

## **[Draft Reported Bill for H.R. 1560]**

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

2 (a) **SHORT TITLE.**—This Act may be cited as the  
3 “Protecting Cyber Networks Act”.

4 (b) **TABLE OF CONTENTS.**—The table of contents of  
5 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.

### **6 SEC. 2. SHARING OF CYBER THREAT INDICATORS AND DE- 7 FENSIVE MEASURES BY THE FEDERAL GOV- 8 ERNMENT WITH NON-FEDERAL ENTITIES.**

9 (a) **IN GENERAL.**—Title I of the National Security  
10 Act of 1947 (50 U.S.C. 3021 et seq.) is amended by in-  
11 serting after section 110 (50 U.S.C. 3045) the following  
12 new section:

1 **“SEC. 111. SHARING OF CYBER THREAT INDICATORS AND**  
2 **DEFENSIVE MEASURES BY THE FEDERAL**  
3 **GOVERNMENT WITH NON-FEDERAL ENTITIES.**

4 “(a) SHARING BY THE FEDERAL GOVERNMENT.—

5 “(1) IN GENERAL.—Consistent with the protec-  
6 tion of classified information, intelligence sources  
7 and methods, and privacy and civil liberties, the Di-  
8 rector of National Intelligence, in consultation with  
9 the heads of the other appropriate Federal entities,  
10 shall develop and promulgate procedures to facilitate  
11 and promote—

12 “(A) the timely sharing of classified cyber  
13 threat indicators in the possession of the Fed-  
14 eral Government with representatives of rel-  
15 evant non-Federal entities with appropriate se-  
16 curity clearances;

17 “(B) the timely sharing with relevant non-  
18 Federal entities of cyber threat indicators or in-  
19 formation in the possession of the Federal Gov-  
20 ernment that may be declassified and shared at  
21 an unclassified level; and

22 “(C) the sharing with non-Federal entities,  
23 if appropriate, of information in the possession  
24 of the Federal Government about imminent or  
25 ongoing cybersecurity threats to such entities to

1           prevent or mitigate adverse impacts from such  
2           cybersecurity threats.

3           “(2) DEVELOPMENT OF PROCEDURES.—The  
4           procedures developed and promulgated under para-  
5           graph (1) shall—

6                   “(A) ensure the Federal Government has  
7                   and maintains the capability to share cyber  
8                   threat indicators in real time consistent with  
9                   the protection of classified information;

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

16                   “(C) include procedures for notifying non-  
17                   Federal entities that have received a cyber  
18                   threat indicator from a Federal entity in ac-  
19                   cordance with this Act that is known or deter-  
20                   mined to be in error or in contravention of the  
21                   requirements of this section, the Protecting  
22                   Cyber Networks Act, or the amendments made  
23                   by such Act or another provision of Federal law  
24                   or policy of such error or contravention;

1           “(D) include requirements for Federal en-  
2           tities receiving a cyber threat indicator or de-  
3           fensive measure to implement appropriate secu-  
4           rity controls to protect against unauthorized ac-  
5           cess to, or acquisition of, such cyber threat in-  
6           dicator or defensive measure;

7           “(E) include procedures that require Fed-  
8           eral entities, prior to the sharing of a cyber  
9           threat indicator, to—

10           “(i) review such cyber threat indicator  
11           to assess whether such cyber threat indi-  
12           cator, in contravention of the requirement  
13           under section 3(d)(2) of the Protecting  
14           Cyber Networks Act, contains any infor-  
15           mation that such Federal entity knows at  
16           the time of sharing to be personal informa-  
17           tion of, or information identifying, a spe-  
18           cific person not directly related to a  
19           cybersecurity threat and remove such in-  
20           formation; or

21           “(ii) implement a technical capability  
22           configured to remove or exclude any per-  
23           sonal information of, or information identi-  
24           fying, a specific person not directly related  
25           to a cybersecurity threat; and

1                   “(F) include procedures to promote the ef-  
2                   ficient granting of security clearances to appro-  
3                   priate representatives of non-Federal entities.

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

9                   (b) SUBMITTAL TO CONGRESS.—Not later than 90  
10                  days after the date of the enactment of this Act, the Direc-  
11                  tor of National Intelligence, in consultation with the heads  
12                  of the other appropriate Federal entities, shall submit to  
13                  Congress the procedures required by section 111(a) of the  
14                  National Security Act of 1947, as inserted by subsection  
15                  (a) of this section.

