

114TH CONGRESS  
2D SESSION

# H. R. 1560

---

IN THE SENATE OF THE UNITED STATES

APRIL 27, 2015

Received

JULY 14, 2016

Read twice and referred to the Committee on Homeland Security and  
Governmental Affairs

---

## AN ACT

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, 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. TABLE OF CONTENTS.**

4 The table of contents of this Act is as follows:

Sec. 1. Table of Contents.

TITLE I—PROTECTING CYBER NETWORKS ACT

Sec. 101. Short title.

Sec. 102. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.

Sec. 103. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

Sec. 104. Sharing of cyber threat indicators and defensive measures with appropriate Federal entities other than the Department of Defense or the National Security Agency.

Sec. 105. Federal Government liability for violations of privacy or civil liberties.

Sec. 106. Protection from liability.

Sec. 107. Oversight of Government activities.

Sec. 108. Report on cybersecurity threats.

Sec. 109. Construction and preemption.

Sec. 110. Definitions.

Sec. 111. Comptroller General report on removal of personal identifying information.

Sec. 112. Sunset.

TITLE II—NATIONAL CYBERSECURITY PROTECTION  
 ADVANCEMENT ACT

Sec. 201. Short title.

Sec. 202. National Cybersecurity and Communications Integration Center.

Sec. 203. Information sharing structure and processes.

Sec. 204. Information sharing and analysis organizations.

Sec. 205. Streamlining of Department of Homeland Security cybersecurity and infrastructure protection organization.

Sec. 206. Cyber incident response plans.

Sec. 207. Security and resiliency of public safety communications; Cybersecurity awareness campaign.

Sec. 208. Critical infrastructure protection research and development.

Sec. 209. Report on reducing cybersecurity risks in DHS data centers.

Sec. 210. Assessment.

Sec. 211. Consultation.

Sec. 212. Technical assistance.

Sec. 213. Prohibition on new regulatory authority.

Sec. 214. Sunset.

Sec. 215. Prohibition on new funding.

Sec. 216. Protection of Federal information systems.

Sec. 217. Sunset.

Sec. 218. Report on cybersecurity vulnerabilities of United States ports.

Sec. 219. Report on cybersecurity and critical infrastructure.

Sec. 220. GAO report on impact privacy and civil liberties.

1     **TITLE I—PROTECTING CYBER**  
2                     **NETWORKS ACT**

3     **SEC. 101. SHORT TITLE.**

4             This title may be cited as the “Protecting Cyber Net-  
5 works Act”.

6     **SEC. 102. SHARING OF CYBER THREAT INDICATORS AND**  
7                     **DEFENSIVE MEASURES BY THE FEDERAL**  
8                     **GOVERNMENT 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:

13     **“SEC. 111. SHARING OF CYBER THREAT INDICATORS AND**  
14                     **DEFENSIVE MEASURES BY THE FEDERAL**  
15                     **GOVERNMENT WITH NON-FEDERAL ENTITIES.**

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

17                     “(1) IN GENERAL.—Consistent with the protec-  
18 tion of classified information, intelligence sources  
19 and methods, and privacy and civil liberties, the Di-  
20 rector of National Intelligence, in consultation with  
21 the heads of the other appropriate Federal entities,  
22 shall develop and promulgate procedures to facilitate  
23 and promote—

24                             “(A) the timely sharing of classified cyber  
25 threat indicators in the possession of the Fed-

1           eral Government with representatives of rel-  
2           evant non-Federal entities with appropriate se-  
3           curity clearances;

4           “(B) the timely sharing with relevant non-  
5           Federal entities of cyber threat indicators in the  
6           possession of the Federal Government that may  
7           be declassified and shared at an unclassified  
8           level; and

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

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

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

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

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

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

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

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

21 “(i) review such cyber threat indicator  
22 to assess whether such cyber threat indi-  
23 cator, in contravention of the requirement  
24 under section 3(d)(2) of the Protecting  
25 Cyber Networks Act, contains any infor-

1           mation that such Federal entity knows at  
2           the time of sharing to be personal informa-  
3           tion of or information identifying a specific  
4           person not directly related to a cybersecu-  
5           rity threat and remove such information;  
6           or

7           “(ii) implement a technical capability  
8           configured to remove or exclude any per-  
9           sonal information of or information identi-  
10          fying a specific person not directly related  
11          to a cybersecurity threat; and

12          “(F) include procedures to promote the ef-  
13          ficient granting of security clearances to appro-  
14          priate representatives of non-Federal entities.

