

114TH CONGRESS  
1ST SESSION

# H. R. 1560

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

---

## IN THE HOUSE OF REPRESENTATIVES

MARCH 24, 2015

Mr. NUNES (for himself, Mr. SCHIFF, Mr. WESTMORELAND, and Mr. HIMES) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

---

## 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.  
 19 15801)), shall develop and promulgate procedures to  
 20 facilitate and promote—

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

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

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

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

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

24           “(B) incorporate, to the greatest extent  
25 practicable, existing processes and existing roles

1 and responsibilities of Federal and non-Federal  
2 entities for information sharing by the Federal  
3 Government, including sector-specific informa-  
4 tion sharing and analysis centers;

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

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

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

23 “(i) review such cyber threat indicator  
24 to assess whether such cyber threat indi-  
25 cator, in contravention of the requirement

1 under section 3(d)(2) of the Protecting  
2 Cyber Networks Act, contains any infor-  
3 mation that such Federal entity knows at  
4 the time of sharing to be personal informa-  
5 tion of, or information identifying, a spe-  
6 cific person not directly related to a cyber-  
7 security threat and remove such informa-  
8 tion; or

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

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

19 (b) SUBMITTAL TO CONGRESS.—Not later than 90  
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 other appropriate Federal entities, shall submit to  
23 Congress the procedures required by section 111(a) of the  
24 National Security Act of 1947, as inserted by subsection  
25 (a) of this section.

1 (c) TABLE OF CONTENTS AMENDMENT.—The table  
 2 of contents in the first section of the National Security  
 3 Act of 1947 is amended by inserting after the item relat-  
 4 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.”.

5 **SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
 6 **ANALYZING, AND MITIGATING CYBERSECU-**  
 7 **RITY THREATS.**

8 (a) AUTHORIZATION FOR PRIVATE-SECTOR DEFEN-  
 9 SIVE MONITORING.—

10 (1) IN GENERAL.—Notwithstanding any other  
 11 provision of law, a private entity may, for a cyberse-  
 12 curity purpose, monitor—

13 (A) an information system of such private  
 14 entity;

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

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

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

1 (A) authorize the monitoring of an infor-  
2 mation system, or the use of any information  
3 obtained through such monitoring, other than  
4 as provided in this Act;

5 (B) authorize the Federal Government to  
6 conduct surveillance of any person; or

7 (C) limit otherwise lawful activity.

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

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

15 (A) an information system of such private  
16 entity to protect the rights or property of the  
17 private entity; and

18 (B) an information system of a non-Fed-  
19 eral entity or a Federal entity upon written au-  
20 thorization of such non-Federal entity or such  
21 Federal entity for operation of such defensive  
22 measure to protect the rights or property of  
23 such private entity, such non-Federal entity, or  
24 such Federal entity.

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

10                   (A) the private entity operating such de-  
11 fensive measure; or

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

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

18                   (A) to authorize the use of a defensive  
19 measure other than as provided in this sub-  
20 section; or

21                   (B) to limit otherwise lawful activity.

22           (c) AUTHORIZATION FOR SHARING OR RECEIVING  
23 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-  
24 URES.—



1           (1) IN GENERAL.—Except as provided in para-  
2           graph (2) and notwithstanding any other provision  
3           of law, a non-Federal entity may, for a cybersecurity  
4           purpose and consistent with the requirement under  
5           subsection (d)(2) to remove personal information of,  
6           or information identifying, a specific person not di-  
7           rectly related to a cybersecurity threat and the pro-  
8           tection of classified information—

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

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

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

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

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

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

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

16           (D) authorize the Federal Government to  
17 conduct surveillance of any person; or

18           (E) limit otherwise lawful activity.

19       (d) PROTECTION AND USE OF INFORMATION.—

20           (1) SECURITY OF INFORMATION.—A non-Fed-  
21 eral entity monitoring an information system, oper-  
22 ating a defensive measure, or providing or receiving  
23 a cyber threat indicator or defensive measure under  
24 this section shall implement an appropriate security  
25 control to protect against unauthorized access to, or

1 acquisition of, such cyber threat indicator or defen-  
2 sive measure.

