 (D) authorize the Federal Government to
19 conduct surveillance of any person; or

20 (E) limit otherwise lawful activity.

21 (d) PROTECTION AND USE OF INFORMATION.—

22 (1) SECURITY OF INFORMATION.—A non-Fed-
23 eral entity monitoring an information system, oper-
24 ating a defensive measure, or providing or receiving
25 a cyber threat indicator or defensive measure under

1 this section shall implement an appropriate security
2 control to protect against unauthorized access to, or
3 acquisition of, such cyber threat indicator or defen-
4 sive measure.

5 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
6 TION.—A non-Federal entity sharing a cyber threat
7 indicator pursuant to this Act shall, prior to such
8 sharing, take reasonable efforts to—

9 (A) review such cyber threat indicator to
10 assess whether such cyber threat indicator con-
11 tains any information that the non-Federal en-
12 tity knows at the time of sharing to be personal
13 information of, or information identifying, a
14 specific person not directly related to a
15 cybersecurity threat and remove such informa-
16 tion; or

17 (B) implement a technical capability con-
18 figured to remove any information contained
19 within such indicator that the non-Federal enti-
20 ty knows at the time of sharing to be personal
21 information of, or information identifying, a
22 specific person not directly related to a
23 cybersecurity threat.

24 (3) USE OF CYBER THREAT INDICATORS AND
25 DEFENSIVE MEASURES BY NON-FEDERAL ENTI-

1 TIES.—A non-Federal entity may, for a
2 cybersecurity purpose—

3 (A) use a cyber threat indicator or defen-
4 sive measure shared or received under this sec-
5 tion to monitor or operate a defensive measure
6 on—

7 (i) an information system of such non-
8 Federal entity; or

9 (ii) an information system of another
10 non-Federal entity or a Federal entity
11 upon the written authorization of that
12 other non-Federal entity or that Federal
13 entity; and

14 (B) otherwise use, retain, and further
15 share such cyber threat indicator or defensive
16 measure subject to—

17 (i) an otherwise lawful restriction
18 placed by the sharing non-Federal entity
19 or Federal entity on such cyber threat in-
20 dicator or defensive measure; or

21 (ii) an otherwise applicable provision
22 of law.

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

25 (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 non-Federal entity sharing such indicator,
7 be used by a State, tribal, or local govern-
8 ment for the purpose of preventing, inves-
9 tigating, or prosecuting a felonious crimi-
10 nal act.

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, except as
25 otherwise required by applicable State,

1 tribal, or local law requiring disclosure in
2 any criminal prosecution.

3 (e) NO RIGHT OR BENEFIT.—The sharing of a cyber
4 threat indicator with a non-Federal entity under this Act
5 shall not create a right or benefit to similar information
6 by such non-Federal entity or any other non-Federal enti-
7 ty.

8 **SEC. 4. SHARING OF CYBER THREAT INDICATORS AND DE-**
9 **FENSIVE MEASURES WITH APPROPRIATE**
10 **FEDERAL ENTITIES OTHER THAN THE DE-**
11 **PARTMENT OF DEFENSE OR THE NATIONAL**
12 **SECURITY AGENCY.**

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

15 (1) IN GENERAL.—Section 111 of the National
16 Security Act of 1947, as inserted by section 2 of this
17 Act, is amended by—

18 (A) redesignating subsection (b) as sub-
19 section (c); and

20 (B) by inserting after subsection (a) the
21 following new subsection:

22 “(b) POLICIES AND PROCEDURES FOR SHARING
23 WITH THE APPROPRIATE FEDERAL ENTITIES OTHER
24 THAN THE DEPARTMENT OF DEFENSE OR THE NA-
25 TIONAL SECURITY AGENCY.—

1 “(1) ESTABLISHMENT.—The President shall
2 develop and submit to Congress policies and proce-
3 dures relating to the receipt of cyber threat indica-
4 tors and defensive measures by the Federal Govern-
5 ment.