16                  (c) TABLE OF CONTENTS AMENDMENT.—The table  
17                  of contents in the first section of the National Security  
18                  Act of 1947 is amended by inserting after the item relat-  
19                  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.”.

20   **SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
21                               **ANALYZING,                   AND                   MITIGATING**  
22                               **CYBERSECURITY THREATS.**

23                  (a) AUTHORIZATION FOR PRIVATE-SECTOR DEFEN-  
24                  SIVE MONITORING.—

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

4           (A) an information system of such private  
5 entity;

6           (B) an information system of a non-Fed-  
7 eral entity or a Federal entity, upon the written  
8 authorization of such non-Federal entity or  
9 such Federal entity; and

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

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

16           (A) authorize the monitoring of an infor-  
17 mation system, or the use of any information  
18 obtained through such monitoring, other than  
19 as provided in this Act;

20           (B) authorize the Federal Government to  
21 conduct surveillance of any person; or

22           (C) limit otherwise lawful activity.

23           (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE  
24 MEASURES.—

1           (1) IN GENERAL.—Except as provided in para-  
2           graph (2) and notwithstanding any other provision  
3           of law, a private entity may, for a cybersecurity pur-  
4           pose, operate a defensive measure that is operated  
5           on and the effects of which are limited to—

6                   (A) an information system of such private  
7                   entity to protect the rights or property of the  
8                   private entity; and

9                   (B) an information system of a non-Fed-  
10                  eral entity or a Federal entity upon written au-  
11                  thorization of such non-Federal entity or such  
12                  Federal entity for operation of such defensive  
13                  measure to protect the rights or property of  
14                  such private entity, such non-Federal entity, or  
15                  such Federal entity.

16           (2) LIMITATION.—The authority provided in  
17           paragraph (1) does not include the intentional or  
18           reckless operation of any defensive measure that de-  
19           stroys, renders unusable or inaccessible (in whole or  
20           in part), substantially harms, or initiates a new ac-  
21           tion, process, or procedure on an information system  
22           or information stored on, processed by, or transiting  
23           such information system not owned by—

24                   (A) the private entity operating such de-  
25                   fensive measure; or

1 (B) a non-Federal entity or a Federal enti-  
2 ty that has provided written authorization to  
3 that private entity for operation of such defen-  
4 sive measure in accordance with this subsection.

5 (3) CONSTRUCTION.—Nothing in this sub-  
6 section shall be construed—

7 (A) to authorize the use of a defensive  
8 measure other than as provided in this sub-  
9 section; or

10 (B) to limit otherwise lawful activity.

11 (c) AUTHORIZATION FOR SHARING OR RECEIVING  
12 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-  
13 URES.—

14 (1) IN GENERAL.—Except as provided in para-  
15 graph (2) and notwithstanding any other provision  
16 of law, a non-Federal entity may, for a cybersecurity  
17 purpose and consistent with the requirement under  
18 subsection (d)(2) to remove personal information of,  
19 or information identifying, a specific person not di-  
20 rectly related to a cybersecurity threat and the pro-  
21 tection of classified information—

22 (A) share a cyber threat indicator or de-  
23 fensive measure with any other non-Federal en-  
24 tity or an appropriate Federal entity (other  
25 than the Department of Defense or any compo-



1           ment of the Department, including the National  
2           Security Agency); and

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

6           (2) **LAWFUL RESTRICTION.**—A non-Federal en-  
7           tity receiving a cyber threat indicator or defensive  
8           measure from another non-Federal entity or a Fed-  
9           eral entity shall comply with otherwise lawful restric-  
10          tions placed on the sharing or use of such cyber  
11          threat indicator or defensive measure by the sharing  
12          non-Federal entity or Federal entity.

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

15                   (A) authorize the sharing or receiving of a  
16          cyber threat indicator or defensive measure  
17          other than as provided in this subsection;

18                   (B) authorize the sharing or receiving of  
19          classified information by or with any person not  
20          authorized to access such classified information;

21                   (C) prohibit any Federal entity from en-  
22          gaging in formal or informal technical discus-  
23          sion regarding cyber threat indicators or defen-  
24          sive measures with a non-Federal entity or from  
25          providing technical assistance to address

1 vulnerabilities or mitigate threats at the request  
2 of such an entity;

3 (D) limit otherwise lawful activity;

4 (E) prohibit a non-Federal entity, if au-  
5 thorized by applicable law or regulation other  
6 than this Act, from sharing a cyber threat indi-  
7 cator or defensive measure with the Depart-  
8 ment of Defense or any component of the De-  
9 partment, including the National Security  
10 Agency; or

11 (F) authorize the Federal Government to  
12 conduct surveillance of any person.