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

20          (b) SUBMITTAL TO CONGRESS.—Not later than 90  
21          days after the date of the enactment of this title, the Di-  
22          rector of National Intelligence, in consultation with the  
23          heads of the other appropriate Federal entities, shall sub-  
24          mit to Congress the procedures required by section 111(a)

1 of the National Security Act of 1947, as inserted by sub-  
2 section (a) of this section.

3 (c) TABLE OF CONTENTS AMENDMENT.—The table  
4 of contents in the first section of the National Security  
5 Act of 1947 is amended by inserting after the item relat-  
6 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.”.

7 **SEC. 103. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
8 **ANALYZING, AND MITIGATING CYBERSECU-**  
9 **RITY THREATS.**

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

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

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

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

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

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

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

7           (B) authorize the Federal Government to  
8 conduct surveillance of any person; or

9           (C) limit otherwise lawful activity.

10       (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE  
11 MEASURES.—

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

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

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



1           such private entity, such non-Federal entity, or  
2           such Federal entity.

3           (2) LIMITATION.—The authority provided in  
4           paragraph (1) does not include a defensive measure  
5           that destroys, renders unusable or inaccessible (in  
6           whole or in part), or substantially harms an infor-  
7           mation system or information stored on, processed  
8           by, or transiting such information system not owned  
9           by—

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 on the information system or in-  
16                   formation of the entity in accordance with this  
17                   subsection.

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

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

23                   (B) to limit otherwise lawful activity.

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

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

12 (A) share a lawfully obtained cyber threat  
13 indicator or defensive measure with any other  
14 non-Federal entity or an appropriate Federal  
15 entity (other than the Department of Defense  
16 or any component of the Department, including  
17 the National Security Agency); and

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

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

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

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

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

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

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

18 (D) limit otherwise lawful activity;

19 (E) prohibit otherwise lawful sharing by a  
20 non-Federal entity of a cyber threat indicator  
21 or defensive measure with the Department of  
22 Defense or any component of the Department,  
23 including the National Security Agency; or

24 (F) authorize the Federal Government to  
25 conduct surveillance of any person.

1 (d) PROTECTION AND USE OF INFORMATION.—

2 (1) SECURITY OF INFORMATION.—A non-Fed-  
3 eral entity monitoring an information system, oper-  
4 ating a defensive measure, or providing or receiving  
5 a cyber threat indicator or defensive measure under  
6 this section shall implement an appropriate security  
7 control to protect against unauthorized access to, or  
8 acquisition of, such cyber threat indicator or defen-  
9 sive measure.

10 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-  
11 TION.—A non-Federal entity sharing a cyber threat  
12 indicator pursuant to this title shall, prior to such  
13 sharing, take reasonable efforts to—

14 (A) review such cyber threat indicator to  
15 assess whether such cyber threat indicator con-  
16 tains any information that the non-Federal en-  
17 tity reasonably believes at the time of sharing  
18 to be personal information of or information  
19 identifying a specific person not directly related  
20 to a cybersecurity threat and remove such infor-  
21 mation; or

22 (B) implement a technical capability con-  
23 figured to remove any information contained  
24 within such indicator that the non-Federal enti-  
25 ty reasonably believes at the time of sharing to

1 be personal information of or information iden-  
2 tifying a specific person not directly related to  
3 a cybersecurity threat.

4 (3) USE OF CYBER THREAT INDICATORS AND  
5 DEFENSIVE MEASURES BY NON-FEDERAL ENTI-  
6 TIES.—A non-Federal entity may, for a cybersecu-  
7 rity purpose—

8 (A) use a cyber threat indicator or defen-  
9 sive measure shared or received under this sec-  
10 tion to monitor or operate a defensive measure  
11 on—

12 (i) an information system of such non-  
13 Federal entity; or

14 (ii) an information system of another  
15 non-Federal entity or a Federal entity  
16 upon the written authorization of that  
17 other non-Federal entity or that Federal  
18 entity; and

19 (B) otherwise use, retain, and further  
20 share such cyber threat indicator or defensive  
21 measure subject to—

22 (i) an otherwise lawful restriction  
23 placed by the sharing non-Federal entity  
24 or Federal entity on such cyber threat in-  
25 dicator or defensive measure; or

1 (ii) an otherwise applicable provision  
2 of law.