6 “(2) REQUIREMENTS CONCERNING POLICIES
7 AND PROCEDURES.—The policies and procedures re-
8 quired under paragraph (1) shall—

9 “(A) be developed in accordance with the
10 privacy and civil liberties guidelines required
11 under section 4(b) of the Protecting Cyber Net-
12 works Act;

13 “(B) ensure that—

14 “(i) a cyber threat indicator shared by
15 a non-Federal entity with an appropriate
16 Federal entity (other than the Department
17 of Defense or any component of the De-
18 partment, including the National Security
19 Agency) pursuant to section 3 of such Act
20 is shared in real-time with all of the appro-
21 priate Federal entities (including all rel-
22 evant components thereof);

23 “(ii) the sharing of such cyber threat
24 indicator with appropriate Federal entities
25 is not subject to any delay, modification, or

1 any other action without good cause that
2 could impede receipt by all of the appro-
3 priate Federal entities; and

4 “(iii) such cyber threat indicator is
5 provided to each other Federal entity to
6 which such cyber threat indicator is rel-
7 evant; and

8 “(C) ensure there—

9 “(i) is an audit capability; and

10 “(ii) are appropriate sanctions in
11 place for officers, employees, or agents of
12 a Federal entity who knowingly and will-
13 fully use a cyber threat indicator or de-
14 fense measure shared with the Federal
15 Government by a non-Federal entity under
16 the Protecting Cyber Networks Act other
17 than in accordance with this section and
18 such Act.”.

19 (2) SUBMISSION.—The President shall submit
20 to Congress—

21 (A) not later than 90 days after the date
22 of the enactment of this Act, interim policies
23 and procedures required under section
24 111(b)(1) of the National Security Act of 1947,

1 as inserted by paragraph (1) of this section;
2 and

3 (B) not later than 180 days after such
4 date, final policies and procedures required
5 under such section 111(b)(1).

6 (b) PRIVACY AND CIVIL LIBERTIES.—

7 (1) GUIDELINES OF ATTORNEY GENERAL.—The
8 Attorney General, in consultation with the heads of
9 the other appropriate Federal agencies and with offi-
10 cers designated under section 1062 of the Intel-
11 ligence Reform and Terrorism Prevention Act of
12 2004 (42 U.S.C. 2000ee–1), shall develop and peri-
13 odically review guidelines relating to privacy and
14 civil liberties that govern the receipt, retention, use,
15 and dissemination of cyber threat indicators by a
16 Federal entity obtained in accordance with this Act
17 and the amendments made by this Act.

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

23 (A) limit the impact on privacy and civil
24 liberties of activities by the Federal Government
25 under this Act, including guidelines to ensure

1 that personal information of, or information
2 identifying, specific persons is properly removed
3 from information received, retained, used, or
4 disseminated by a Federal entity in accordance
5 with this Act or the amendments made by this
6 Act;

7 (B) limit the receipt, retention, use, and
8 dissemination of cyber threat indicators con-
9 taining personal information of, or information
10 identifying, specific persons, including by estab-
11 lishing—

12 (i) a process for the timely destruction
13 of such information that is known not to
14 be directly related to a use for a
15 cybersecurity purpose;

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

19 (iii) a process to inform recipients
20 that such indicators may only be used for
21 a cybersecurity purpose;

22 (C) include requirements to safeguard
23 cyber threat indicators containing personal in-
24 formation of, or identifying, specific persons
25 from unauthorized access or acquisition, includ-

1 ing appropriate sanctions for activities by offi-
2 cers, employees, or agents of the Federal Gov-
3 ernment in contravention of such guidelines;

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

10 (E) be consistent with any other applicable
11 provisions of law and the fair information prac-
12 tice principles set forth in appendix A of the
13 document entitled “National Strategy for
14 Trusted Identities in Cyberspace” and pub-
15 lished by the President in April, 2011; and

16 (F) include steps that may be needed so
17 that dissemination of cyber threat indicators is
18 consistent with the protection of classified infor-
19 mation and other sensitive national security in-
20 formation.

21 (c) NATIONAL CYBER THREAT INTELLIGENCE INTE-
22 GRATION CENTER.—

23 (1) ESTABLISHMENT.—Title I of the National
24 Security Act of 1947 (50 U.S.C. 3021 et seq.), as

1 amended by section 2 of this Act, is further amend-
2 ed—

3 (A) by redesignating section 119B as sec-
4 tion 119C; and

5 (B) by inserting after section 119A the fol-
6 lowing new section:

7 **“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION**
8 **CENTER.**

9 “(a) ESTABLISHMENT.—There is within the Office of
10 the Director of National Intelligence a Cyber Threat Intel-
11 ligence Integration Center.