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

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

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

21 (3) USE OF CYBER THREAT INDICATORS AND  
22 DEFENSIVE MEASURES BY NON-FEDERAL ENTI-  
23 TIES.—A non-Federal entity may, for a cybersecu-  
24 rity purpose—

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

5 (i) an information system of such non-  
6 Federal entity; or

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

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

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

19 (ii) an otherwise applicable provision  
20 of law.

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

23 (A) LAW ENFORCEMENT USE.—

24 (i) PRIOR WRITTEN CONSENT.—Ex-  
25 cept as provided in clause (ii), a cyber

1 threat indicator shared with a State, tribal,  
2 or local government under this section  
3 may, with the prior written consent of the  
4 non-Federal entity sharing such indicator,  
5 be used by a State, tribal, or local govern-  
6 ment for the purpose of preventing, inves-  
7 tigating, or prosecuting a felonious crimi-  
8 nal act.

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

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

18 (i) deemed voluntarily shared informa-  
19 tion; and

20 (ii) exempt from disclosure under any  
21 State, tribal, or local law requiring disclo-  
22 sure of information or records, except as  
23 otherwise required by applicable State,  
24 tribal, or local law requiring disclosure in  
25 any criminal prosecution.

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

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

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

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

16 (A) redesignating subsection (b) as sub-  
17 section (c); and

18 (B) by inserting after subsection (a) the  
19 following new subsection:

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

24 “(1) ESTABLISHMENT.—The President shall  
25 develop and submit to Congress policies and proce-

1       dures relating to the receipt of cyber threat indica-  
2       tors and defensive measures by the Federal Govern-  
3       ment.

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

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

11                     “(B) ensure that—

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

21                               “(ii) the sharing of such cyber threat  
22                               indicator with appropriate Federal entities  
23                               is not subject to any delay, modification, or  
24                               any other action without good cause that

1 could impede receipt by all of the appro-  
2 priate Federal entities; and

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

7 “(C) ensure there—

8 “(i) is an audit capability; and

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

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

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



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

4 (b) PRIVACY AND CIVIL LIBERTIES.—

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

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

20 (A) limit the impact on privacy and civil  
21 liberties of activities by the Federal Government  
22 under this Act, including guidelines to ensure  
23 that personal information of, or information  
24 identifying, specific persons is properly removed  
25 from information received, retained, used, or

1 disseminated by a Federal entity in accordance  
2 with this Act or the amendments made by this  
3 Act;

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

9 (i) a process for the timely destruction  
10 of such information that is known not to  
11 be directly related to a use for a cybersecu-  
12 rity purpose;

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

16 (iii) a process to inform recipients  
17 that such indicators may only be used for  
18 a cybersecurity purpose;

19 (C) include requirements to safeguard  
20 cyber threat indicators containing personal in-  
21 formation of, or identifying, specific persons  
22 from unauthorized access or acquisition, includ-  
23 ing appropriate sanctions for activities by offi-  
24 cers, employees, or agents of the Federal Gov-  
25 ernment in contravention of such guidelines;

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

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

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

18 (c) NATIONAL CYBER THREAT INTELLIGENCE INTE-  
19 GRATION CENTER.—

20 (1) ESTABLISHMENT.—Title I of the National  
21 Security Act of 1947 (50 U.S.C. 3021 et seq.), as  
22 amended by section 2 of this Act, is further amend-  
23 ed—

24 (A) by redesignating section 119B as sec-  
25 tion 119C; and

1 (B) by inserting after section 119A the fol-  
2 lowing new section:

3 **“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION**  
4 **CENTER.**

5 “(a) ESTABLISHMENT.—There is within the Office of  
6 the Director of National Intelligence a Cyber Threat Intel-  
7 ligence Integration Center.

8 “(b) DIRECTOR.—There is a Director of the Cyber  
9 Threat Intelligence Integration Center, who shall be the  
10 head of the Cyber Threat Intelligence Integration Center,  
11 and who shall be appointed by the Director of National  
12 Intelligence.