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

5 (A) LAW ENFORCEMENT USE.—A State,  
6 tribal, or local government may use a cyber  
7 threat indicator shared with such State, tribal,  
8 or local government for the purposes described  
9 in clauses (i), (ii), and (iii) of section  
10 104(d)(5)(A).

11 (B) EXEMPTION FROM DISCLOSURE.—A  
12 cyber threat indicator or defensive measure  
13 shared with a State, tribal, or local government  
14 under this section shall be—

15 (i) deemed voluntarily shared informa-  
16 tion; and

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

23 (e) NO RIGHT OR BENEFIT.—The sharing of a cyber  
24 threat indicator with a non-Federal entity under this title  
25 shall not create a right or benefit to similar information

1 by such non-Federal entity or any other non-Federal enti-  
2 ty.

3 (f) SMALL BUSINESS PARTICIPATION.—

4 (1) ASSISTANCE.—The Administrator of the  
5 Small Business Administration shall provide assist-  
6 ance to small businesses and small financial institu-  
7 tions to monitor information and information sys-  
8 tems, operate defensive measures, and share and re-  
9 ceive cyber threat indicators and defensive measures  
10 under this section.

11 (2) REPORT.—Not later than 1 year after the  
12 date of the enactment of this title, the Administrator  
13 of the Small Business Administration shall submit  
14 to the President a report on the degree to which  
15 small businesses and small financial institutions are  
16 able to engage in cyber threat information sharing  
17 under this section. Such report shall include the rec-  
18 ommendations of the Administrator for improving  
19 the ability of such businesses and institutions to en-  
20 gage in cyber threat information sharing and to use  
21 shared information to defend their networks.

22 (3) OUTREACH.—The Federal Government  
23 shall conduct outreach to small businesses and small  
24 financial institutions to encourage such businesses

1 and institutions to exercise their authority under  
2 this section.

3 **SEC. 104. SHARING OF CYBER THREAT INDICATORS AND**  
4 **DEFENSIVE MEASURES WITH APPROPRIATE**  
5 **FEDERAL ENTITIES OTHER THAN THE DE-**  
6 **PARTMENT OF DEFENSE OR THE NATIONAL**  
7 **SECURITY AGENCY.**

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

10 (1) IN GENERAL.—Section 111 of the National  
11 Security Act of 1947, as inserted by section 102 of  
12 this title, is amended—

13 (A) by redesignating subsection (b) as sub-  
14 section (c); and

15 (B) by inserting after subsection (a) the  
16 following new subsection:

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

21 “(1) ESTABLISHMENT.—The President shall  
22 develop and submit to Congress policies and proce-  
23 dures relating to the receipt of cyber threat indica-  
24 tors and defensive measures by the Federal Govern-  
25 ment.



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

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

8                   “(B) ensure that—

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

18                           “(ii) the sharing of such cyber threat  
19                           indicator with appropriate Federal entities  
20                           is not subject to any delay, modification, or  
21                           any other action without good cause that  
22                           could impede receipt by all of the appro-  
23                           priate Federal entities; and

24                           “(iii) such cyber threat indicator is  
25                           provided to each other Federal entity to

1           which such cyber threat indicator is rel-  
2           evant; and

3           “(C) ensure there—

4                 “(i) is an audit capability; and

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

14           (2) SUBMISSION.—The President shall submit  
15          to Congress—

16                 (A) not later than 90 days after the date  
17          of the enactment of this title, interim policies  
18          and procedures required under section  
19          111(b)(1) of the National Security Act of 1947,  
20          as inserted by paragraph (1) of this section;  
21          and

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

25          (b) PRIVACY AND CIVIL LIBERTIES.—

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

12           (2) CONTENT.—The guidelines developed and  
13    reviewed under paragraph (1) shall, consistent with  
14    the need to protect information systems from cyber-  
15    security threats and mitigate cybersecurity threats—