12 “(b) DIRECTOR.—There is a Director of the Cyber
13 Threat Intelligence Integration Center, who shall be the
14 head of the Cyber Threat Intelligence Integration Center,
15 and who shall be appointed by the Director of National
16 Intelligence.

17 “(c) PRIMARY MISSIONS.—The Cyber Threat Intel-
18 ligence Integration Center shall—

19 “(1) serve as the primary organization within
20 the Federal Government for analyzing and inte-
21 grating all intelligence possessed or acquired by the
22 United States pertaining to cyber threats;

23 “(2) ensure that appropriate departments and
24 agencies have full access to and receive all-source in-
25 telligence support needed to execute the cyber threat

1 intelligence activities of such agencies and to per-
2 form independent, alternative analyses;

3 “(3) disseminate cyber threat analysis to the
4 President, the appropriate departments and agencies
5 of the Federal Government, and the appropriate
6 committees of Congress;

7 “(4) coordinate cyber threat intelligence activi-
8 ties of the departments and agencies of the Federal
9 Government; and

10 “(5) conduct strategic cyber threat intelligence
11 planning for the Federal Government.

12 “(d) LIMITATIONS.—The Cyber Threat Intelligence
13 Integration Center shall—

14 “(1) have not more than 50 permanent posi-
15 tions;

16 “(2) in carrying out the primary missions of the
17 Center described in subsection (c), may not augment
18 staffing through detailees, assignees, or core con-
19 tractor personnel or enter into any personal services
20 contracts to exceed the limitation under paragraph
21 (1); and

22 “(3) be located in a building owned or operated
23 by an element of the intelligence community as of
24 the date of the enactment of this section.”

1 (4) TABLE OF CONTENTS AMENDMENTS.—The
2 table of contents in the first section of the National
3 Security Act of 1947, as amended by section 2 of
4 this Act, is further amended by striking the item re-
5 lating to section 119B and inserting the following
6 new items:

“Sec. 119B. Cyber Threat Intelligence Integration Center.

“Sec. 119C. National intelligence centers.”.

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 a cyber threat indicator or
11 defensive measure to the Federal Government under
12 this Act shall not constitute a waiver of any applica-
13 ble privilege or protection provided by law, including
14 trade secret protection.

15 (2) PROPRIETARY INFORMATION.—Consistent
16 with section 3(c)(2), a cyber threat indicator or de-
17 fensive measure provided by a non-Federal entity to
18 the Federal Government under this Act shall be con-
19 sidered the commercial, financial, and proprietary
20 information of the non-Federal entity that is the
21 originator of such cyber threat indicator or defensive
22 measure when so designated by such non-Federal
23 entity or a non-Federal entity acting in accordance
24 with the written authorization of the non-Federal

1 entity that is the originator of such cyber threat in-
2 dicator or defensive measure.

3 (3) EXEMPTION FROM DISCLOSURE.—A cyber
4 threat indicator or defensive measure provided to the
5 Federal Government under this Act shall be—

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

11 (B) withheld, without discretion, from the
12 public under section 552(b)(3)(B) of title 5,
13 United States Code, and any State, tribal, or
14 local provision of law requiring disclosure of in-
15 formation or records, except as otherwise re-
16 quired by applicable Federal, State, tribal, or
17 local law requiring disclosure in any criminal
18 prosecution.

19 (4) EX PARTE COMMUNICATIONS.—The provi-
20 sion of a cyber threat indicator or defensive measure
21 to the Federal Government under this Act shall not
22 be subject to a rule of any Federal department or
23 agency or any judicial doctrine regarding ex parte
24 communications with a decision-making official.

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

1 (A) AUTHORIZED ACTIVITIES.—A cyber
2 threat indicator or defensive measure provided
3 to the Federal Government under this Act may
4 be disclosed to, retained by, and used by, con-
5 sistent with otherwise applicable provisions of
6 Federal law, any department, agency, compo-
7 nent, officer, employee, or agent of the Federal
8 Government solely for—

9 (i) a cybersecurity purpose;

10 (ii) the purpose of responding to,
11 prosecuting, or otherwise preventing or
12 mitigating a threat of death or serious
13 bodily harm or an offense arising out of
14 such a threat;

15 (iii) the purpose of responding to, or
16 otherwise preventing or mitigating, a seri-
17 ous threat to a minor, including sexual ex-
18 ploitation and threats to physical safety; or

19 (iv) the purpose of preventing, inves-
20 tigating, disrupting, or prosecuting any of
21 the offenses listed in sections 1028, 1029,
22 1030, and 3559(c)(2)(F) and chapters 37
23 and 90 of title 18, United States Code.