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

15 “(1) serve as the primary organization within  
16 the Federal Government for analyzing and inte-  
17 grating all intelligence possessed or acquired by the  
18 United States pertaining to cyber threats;

19 “(2) ensure that appropriate departments and  
20 agencies have full access to and receive all-source in-  
21 telligence support needed to execute the cyber threat  
22 intelligence activities of such agencies and to per-  
23 form independent, alternative analyses;

24 “(3) disseminate cyber threat analysis to the  
25 President, the appropriate departments and agencies

1 of the Federal Government, and the appropriate  
2 committees of Congress;

3 “(4) coordinate cyber threat intelligence activi-  
4 ties of the departments and agencies of the Federal  
5 Government; and

6 “(5) conduct strategic cyber threat intelligence  
7 planning for the Federal Government.

8 “(d) LIMITATIONS.—The Cyber Threat Intelligence  
9 Integration Center shall—

10 “(1) have not more than 50 permanent posi-  
11 tions;

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

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

21 (4) TABLE OF CONTENTS AMENDMENTS.—The  
22 table of contents in the first section of the National  
23 Security Act of 1947, as amended by section 2 of  
24 this Act, is further amended by striking the item re-

1       lating to section 119B and inserting the following  
2       new items:

“Sec. 119B. Cyber Threat Intelligence Integration Center.  
“Sec. 119C. National intelligence centers.”.

3       (d) INFORMATION SHARED WITH OR PROVIDED TO  
4 THE FEDERAL GOVERNMENT.—

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

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

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

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

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

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

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

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

1 to the Federal Government under this Act may  
2 be disclosed to, retained by, and used by, con-  
3 sistent with otherwise applicable provisions of  
4 Federal law, any department, agency, compo-  
5 nent, officer, employee, or agent of the Federal  
6 Government solely for—

7 (i) a cybersecurity purpose;

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

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

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

22 (B) PROHIBITED ACTIVITIES.—A cyber  
23 threat indicator or defensive measure provided  
24 to the Federal Government under this Act shall  
25 not be disclosed to, retained by, or used by any



1 Federal department or agency for any use not  
2 permitted under subparagraph (A).

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

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

15 (ii) the privacy and civil liberties  
16 guidelines required by subsection (b).

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

19 (a) IN GENERAL.—If a department or agency of the  
20 Federal Government intentionally or willfully violates the  
21 privacy and civil liberties guidelines issued by the Attorney  
22 General under section 4(b), the United States shall be lia-  
23 ble to a person injured by such violation in an amount  
24 equal to the sum of—

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

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

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

9           (1) the district in which the complainant re-  
10          sides;

11          (2) the district in which the principal place of  
12          business of the complainant is located;

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

16          (4) the District of Columbia.

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

22          (d) EXCLUSIVE CAUSE OF ACTION.—A cause of ac-  
23          tion under this subsection shall be the exclusive means  
24          available to a complainant seeking a remedy for a violation

1 by a department or agency of the Federal Government  
2 under this Act.

3 **SEC. 6. PROTECTION FROM LIABILITY.**

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

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

20 (c) WILLFUL MISCONDUCT.—

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

23 (A) to require dismissal of a cause of ac-  
24 tion against a non-Federal entity (including a  
25 private entity) that has engaged in willful mis-

1           conduct in the course of conducting activities  
2           authorized by this Act or the amendments made  
3           by this Act; or

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

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

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

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

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

22                 (C) in disregard of a known or obvious risk  
23                 that is so great as to make it highly probable  
24                 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 cyber-  
16      security threats, including cyber attacks, theft, and data  
17      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 cyberse-

1 security threats (including cyber attacks, theft, and  
2 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 activity 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 (l) 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 “cy-  
19 bersecurity 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 cyberse-  
24                curity 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 cy-  
16 bersecurity 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, pro-  
24 cessed by, or transiting an information system that

1 prevents or mitigates a known or suspected cyberse-  
2 curity 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 cy-  
7           bersecurity 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).

○