16           (A) limit the impact on privacy and civil  
17    liberties of activities by the Federal Government  
18    under this title, including guidelines to ensure  
19    that personal information of or information  
20    identifying specific persons is properly removed  
21    from information received, retained, used, or  
22    disseminated by a Federal entity in accordance  
23    with this title or the amendments made by this  
24    title;

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

6 (i) a process for the prompt destruc-  
7 tion of such information that is known not  
8 to be directly related to a use for a cyber-  
9 security purpose;

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

13 (iii) a process to inform recipients  
14 that such indicators may only be used for  
15 a cybersecurity purpose;

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

23 (D) include procedures for notifying non-  
24 Federal entities and Federal entities if informa-  
25 tion received pursuant to this section is known

1 or determined by a Federal entity receiving  
2 such information not to constitute a cyber  
3 threat indicator;

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

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

15 (3) SUBMISSION.—The Attorney General shall  
16 submit to Congress—

17 (A) not later than 90 days after the date  
18 of the enactment of this title, interim guidelines  
19 required under paragraph (1); and

20 (B) not later than 180 days after such  
21 date, final guidelines required under such para-  
22 graph.

23 (c) NATIONAL CYBER THREAT INTELLIGENCE INTE-  
24 GRATION CENTER.—

1           (1) ESTABLISHMENT.—Title I of the National  
2           Security Act of 1947 (50 U.S.C. 3021 et seq.), as  
3           amended by section 102 of this title, is further  
4           amended—

5                   (A) by redesignating section 119B as sec-  
6                   tion 119C; and

7                   (B) by inserting after section 119A the fol-  
8                   lowing new section:

9           **“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION**  
10                   **CENTER.**

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

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

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

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

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

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

10           “(4) coordinate cyber threat intelligence activi-  
11 ties of the departments and agencies of the Federal  
12 Government; and

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

15           “(d) LIMITATIONS.—The Cyber Threat Intelligence  
16 Integration Center shall—

17           “(1) have not more than 50 permanent posi-  
18 tions;

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

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

4           (2) TABLE OF CONTENTS AMENDMENTS.—The  
5           table of contents in the first section of the National  
6           Security Act of 1947, as amended by section 102 of  
7           this title, is further amended by striking the item re-  
8           lating to section 119B and inserting the following  
9           new items:

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

10          (d) INFORMATION SHARED WITH OR PROVIDED TO  
11          THE FEDERAL GOVERNMENT.—

12           (1) NO WAIVER OF PRIVILEGE OR PROTEC-  
13           TION.—The provision of a cyber threat indicator or  
14           defensive measure to the Federal Government under  
15           this title shall not constitute a waiver of any applica-  
16           ble privilege or protection provided by law, including  
17           trade secret protection.

18           (2) PROPRIETARY INFORMATION.—Consistent  
19           with this title, a cyber threat indicator or defensive  
20           measure provided by a non-Federal entity to the  
21           Federal Government under this title shall be consid-  
22           ered the commercial, financial, and proprietary in-  
23           formation of the non-Federal entity that is the origi-  
24           nator of such cyber threat indicator or defensive



1 measure when so designated by such non-Federal  
2 entity or a non-Federal entity acting in accordance  
3 with the written authorization of the non-Federal  
4 entity that is the originator of such cyber threat in-  
5 dicator or defensive measure.

6 (3) EXEMPTION FROM DISCLOSURE.—A cyber  
7 threat indicator or defensive measure provided to the  
8 Federal Government under this title shall be—

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

14 (B) withheld, without discretion, from the  
15 public under section 552(b)(3) of title 5, United  
16 States Code, and any State, tribal, or local pro-  
17 vision of law requiring disclosure of information  
18 or records, except as otherwise required by ap-  
19 plicable Federal, State, tribal, or local law re-  
20 quiring disclosure in any criminal prosecution.

21 (4) EX PARTE COMMUNICATIONS.—The provi-  
22 sion of a cyber threat indicator or defensive measure  
23 to the Federal Government under this title shall not  
24 be subject to a rule of any Federal department or

1 agency or any judicial doctrine regarding ex parte  
2 communications with a decision-making official.