24 (B) PROHIBITED ACTIVITIES.—A cyber
25 threat indicator or defensive measure provided

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

5 (C) PRIVACY AND CIVIL LIBERTIES.—A
6 cyber threat indicator or defensive measure pro-
7 vided to the Federal Government under this Act
8 shall be retained, used, and disseminated by the
9 Federal Government in accordance with—

10 (i) the policies and procedures relating
11 to the receipt of cyber threat indicators
12 and defensive measures by the Federal
13 Government required by subsection (b) of
14 section 111 of the National Security Act of
15 1947, as added by subsection (a) of this
16 section; and

17 (ii) the privacy and civil liberties
18 guidelines required by subsection (b).

19 **SEC. 5. FEDERAL GOVERNMENT LIABILITY FOR VIOLA-**
20 **TIONS OF PRIVACY OR CIVIL LIBERTIES.**

21 (a) IN GENERAL.—If a department or agency of the
22 Federal Government intentionally or willfully violates the
23 privacy and civil liberties guidelines issued by the Attorney
24 General under section 4(b), the United States shall be lia-

1 ble to a person injured by such violation in an amount
2 equal to the sum of—

3 (1) the actual damages sustained by the person
4 as a result of the violation or \$1,000, whichever is
5 greater; and

6 (2) the costs of the action together with reason-
7 able attorney fees as determined by the court.

8 (b) VENUE.—An action to enforce liability created
9 under this section may be brought in the district court
10 of the United States in—

11 (1) the district in which the complainant re-
12 sides;

13 (2) the district in which the principal place of
14 business of the complainant is located;

15 (3) the district in which the department or
16 agency of the Federal Government that violated such
17 privacy and civil liberties guidelines is located; or

18 (4) the District of Columbia.

19 (c) STATUTE OF LIMITATIONS.—No action shall lie
20 under this subsection unless such action is commenced not
21 later than two years after the date of the violation of the
22 privacy and civil liberties guidelines issued by the Attorney
23 General under section 4(b) that is the basis for the action.

24 (d) EXCLUSIVE CAUSE OF ACTION.—A cause of ac-
25 tion under this subsection shall be the exclusive means

1 available to a complainant seeking a remedy for a violation
2 by a department or agency of the Federal Government
3 under this Act.

4 **SEC. 6. PROTECTION FROM LIABILITY.**

5 (a) MONITORING OF INFORMATION SYSTEMS.—No
6 cause of action shall lie or be maintained in any court
7 against any private entity, and such action shall be
8 promptly dismissed, for the monitoring of an information
9 system and information under section 3(a) that is con-
10 ducted in good faith in accordance with this Act and the
11 amendments made by this Act.

12 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
13 CATORS.—No cause of action shall lie or be maintained
14 in any court against any non-Federal entity, and such ac-
15 tion shall be promptly dismissed, for the sharing or receipt
16 of a cyber threat indicator or defensive measure under sec-
17 tion 3(c), or a good faith failure to act based on such shar-
18 ing or receipt, if such sharing or receipt is conducted in
19 good faith in accordance with this Act and the amend-
20 ments made by this Act.

21 (c) WILLFUL MISCONDUCT.—

22 (1) RULE OF CONSTRUCTION.—Nothing in this
23 section shall be construed—

24 (A) to require dismissal of a cause of ac-
25 tion against a non-Federal entity (including a

1 private entity) that has engaged in willful mis-
2 conduct in the course of conducting activities
3 authorized by this Act or the amendments made
4 by this Act; or

5 (B) to undermine or limit the availability
6 of otherwise applicable common law or statu-
7 tory defenses.

8 (2) PROOF OF WILLFUL MISCONDUCT.—In any
9 action claiming that subsection (a) or (b) does not
10 apply due to willful misconduct described in para-
11 graph (1), the plaintiff shall have the burden of
12 proving by clear and convincing evidence the willful
13 misconduct by each non-Federal entity subject to
14 such claim and that such willful misconduct proxi-
15 mately caused injury to the plaintiff.