13 (d) PROTECTION AND USE OF INFORMATION.—

14 (1) SECURITY OF INFORMATION.—A non-Fed-  
15 eral entity monitoring an information system, oper-  
16 ating a defensive measure, or providing or receiving  
17 a cyber threat indicator or defensive measure under  
18 this section shall implement an appropriate security  
19 control to protect against unauthorized access to, or  
20 acquisition of, such cyber threat indicator or defen-  
21 sive measure.

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

1 (A) review such cyber threat indicator to  
2 assess whether such cyber threat indicator con-  
3 tains any information that the non-Federal en-  
4 tity reasonably believes at the time of sharing  
5 to be personal information of, or information  
6 identifying, a specific person not directly related  
7 to a cybersecurity threat and remove such infor-  
8 mation; or

9 (B) implement a technical capability con-  
10 figured to remove any information contained  
11 within such indicator that the non-Federal enti-  
12 ty reasonably believes at the time of sharing to  
13 be personal information of, or information iden-  
14 tifying, a specific person not directly related to  
15 a cybersecurity threat.

16 (3) USE OF CYBER THREAT INDICATORS AND  
17 DEFENSIVE MEASURES BY NON-FEDERAL ENTI-  
18 TIES.—A non-Federal entity may, for a  
19 cybersecurity purpose—

20 (A) use a cyber threat indicator or defen-  
21 sive measure shared or received under this sec-  
22 tion to monitor or operate a defensive measure  
23 on—

24 (i) an information system of such non-  
25 Federal entity; or

1 (ii) an information system of another  
2 non-Federal entity or a Federal entity  
3 upon the written authorization of that  
4 other non-Federal entity or that Federal  
5 entity; and

6 (B) otherwise use, retain, and further  
7 share such cyber threat indicator or defensive  
8 measure subject to—

9 (i) an otherwise lawful restriction  
10 placed by the sharing non-Federal entity  
11 or Federal entity on such cyber threat in-  
12 dicator or defensive measure; or

13 (ii) an otherwise applicable provision  
14 of law.

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

17 (A) LAW ENFORCEMENT USE.—A State,  
18 tribal, or local government may use a cyber  
19 threat indicator shared with such State, tribal,  
20 or local government for the purposes described  
21 in clauses (i), (ii), and (iii) of section  
22 4(d)(5)(A).

23 (B) EXEMPTION FROM DISCLOSURE.—A  
24 cyber threat indicator shared with a State, trib-

1 al, or local government under this section shall  
2 be—

3 (i) deemed voluntarily shared informa-  
4 tion; and

5 (ii) exempt from disclosure under any  
6 State, tribal, or local law requiring disclo-  
7 sure of information or records, except as  
8 otherwise required by applicable State,  
9 tribal, or local law requiring disclosure in  
10 any criminal prosecution.

11 (e) NO RIGHT OR BENEFIT.—The sharing of a cyber  
12 threat indicator with a non-Federal entity under this Act  
13 shall not create a right or benefit to similar information  
14 by such non-Federal entity or any other non-Federal enti-  
15 ty.

16 **SEC. 4. SHARING OF CYBER THREAT INDICATORS AND DE-**  
17 **FENSIVE MEASURES WITH APPROPRIATE**  
18 **FEDERAL ENTITIES OTHER THAN THE DE-**  
19 **PARTMENT OF DEFENSE OR THE NATIONAL**  
20 **SECURITY AGENCY.**

21 (a) REQUIREMENT FOR POLICIES AND PROCE-  
22 DURES.—

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

1 (A) redesignating subsection (b) as sub-  
2 section (c); and

3 (B) by inserting after subsection (a) the  
4 following new subsection:

5 “(b) POLICIES AND PROCEDURES FOR SHARING  
6 WITH THE APPROPRIATE FEDERAL ENTITIES OTHER  
7 THAN THE DEPARTMENT OF DEFENSE OR THE NA-  
8 TIONAL SECURITY AGENCY.—

9 “(1) ESTABLISHMENT.—The President shall  
10 develop and submit to Congress policies and proce-  
11 dures relating to the receipt of cyber threat indica-  
12 tors and defensive measures by the Federal Govern-  
13 ment.