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

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

12 (i) a cybersecurity purpose;

13 (ii) the purpose of responding to, in-  
14 vestigating, prosecuting, or otherwise pre-  
15 venting or mitigating a threat of death or  
16 serious bodily harm or an offense arising  
17 out of such a threat;

18 (iii) the purpose of responding to, in-  
19 vestigating, prosecuting, or otherwise pre-  
20 venting or mitigating, a serious threat to a  
21 minor, including sexual exploitation and  
22 threats to physical safety; or

23 (iv) the purpose of preventing, inves-  
24 tigating, disrupting, or prosecuting any of  
25 the offenses listed in sections 1028, 1029,

1                   1030, and 3559(c)(2)(F) and chapters 37  
2                   and 90 of title 18, United States Code.

3                   (B) PROHIBITED ACTIVITIES.—A cyber  
4                   threat indicator or defensive measure provided  
5                   to the Federal Government under this title shall  
6                   not be disclosed to, retained by, or used by any  
7                   Federal department or agency for any use not  
8                   permitted under subparagraph (A).

9                   (C) PRIVACY AND CIVIL LIBERTIES.—A  
10                  cyber threat indicator or defensive measure pro-  
11                  vided to the Federal Government under this  
12                  title shall be retained, used, and disseminated  
13                  by the Federal Government in accordance  
14                  with—

15                         (i) the policies and procedures relating  
16                         to the receipt of cyber threat indicators  
17                         and defensive measures by the Federal  
18                         Government required by subsection (b) of  
19                         section 111 of the National Security Act of  
20                         1947, as added by subsection (a) of this  
21                         section; and

22                         (ii) the privacy and civil liberties  
23                         guidelines required by subsection (b).

1 **SEC. 105. FEDERAL GOVERNMENT LIABILITY FOR VIOLA-**  
2 **TIONS OF PRIVACY OR CIVIL LIBERTIES.**

3 (a) IN GENERAL.—If a department or agency of the  
4 Federal Government intentionally or willfully violates the  
5 privacy and civil liberties guidelines issued by the Attorney  
6 General under section 104(b), the United States shall be  
7 liable to a person injured by such violation in an amount  
8 equal to the sum of—

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

12 (2) reasonable attorney fees as determined by  
13 the court and other litigation costs reasonably in-  
14 curred in any case under this subsection in which  
15 the complainant has substantially prevailed.

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

19 (1) the district in which the complainant re-  
20 sides;

21 (2) the district in which the principal place of  
22 business of the complainant is located;

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

26 (4) the District of Columbia.

1 (c) STATUTE OF LIMITATIONS.—No action shall lie  
2 under this section unless such action is commenced not  
3 later than 2 years after the date on which the cause of  
4 action arises.

5 (d) EXCLUSIVE CAUSE OF ACTION.—A cause of ac-  
6 tion under this section shall be the exclusive means avail-  
7 able to a complainant seeking a remedy for a violation by  
8 a department or agency of the Federal Government under  
9 this title.

10 **SEC. 106. PROTECTION FROM LIABILITY.**

11 (a) MONITORING OF INFORMATION SYSTEMS.—No  
12 cause of action shall lie or be maintained in any court  
13 against any private entity, and such action shall be  
14 promptly dismissed, for the monitoring of an information  
15 system and information under section 103(a) that is con-  
16 ducted in accordance with this title and the amendments  
17 made by this title.

18 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-  
19 CATORS.—No cause of action shall lie or be maintained  
20 in any court against any non-Federal entity, and such ac-  
21 tion shall be promptly dismissed, for the sharing or receipt  
22 of a cyber threat indicator or defensive measure under sec-  
23 tion 103(c), or a good faith failure to act based on such  
24 sharing or receipt, if such sharing or receipt is conducted

1 in accordance with this title and the amendments made  
2 by this title.

3 (c) WILLFUL MISCONDUCT.—

4 (1) RULE OF CONSTRUCTION.—Nothing in this  
5 section shall be construed—

6 (A) to require dismissal of a cause of ac-  
7 tion against a non-Federal entity (including a  
8 private entity) that has engaged in willful mis-  
9 conduct in the course of conducting activities  
10 authorized by this title or the amendments  
11 made by this title; or

12 (B) to undermine or limit the availability  
13 of otherwise applicable common law or statu-  
14 tory defenses.