16 (3) WILLFUL MISCONDUCT DEFINED.—In this
17 subsection, the term “willful misconduct” means an
18 act or omission that is taken—

19 (A) intentionally to achieve a wrongful
20 purpose;

21 (B) knowingly without legal or factual jus-
22 tification; and

23 (C) in disregard of a known or obvious risk
24 that is so great as to make it highly probable
25 that the harm will outweigh the benefit.

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

2 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

3 (1) IN GENERAL.—Section 111 of the National
4 Security Act of 1947, as amended by section 4(a) of
5 this Act, is further amended—

6 (A) by redesignating subsection (c) (as re-
7 designated by such section 4(a)) as subsection
8 (d); and

9 (B) by inserting after subsection (b) (as
10 inserted by such section 4(a)) the following new
11 subsection:

12 “(c) BIENNIAL REPORT ON IMPLEMENTATION.—

13 “(1) IN GENERAL.—Not less frequently than
14 once every two years, the Director of National Intel-
15 ligence, in consultation with the heads of the other
16 appropriate Federal entities, shall submit to Con-
17 gress a report concerning the implementation of this
18 section and the Protecting Cyber Networks Act.

19 “(2) CONTENTS.—Each report submitted under
20 paragraph (1) shall include the following:

21 “(A) An assessment of the sufficiency of
22 the policies, procedures, and guidelines required
23 by this section and section 4 of the Protecting
24 Cyber Networks Act in ensuring that cyber
25 threat indicators are shared effectively and re-
26 sponsibly within the Federal Government.

1 “(B) An assessment of whether the proce-
2 dures developed under section 3 of such Act
3 comply with the goals described in subpara-
4 graphs (A), (B), and (C) of subsection (a)(1).

5 “(C) An assessment of whether cyber
6 threat indicators have been properly classified
7 and an accounting of the number of security
8 clearances authorized by the Federal Govern-
9 ment for the purposes of this section and such
10 Act.

11 “(D) A review of the type of cyber threat
12 indicators shared with the Federal Government
13 under this section and such Act, including the
14 following:

15 “(i) The degree to which such infor-
16 mation may impact the privacy and civil
17 liberties of specific persons.

18 “(ii) A quantitative and qualitative as-
19 sessment of the impact of the sharing of
20 such cyber threat indicators with the Fed-
21 eral Government on privacy and civil lib-
22 erties of specific persons.

23 “(iii) The adequacy of any steps taken
24 by the Federal Government to reduce such
25 impact.

1 “(E) 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 section or such Act, including the appro-
5 priateness of any subsequent use or dissemina-
6 tion of such cyber threat indicators by a Fed-
7 eral entity under this section or section 4 of
8 such Act.

9 “(F) A description of any significant viola-
10 tions of the requirements of this section or such
11 Act by the Federal Government.

12 “(G) A summary of the number and type
13 of non-Federal entities that received classified
14 cyber threat indicators from the Federal Gov-
15 ernment under this section or such Act and an
16 evaluation of the risks and benefits of sharing
17 such cyber threat indicators.

18 “(3) RECOMMENDATIONS.—Each report sub-
19 mitted under paragraph (1) may include such rec-
20 ommendations as the heads of the appropriate Fed-
21 eral entities may have for improvements or modifica-
22 tions to the authorities and processes under this sec-
23 tion or such Act.

1 “(4) FORM OF REPORT.—Each report required
2 by paragraph (1) shall be submitted in unclassified
3 form, but may include a classified annex.”.

4 (2) INITIAL REPORT.—The first report required
5 under subsection (c) of section 111 of the National
6 Security Act of 1947, as inserted by paragraph (1)
7 of this subsection, shall be submitted not later than
8 one year after the date of the enactment of this Act.