14 “(2) REQUIREMENTS CONCERNING POLICIES  
15 AND PROCEDURES.—The policies and procedures re-  
16 quired under paragraph (1) shall—

17 “(A) be developed in accordance with the  
18 privacy and civil liberties guidelines required  
19 under section 4(b) of the Protecting Cyber Net-  
20 works Act;

21 “(B) ensure that—

22 “(i) a cyber threat indicator shared by  
23 a non-Federal entity with an appropriate  
24 Federal entity (other than the Department  
25 of Defense or any component of the De-

1           department, including the National Security  
2           Agency) pursuant to section 3 of such Act  
3           is shared in real-time with all of the appro-  
4           priate Federal entities (including all rel-  
5           evant components thereof);

6           “(ii) the sharing of such cyber threat  
7           indicator with appropriate Federal entities  
8           is not subject to any delay, modification, or  
9           any other action without good cause that  
10          could impede receipt by all of the appro-  
11          priate Federal entities; and

12          “(iii) such cyber threat indicator is  
13          provided to each other Federal entity to  
14          which such cyber threat indicator is rel-  
15          evant; and

16          “(C) ensure there—

17                  “(i) is an audit capability; and

18                  “(ii) are appropriate sanctions in  
19                  place for officers, employees, or agents of  
20                  a Federal entity who knowingly and will-  
21                  fully use a cyber threat indicator or de-  
22                  fense measure shared with the Federal  
23                  Government by a non-Federal entity under  
24                  the Protecting Cyber Networks Act other

1           than in accordance with this section and  
2           such Act.”.

3           (2) SUBMISSION.—The President shall submit  
4           to Congress—

5                   (A) not later than 90 days after the date  
6                   of the enactment of this Act, interim policies  
7                   and procedures required under section  
8                   111(b)(1) of the National Security Act of 1947,  
9                   as inserted by paragraph (1) of this section;  
10                  and

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

14           (b) PRIVACY AND CIVIL LIBERTIES.—

15                   (1) GUIDELINES OF ATTORNEY GENERAL.—The  
16                   Attorney General, in consultation with the heads of  
17                   the other appropriate Federal agencies and with offi-  
18                   cers designated under section 1062 of the Intel-  
19                   ligence Reform and Terrorism Prevention Act of  
20                   2004 (42 U.S.C. 2000ee–1), shall develop and peri-  
21                   odically review guidelines relating to privacy and  
22                   civil liberties that govern the receipt, retention, use,  
23                   and dissemination of cyber threat indicators by a  
24                   Federal entity obtained in accordance with this Act  
25                   and the amendments made by this Act.



1           (2) CONTENT.—The guidelines developed and  
2 reviewed under paragraph (1) shall, consistent with  
3 the need to protect information systems from  
4 cybersecurity threats and mitigate cybersecurity  
5 threats—

6           (A) limit the impact on privacy and civil  
7 liberties of activities by the Federal Government  
8 under this Act, including guidelines to ensure  
9 that personal information of, or information  
10 identifying, specific persons is properly removed  
11 from information received, retained, used, or  
12 disseminated by a Federal entity in accordance  
13 with this Act or the amendments made by this  
14 Act;

15           (B) limit the receipt, retention, use, and  
16 dissemination of cyber threat indicators con-  
17 taining personal information of, or information  
18 identifying, specific persons, including by estab-  
19 lishing—

20           (i) a process for the prompt destruc-  
21 tion of such information that is known not  
22 to be directly related to a use for a  
23 cybersecurity purpose;

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

4 (iii) a process to inform recipients  
5 that such indicators may only be used for  
6 a cybersecurity purpose;

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

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

20 (E) be consistent with any other applicable  
21 provisions of law and the fair information prac-  
22 tice principles set forth in appendix A of the  
23 document entitled “National Strategy for  
24 Trusted Identities in Cyberspace” and pub-  
25 lished by the President in April, 2011; and

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

6 (3) SUBMISSION.—The Attorney General shall  
7 submit to Congress—

8 (A) not later than 90 days after the date  
9 of the enactment of this Act, interim guidelines  
10 required under paragraph (1); and

11 (B) not later than 180 days after such  
12 date, final guidelines required under such para-  
13 graph.