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

10 (1) BIENNIAL REPORT FROM PRIVACY AND
11 CIVIL LIBERTIES OVERSIGHT BOARD.—

12 (A) IN GENERAL.—Section 1061(e) of the
13 Intelligence Reform and Terrorism Prevention
14 Act of 2004 (42 U.S.C. 2000ee(e)) is amended
15 by adding at the end the following new para-
16 graph:

17 “(3) BIENNIAL REPORT ON CERTAIN CYBER AC-
18 TIVITIES.—The Privacy and Civil Liberties Over-
19 sight Board shall biennially submit to Congress and
20 the President a report containing—

21 “(A) an assessment of the privacy and civil
22 liberties impact of the activities carried out
23 under the Protecting Cyber Networks Act and
24 the amendments made by such Act; and

1 “(B) an assessment of the sufficiency of
2 the policies, procedures, and guidelines estab-
3 lished pursuant to section 4 of the Protecting
4 Cyber Networks Act and the amendments made
5 by such section 4 in addressing privacy and civil
6 liberties concerns.”.

7 (B) INITIAL REPORT.—The first report re-
8 quired under paragraph (3) of section 1061(e)
9 of the Intelligence Reform and Terrorism Pre-
10 vention Act of 2004 (42 U.S.C. 2000ee(e)), as
11 added by subparagraph (A) of this paragraph,
12 shall be submitted not later than 2 years after
13 the date of the enactment of this Act.

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

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

1 jointly submit to Congress a report on the re-
2 ceipt, use, and dissemination of cyber threat in-
3 dicators and defensive measures that have been
4 shared with Federal entities under this Act and
5 the amendments made by this Act.

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 Act or the amendments made by this Act.

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. 8. REPORT ON CYBERSECURITY THREATS.**

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

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

20 (1) An assessment of—

21 (A) the current intelligence sharing and co-
22 operation relationships of the United States
23 with other countries regarding cybersecurity
24 threats (including cyber attacks, theft, and data
25 breaches) directed against the United States

1 that threaten the United States national secu-
2 rity interests, economy, and intellectual prop-
3 erty; and

4 (B) the relative utility of such relation-
5 ships, which elements of the intelligence com-
6 munity participate in such relationships, and
7 whether and how such relationships could be
8 improved.

9 (2) A list and an assessment of the countries
10 and non-state actors that are the primary threats of
11 carrying out a cybersecurity threat (including a
12 cyber attack, theft, or data breach) against the
13 United States and that threaten the United States
14 national security, economy, and intellectual property.

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

23 (4) An assessment of additional technologies or
24 capabilities that would enhance the ability of the
25 United States to prevent and to respond to

1 cybersecurity threats (including cyber attacks, theft,
2 and data breaches).

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

7 (c) FORM OF REPORT.—The report required by sub-
8 section (a) shall be submitted in unclassified form, but
9 may include a classified annex.

10 (d) 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. 9. CONSTRUCTION AND PREEMPTION.**

15 (a) PROHIBITION OF SURVEILLANCE.—Nothing in
16 this Act or the amendments made by this Act shall be
17 construed to authorize the Department of Defense or the
18 National Security Agency or any other element of the in-
19 telligence community to target a person for surveillance.

20 (b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in
21 this Act or the amendments made by this Act shall be
22 construed to limit or prohibit—

23 (1) otherwise lawful disclosures of communica-
24 tions, records, or other information, including re-
25 porting of known or suspected criminal activity, by

1 a non-Federal entity to any other non-Federal entity
2 or the Federal Government; or

3 (2) any otherwise lawful use of such disclosures
4 by any entity of the Federal government, without re-
5 gard to whether such otherwise lawful disclosures
6 duplicate or replicate disclosures made under this
7 Act.

8 (c) WHISTLE BLOWER PROTECTIONS.—Nothing in
9 this Act or the amendments made by this Act shall be
10 construed to prohibit or limit the disclosure of information
11 protected under section 2302(b)(8) of title 5, United
12 States Code (governing disclosures of illegality, waste,
13 fraud, abuse, or public health or safety threats), section
14 7211 of title 5, United States Code (governing disclosures
15 to Congress), section 1034 of title 10, United States Code
16 (governing disclosure to Congress by members of the mili-
17 tary), or any similar provision of Federal or State law..

18 (d) PROTECTION OF SOURCES AND METHODS.—
19 Nothing in this Act or the amendments made by this Act
20 shall be construed—

21 (1) as creating any immunity against, or other-
22 wise affecting, any action brought by the Federal
23 Government, or any department or agency thereof,
24 to enforce any law, executive order, or procedure

1 governing the appropriate handling, disclosure, or
2 use of classified information;

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

5 (3) to modify the authority of a department or
6 agency of the Federal Government to protect classi-
7 fied information, intelligence sources and methods,
8 and the national security of the United States.