14 (c) NATIONAL CYBER THREAT INTELLIGENCE INTE-  
15 GRATION CENTER.—

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

20 (A) by redesignating section 119B as sec-  
21 tion 119C; and

22 (B) by inserting after section 119A the fol-  
23 lowing new section:

1 **“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION**  
2 **CENTER.**

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

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

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

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

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

22 “(3) disseminate cyber threat analysis to the  
23 President, the appropriate departments and agencies  
24 of the Federal Government, and the appropriate  
25 committees of Congress;

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

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

6           “(d) LIMITATIONS.—The Cyber Threat Intelligence  
7 Integration Center shall—

8           “(1) have not more than 50 permanent posi-  
9 tions;

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

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

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

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

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

1 (d) INFORMATION SHARED WITH OR PROVIDED TO  
2 THE FEDERAL GOVERNMENT.—

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

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

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

24 (A) deemed voluntarily shared information  
25 and exempt from disclosure under section 552

1 of title 5, United States Code, and any State,  
2 tribal, or local law requiring disclosure of infor-  
3 mation or records; and

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

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

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

19 (A) AUTHORIZED ACTIVITIES.—A cyber  
20 threat indicator or defensive measure provided  
21 to the Federal Government under this Act may  
22 be disclosed to, retained by, and used by, con-  
23 sistent with otherwise applicable provisions of  
24 Federal law, any department, agency, compo-

1           nent, officer, employee, or agent of the Federal  
2           Government solely for—

3                   (i) a cybersecurity purpose;

4                   (ii) the purpose of responding to,  
5                   prosecuting, or otherwise preventing or  
6                   mitigating a threat of death or serious  
7                   bodily harm or an offense arising out of  
8                   such a threat;

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

13                   (iv) the purpose of preventing, inves-  
14                   tigating, disrupting, or prosecuting any of  
15                   the offenses listed in sections 1028, 1029,  
16                   1030, and 3559(c)(2)(F) and chapters 37  
17                   and 90 of title 18, United States Code.

18           (B) PROHIBITED ACTIVITIES.—A cyber  
19           threat indicator or defensive measure provided  
20           to the Federal Government under this Act shall  
21           not be disclosed to, retained by, or used by any  
22           Federal department or agency for any use not  
23           permitted under subparagraph (A).

24           (C) PRIVACY AND CIVIL LIBERTIES.—A  
25           cyber threat indicator or defensive measure pro-



1 vided to the Federal Government under this Act  
2 shall be retained, used, and disseminated by the  
3 Federal Government in accordance with—

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

11 (ii) the privacy and civil liberties  
12 guidelines required by subsection (b).

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

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

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

24 (2) reasonable attorney fees as determined by  
25 the court and other litigation costs reasonably in-

1 curred in any case under this subsection in which  
2 the complainant has substantially prevailed.

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

6 (1) the district in which the complainant re-  
7 sides;

8 (2) the district in which the principal place of  
9 business of the complainant is located;

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

13 (4) the District of Columbia.

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

19 (d) EXCLUSIVE CAUSE OF ACTION.—A cause of ac-  
20 tion under this subsection shall be the exclusive means  
21 available to a complainant seeking a remedy for a violation  
22 by a department or agency of the Federal Government  
23 under this Act.

1 **SEC. 6. PROTECTION FROM LIABILITY.**

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

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

18 (c) WILLFUL MISCONDUCT.—

19 (1) RULE OF CONSTRUCTION.—Nothing in this  
20 section shall be construed—

21 (A) to require dismissal of a cause of ac-  
22 tion against a non-Federal entity (including a  
23 private entity) that has engaged in willful mis-  
24 conduct in the course of conducting activities  
25 authorized by this Act or the amendments made  
26 by this Act; or

1 (B) to undermine or limit the availability  
2 of otherwise applicable common law or statu-  
3 tory defenses.

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

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

15 (A) intentionally to achieve a wrongful  
16 purpose;

17 (B) knowingly without legal or factual jus-  
18 tification; and

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

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

23 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

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

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

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

10       “(c) BIENNIAL REPORT ON IMPLEMENTATION.—

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

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

19           “(A) An assessment of the sufficiency of  
20 the policies, procedures, and guidelines required  
21 by this section and section 4 of the Protecting  
22 Cyber Networks Act in ensuring that cyber  
23 threat indicators are shared effectively and re-  
24 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                 “ (i) an assessment of all reports of  
13                 officers, employees, and agents of the Fed-  
14                 eral Government misusing information pro-  
15                 vided to the Federal Government under the  
16                 Protecting Cyber Networks Act or this sec-  
17                 tion, without regard to whether the misuse  
18                 was knowing or wilful; and

19                 “(ii) an assessment of all disciplinary  
20                 actions taken against such officers, em-  
21                 ployees, and agents.

22           “(G) A summary of the number and type  
23           of non-Federal entities that received classified  
24           cyber threat indicators from the Federal Gov-  
25           ernment under this section or such Act and an

1 evaluation of the risks and benefits of sharing  
2 such cyber threat indicators.

3 “(H) An assessment of any personal infor-  
4 mation of, or information identifying, a specific  
5 person not directly related to a cybersecurity  
6 threat that—

7 “(i) was shared by a non-Federal enti-  
8 ty with the Federal Government under this  
9 Act in contravention of section 3(d)(2); or

10 “(ii) was shared within the Federal  
11 Government under this Act in contraven-  
12 tion of the guidelines required by section  
13 4(b).

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

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

23 “(5) PUBLIC AVAILABILITY OF REPORTS.—The  
24 Director of National Intelligence shall make publicly



1 available the unclassified portion of each report re-  
2 quired by paragraph (1).”.

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

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

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

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

16 “(3) BIENNIAL REPORT ON CERTAIN CYBER AC-  
17 TIVITIES.—

18 “(A) REPORT REQUIRED.—The Privacy  
19 and Civil Liberties Oversight Board shall bien-  
20 nially submit to Congress and the President a  
21 report containing—

22 “(i) an assessment of the privacy and  
23 civil liberties impact of the activities car-  
24 ried out under the Protecting Cyber Net-

1 works Act and the amendments made by  
2 such Act; and

3 “(ii) an assessment of the sufficiency  
4 of the policies, procedures, and guidelines  
5 established pursuant to section 4 of the  
6 Protecting Cyber Networks Act and the  
7 amendments made by such section 4 in ad-  
8 dressing privacy and civil liberties con-  
9 cerns.

10 “(B) RECOMMENDATIONS.—Each report  
11 submitted under this paragraph may include  
12 such recommendations as the Privacy and Civil  
13 Liberties Oversight Board may have for im-  
14 provements or modifications to the authorities  
15 under the Protecting Cyber Networks Act or  
16 the amendments made by such Act.

17 “(C) FORM.—Each report required under  
18 this paragraph shall be submitted in unclassi-  
19 fied form, but may include a classified annex.

20 “(D) PUBLIC AVAILABILITY OF RE-  
21 PORTS.—The Privacy and Civil Liberties Over-  
22 sight Board shall make publicly available the  
23 unclassified portion of each report required by  
24 subparagraph (A).”.

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

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

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

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

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

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

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

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

16 (C) RECOMMENDATIONS.—Each report  
17 submitted under this paragraph may include  
18 such recommendations as the Inspectors Gen-  
19 eral referred to in subparagraph (A) may have  
20 for improvements or modifications to the au-  
21 thorities under this Act or the amendments  
22 made by this Act.

23 (D) FORM.—Each report required under  
24 this paragraph shall be submitted in unclassi-  
25 fied form, but may include a classified annex.

1                   (E) PUBLIC AVAILABILITY OF REPORTS.—  
2           The Inspector General of the Department of  
3           Homeland Security, the Inspector General of  
4           the Intelligence Community, the Inspector Gen-  
5           eral of the Department of Justice, and the In-  
6           specter General of the Department of Defense  
7           shall make publicly available the unclassified  
8           portion of each report required under subpara-  
9           graph (A).

10 **SEC. 8. REPORT ON CYBERSECURITY THREATS.**

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

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

22                   (1) An assessment of—

23                           (A) the current intelligence sharing and co-  
24                           operation relationships of the United States  
25                           with other countries regarding cybersecurity

1 threats (including cyber attacks, theft, and data  
2 breaches) directed against the United States  
3 that threaten the United States national secu-  
4 rity interests, economy, and intellectual prop-  
5 erty; and

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

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

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

1           (4) An assessment of additional technologies or  
2 capabilities that would enhance the ability of the  
3 United States to prevent and to respond to  
4 cybersecurity threats (including cyber attacks, theft,  
5 and data breaches).