9 (e) RELATIONSHIP TO OTHER LAWS.—Nothing in
10 this Act or the amendments made by this Act shall be
11 construed to affect any requirement under any other pro-
12 vision of law for a non-Federal entity to provide informa-
13 tion to the Federal Government.

14 (f) INFORMATION SHARING RELATIONSHIPS.—Noth-
15 ing in this Act or the amendments made by this Act shall
16 be construed—

17 (1) to limit or modify an existing information-
18 sharing relationship;

19 (2) to prohibit a new information-sharing rela-
20 tionship; or

21 (3) to require a new information-sharing rela-
22 tionship between any non-Federal entity and the
23 Federal Government.

1 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS
2 AND RIGHTS.—Nothing in this Act or the amendments
3 made by this Act shall be construed—

4 (1) to amend, repeal, or supersede any current
5 or future contractual agreement, terms of service
6 agreement, or other contractual relationship between
7 any non-Federal entities, or between any non-Fed-
8 eral entity and a Federal entity; or

9 (2) to abrogate trade secret or intellectual prop-
10 erty rights of any non-Federal entity or Federal en-
11 tity.

12 (h) ANTI-TASKING RESTRICTION.—Nothing in this
13 Act or the amendments made by this Act shall be con-
14 strued to permit the Federal Government—

15 (1) to require a non-Federal entity to provide
16 information to the Federal Government;

17 (2) to condition the sharing of a cyber threat
18 indicator with a non-Federal entity on such non-
19 Federal entity's provision of a cyber threat indicator
20 to the Federal Government; or

21 (3) to condition the award of any Federal
22 grant, contract, or purchase on the provision of a
23 cyber threat indicator to a Federal entity.

24 (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-
25 ing in this Act or the amendments made by this Act shall

1 be construed to subject any non-Federal entity to liability
2 for choosing not to engage in a voluntary activiy author-
3 ized in this Act and the amendments made by this Act.

4 (j) USE AND RETENTION OF INFORMATION.—Noth-
5 ing in this Act or the amendments made by this Act shall
6 be construed to authorize, or to modify any existing au-
7 thority of, a department or agency of the Federal Govern-
8 ment to retain or use any information shared under this
9 Act or the amendments made by this Act for any use other
10 than permitted in this Act or the amendments made by
11 this Act.

12 (k) FEDERAL PREEMPTION.—

13 (1) IN GENERAL.—This Act and the amend-
14 ments made by this Act supersede any statute or
15 other provision of law of a State or political subdivi-
16 sion of a State that restricts or otherwise expressly
17 regulates an activity authorized under this Act or
18 the amendments made by this Act.

19 (2) STATE LAW ENFORCEMENT.—Nothing in
20 this Act or the amendments made by this Act shall
21 be construed to supersede any statute or other provi-
22 sion of law of a State or political subdivision of a
23 State concerning the use of authorized law enforce-
24 ment practices and procedures.

1 (1) REGULATORY AUTHORITY.—Nothing in this Act
2 or the amendments made by this Act shall be construed—

3 (1) to authorize the promulgation of any regu-
4 lations not specifically authorized by this Act or the
5 amendments made by this Act;

6 (2) to establish any regulatory authority not
7 specifically established under this Act or the amend-
8 ments made by this Act; or

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

13 **SEC. 10. CONFORMING AMENDMENTS.**

14 Section 552(b) of title 5, United States Code, is
15 amended—

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

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

20 (3) by inserting after paragraph (9) the fol-
21 lowing:

22 “(10) information shared with or provided to
23 the Federal Government pursuant to the Protecting
24 Cyber Networks Act or the amendments made by
25 such Act.”.

1 **SEC. 11. 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) APPROPRIATE FEDERAL ENTITIES.—The
7 term “appropriate Federal entities” means the fol-
8 lowing:

9 (A) The Department of Commerce.

10 (B) The Department of Defense.

11 (C) The Department of Energy.

12 (D) The Department of Homeland Secu-
13 rity.

14 (E) The Department of Justice.

15 (F) The Department of the Treasury.

16 (G) The Office of the Director of National
17 Intelligence.