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

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

13       (d) PUBLIC AVAILABILITY OF REPORT.—The Direc-  
14 tor of National Intelligence shall make publicly available  
15 the unclassified portion of the report required by sub-  
16 section (a).

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

21 **SEC. 9. CONSTRUCTION AND PREEMPTION.**

22       (a) PROHIBITION OF SURVEILLANCE.—Nothing in  
23 this Act or the amendments made by this Act shall be  
24 construed to authorize the Department of Defense or the

1 National Security Agency or any other element of the in-  
2 telligence community to target a person for surveillance.

3 (b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in  
4 this Act or the amendments made by this Act shall be  
5 construed to limit or prohibit—

6 (1) otherwise lawful disclosures of communica-  
7 tions, records, or other information, including re-  
8 porting of known or suspected criminal activity, by  
9 a non-Federal entity to any other non-Federal entity  
10 or the Federal Government; or

11 (2) any otherwise lawful use of such disclosures  
12 by any entity of the Federal government, without re-  
13 gard to whether such otherwise lawful disclosures  
14 duplicate or replicate disclosures made under this  
15 Act.

16 (c) WHISTLE BLOWER PROTECTIONS.—Nothing in  
17 this Act or the amendments made by this Act shall be  
18 construed to prohibit or limit the disclosure of information  
19 protected under section 2302(b)(8) of title 5, United  
20 States Code (governing disclosures of illegality, waste,  
21 fraud, abuse, or public health or safety threats), section  
22 7211 of title 5, United States Code (governing disclosures  
23 to Congress), section 1034 of title 10, United States Code  
24 (governing disclosure to Congress by members of the mili-  
25 tary), or any similar provision of Federal or State law..



1 (d) PROTECTION OF SOURCES AND METHODS.—  
2 Nothing in this Act or the amendments made by this Act  
3 shall be construed—

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

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

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

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

21 (f) INFORMATION SHARING RELATIONSHIPS.—Noth-  
22 ing in this Act or the amendments made by this Act shall  
23 be construed—

24 (1) to limit or modify an existing information-  
25 sharing relationship;

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

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

6           (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS  
7           AND RIGHTS.—Nothing in this Act or the amendments  
8           made by this Act shall be construed—

9           (1) to amend, repeal, or supersede any current  
10          or future contractual agreement, terms of service  
11          agreement, or other contractual relationship between  
12          any non-Federal entities, or between any non-Fed-  
13          eral entity and a Federal entity; or

14          (2) to abrogate trade secret or intellectual prop-  
15          erty rights of any non-Federal entity or Federal en-  
16          tity.

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

20          (1) to require a non-Federal entity to provide  
21          information to the Federal Government;

22          (2) to condition the sharing of a cyber threat  
23          indicator with a non-Federal entity on such non-  
24          Federal entity's provision of a cyber threat indicator  
25          to the Federal Government; or

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

4           (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-  
5           ing in this Act or the amendments made by this Act shall  
6           be construed to subject any non-Federal entity to liability  
7           for choosing not to engage in a voluntary activiy author-  
8           ized in this Act and the amendments made by this Act.

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

17           (k) FEDERAL PREEMPTION.—

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

24           (2) STATE LAW ENFORCEMENT.—Nothing in  
25           this Act or the amendments made by this Act shall

1 be construed to supersede any statute or other provi-  
2 sion of law of a State or political subdivision of a  
3 State concerning the use of authorized law enforce-  
4 ment practices and procedures.

5 (l) REGULATORY AUTHORITY.—Nothing in this Act  
6 or the amendments made by this Act shall be construed—

7 (1) to authorize the promulgation of any regu-  
8 lations not specifically authorized by this Act or the  
9 amendments made by this Act;

10 (2) to establish any regulatory authority not  
11 specifically established under this Act or the amend-  
12 ments made by this Act; or

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

17 **SEC. 10. CONFORMING AMENDMENTS.**

18 Section 552(b) of title 5, United States Code, is  
19 amended—

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

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

24 (3) by inserting after paragraph (9) the fol-  
25 lowing:

1           “(10) information shared with or provided to  
2           the Federal Government pursuant to the Protecting  
3           Cyber Networks Act or the amendments made by  
4           such Act.”.

5 **SEC. 11. DEFINITIONS.**

6           In this Act:

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

10          (2) **APPROPRIATE FEDERAL ENTITIES.**—The  
11          term “appropriate Federal entities” means the fol-  
12          lowing:

13                   (A) The Department of Commerce.