18 (3) CYBERSECURITY PURPOSE.—The term
19 “cybersecurity purpose” means the purpose of pro-
20 tecting an information system or information that is
21 stored on, processed by, or transiting an information
22 system from a cybersecurity threat or security vul-
23 nerability or identifying the source of a cybersecurity
24 threat or using a defensive measure.

25 (4) CYBERSECURITY THREAT.—

1 (A) IN GENERAL.—Except as provided in
2 subparagraph (B), the term “cybersecurity
3 threat” means an action, not protected by the
4 first amendment to the Constitution of the
5 United States, on or through an information
6 system that may result in an unauthorized ef-
7 fort to adversely impact the security, confiden-
8 tiality, integrity, or availability of an informa-
9 tion system or information that is stored on,
10 processed by, or transiting an information sys-
11 tem.

12 (B) EXCLUSION.—The term “cybersecurity
13 threat” does not include any action that solely
14 involves a violation of a consumer term of serv-
15 ice or a consumer licensing agreement.

16 (5) CYBER THREAT INDICATOR.—The term
17 “cyber threat indicator” means information or a
18 physical object that is necessary to describe or iden-
19 tify—

20 (A) malicious reconnaissance, including
21 anomalous patterns of communications that ap-
22 pear to be transmitted for the purpose of gath-
23 ering technical information related to a
24 cybersecurity threat or security vulnerability;

1 (B) a method of defeating a security con-
2 trol or exploitation of a security vulnerability;

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

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

12 (E) malicious cyber command and control;

13 (F) the actual or potential harm caused by
14 an incident, including a description of the infor-
15 mation exfiltrated as a result of a particular
16 cybersecurity threat; or

17 (G) any other attribute of a cybersecurity
18 threat, if disclosure of such attribute is not oth-
19 erwise prohibited by law.

20 (6) DEFENSIVE MEASURE.—The term “defen-
21 sive measure” means an action, device, procedure,
22 technique, or other measure executed on an informa-
23 tion system or information that is stored on, proc-
24 essed by, or transiting an information system that

1 prevents or mitigates a known or suspected
2 cybersecurity threat or security vulnerability.

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

7 (8) INFORMATION SYSTEM.—The term “infor-
8 mation system”—

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

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

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

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

1 (11) MALICIOUS RECONNAISSANCE.—The term
2 “malicious reconnaissance” means a method for ac-
3 tively probing or passively monitoring an information
4 system for the purpose of discerning security
5 vulnerabilities of the information system, if such
6 method is associated with a known or suspected
7 cybersecurity threat.

8 (12) MONITOR.—The term “monitor” means to
9 acquire, identify, scan, or otherwise possess informa-
10 tion that is stored on, processed by, or transiting an
11 information system.

12 (13) NON-FEDERAL ENTITY.—

13 (A) IN GENERAL.—Except as otherwise
14 provided in this paragraph, the term “non-Fed-
15 eral entity” means any private entity, non-Fed-
16 eral government department or agency, or
17 State, tribal, or local government (including a
18 political subdivision, department, officer, em-
19 ployee, or agent thereof).

20 (B) INCLUSIONS.—The term “non-Federal
21 entity” includes a government department or
22 agency (including an officer, employee, or agent
23 thereof) of the District of Columbia, the Com-
24 monwealth of Puerto Rico, the Virgin Islands,
25 Guam, American Samoa, the Northern Mariana

1 Islands, and any other territory or possession of
2 the United States.

3 (C) EXCLUSION.—The term “non-Federal
4 entity” does not include a foreign power as de-
5 fined in section 101 of the Foreign Intelligence
6 Surveillance Act of 1978 (50 U.S.C. 1801).

7 (14) 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 component of a State, tribal, or
17 local government performing electric utility
18 services.

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

23 (15) REAL TIME; REAL-TIME.—The terms “real
24 time” and “real-time” mean a process by which an
25 automated, machine-to-machine system processes

1 cyber threat indicators such that the time in which
2 the occurrence of an event and the reporting or re-
3 cording of it are as simultaneous as technologically
4 practicable.

5 (16) SECURITY CONTROL.—The term “security
6 control” means the management, operational, and
7 technical controls used to protect against an unau-
8 thorized effort to adversely impact the security, con-
9 fidentiality, integrity, and availability of an informa-
10 tion system or its information.

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

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