14                   (B) The Department of Defense.

15                   (C) The Department of Energy.

16                   (D) The Department of Homeland Secu-  
17                   rity.

18                   (E) The Department of Justice.

19                   (F) The Department of the Treasury.

20                   (G) The Office of the Director of National  
21                   Intelligence.

22          (3) **CYBERSECURITY PURPOSE.**—The term  
23          “cybersecurity purpose” means the purpose of pro-  
24          tecting (including through the use of a defensive  
25          measure) an information system or information that

1 is stored on, processed by, or transiting an informa-  
2 tion system from a cybersecurity threat or security  
3 vulnerability or identifying the source of a  
4 cybersecurity threat.

5 (4) CYBERSECURITY THREAT.—

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

17 (B) EXCLUSION.—The term “cybersecurity  
18 threat” does not include any action that solely  
19 involves a violation of a consumer term of serv-  
20 ice or a consumer licensing agreement.

21 (5) CYBER THREAT INDICATOR.—The term  
22 “cyber threat indicator” means information or a  
23 physical object that is necessary to describe or iden-  
24 tify—

1 (A) malicious reconnaissance, including  
2 anomalous patterns of communications that ap-  
3 pear to be transmitted for the purpose of gath-  
4 ering technical information related to a  
5 cybersecurity threat or security vulnerability;

6 (B) a method of defeating a security con-  
7 trol or exploitation of a security vulnerability;

8 (C) a security vulnerability, including  
9 anomalous activity that appears to indicate the  
10 existence of a security vulnerability;

11 (D) a method of causing a user with legiti-  
12 mate access to an information system or infor-  
13 mation that is stored on, processed by, or  
14 transiting an information system to unwittingly  
15 enable the defeat of a security control or exploi-  
16 tation of a security vulnerability;

17 (E) malicious cyber command and control;

18 (F) the actual or potential harm caused by  
19 an incident, including a description of the infor-  
20 mation exfiltrated as a result of a particular  
21 cybersecurity threat; or

22 (G) any other attribute of a cybersecurity  
23 threat, if disclosure of such attribute is not oth-  
24 erwise prohibited by law.

1           (6) DEFENSIVE MEASURE.—The term “defen-  
2           sive measure” means an action, device, procedure,  
3           technique, or other measure executed on an informa-  
4           tion system or information that is stored on, proc-  
5           essed by, or transiting an information system that  
6           prevents or mitigates a known or suspected  
7           cybersecurity threat or security vulnerability.

8           (7) FEDERAL ENTITY.—The term “Federal en-  
9           tity” means a department or agency of the United  
10          States or any component of such department or  
11          agency.

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

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

16                (B) includes industrial control systems,  
17                such as supervisory control and data acquisition  
18                systems, distributed control systems, and pro-  
19                grammable logic controllers.

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

24          (10) MALICIOUS CYBER COMMAND AND CON-  
25          TROL.—The term “malicious cyber command and



1 control” means a method for unauthorized remote  
2 identification of, access to, or use of, an information  
3 system or information that is stored on, processed  
4 by, or transiting an information system.

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

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

16 (13) NON-FEDERAL ENTITY.—

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

24 (B) INCLUSIONS.—The term “non-Federal  
25 entity” includes a government department or

1 agency (including an officer, employee, or agent  
2 thereof) of the District of Columbia, the Com-  
3 monwealth of Puerto Rico, the Virgin Islands,  
4 Guam, American Samoa, the Northern Mariana  
5 Islands, and any other territory or possession of  
6 the United States.

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

11 (14) PRIVATE ENTITY.—

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

19 (B) INCLUSION.—The term “private enti-  
20 ty” includes a component of a State, tribal, or  
21 local government performing electric utility  
22 services.

23 (C) EXCLUSION.—The term “private enti-  
24 ty” does not include a foreign power as defined

1           in section 101 of the Foreign Intelligence Sur-  
2           veillance Act of 1978 (50 U.S.C. 1801).

3           (15) REAL TIME; REAL-TIME.—The terms “real  
4           time” and “real-time” mean a process by which an  
5           automated, machine-to-machine system processes  
6           cyber threat indicators such that the time in which  
7           the occurrence of an event and the reporting or re-  
8           cording of it are as simultaneous as technologically  
9           and operationally practicable.

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

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

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