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

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

1 (A) intentionally to achieve a wrongful  
2 purpose;

3 (B) knowingly without legal or factual jus-  
4 tification; and

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

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

9 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

10 (1) IN GENERAL.—Section 111 of the National  
11 Security Act of 1947, as added by section 102(a)  
12 and amended by section 104(a) of this title, is fur-  
13 ther amended—

14 (A) by redesignating subsection (c) (as re-  
15 designated by such section 104(a)) as sub-  
16 section (d); and

17 (B) by inserting after subsection (b) (as  
18 inserted by such section 104(a)) the following  
19 new subsection:

20 “(c) BIENNIAL REPORT ON IMPLEMENTATION.—

21 “(1) IN GENERAL.—Not less frequently than  
22 once every two years, the Director of National Intel-  
23 ligence, in consultation with the heads of the other  
24 appropriate Federal entities, shall submit to Con-

1       gress a report concerning the implementation of this  
2       section and the Protecting Cyber Networks Act.

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

5               “(A) An assessment of the sufficiency of  
6       the policies, procedures, and guidelines required  
7       by this section and section 4 of the Protecting  
8       Cyber Networks Act in ensuring that cyber  
9       threat indicators are shared effectively and re-  
10      sponsibly within the Federal Government.

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

15              “(C) An assessment of whether cyber  
16      threat indicators have been properly classified  
17      and an accounting of the number of security  
18      clearances authorized by the Federal Govern-  
19      ment for the purposes of this section and such  
20      Act.

21              “(D) A review of the type of cyber threat  
22      indicators shared with the Federal Government  
23      under this section and such Act, including the  
24      following:



1           “(i) The degree to which such infor-  
2           mation may impact the privacy and civil  
3           liberties of specific persons.

4           “(ii) A quantitative and qualitative as-  
5           sessment of the impact of the sharing of  
6           such cyber threat indicators with the Fed-  
7           eral Government on privacy and civil lib-  
8           erties of specific persons.

9           “(iii) The adequacy of any steps taken  
10          by the Federal Government to reduce such  
11          impact.

12          “(E) A review of actions taken by the Fed-  
13          eral Government based on cyber threat indica-  
14          tors shared with the Federal Government under  
15          this section or such Act, including the appro-  
16          priateness of any subsequent use or dissemina-  
17          tion of such cyber threat indicators by a Fed-  
18          eral entity under this section or section 4 of  
19          such Act.

20          “(F) A description of any significant viola-  
21          tions of the requirements of this section or such  
22          Act by the Federal Government—

23                 “(i) an assessment of all reports of of-  
24                 ficers, employees, and agents of the Fed-  
25                 eral Government misusing information pro-

1           vided to the Federal Government under the  
2           Protecting Cyber Networks Act or this sec-  
3           tion, without regard to whether the misuse  
4           was knowing or wilful; and

5           “(ii) an assessment of all disciplinary  
6           actions taken against such officers, em-  
7           ployees, and agents.

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

14          “(H) An assessment of any personal infor-  
15          mation of or information identifying a specific  
16          person not directly related to a cybersecurity  
17          threat that—

18                 “(i) was shared by a non-Federal enti-  
19                 ty with the Federal Government under this  
20                 Act in contravention of section 3(d)(2) of  
21                 such Act; or

22                 “(ii) was shared within the Federal  
23                 Government under this Act in contraven-  
24                 tion of the guidelines required by section  
25                 4(b) of such Act.

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

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

10           “(5) PUBLIC AVAILABILITY OF REPORTS.—The  
11           Director of National Intelligence shall make publicly  
12           available the unclassified portion of each report re-  
13           quired by paragraph (1).”.

14           (2) INITIAL REPORT.—The first report required  
15           under subsection (c) of section 111 of the National  
16           Security Act of 1947, as inserted by paragraph (1)  
17           of this subsection, shall be submitted not later than  
18           1 year after the date of the enactment of this title.

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

20           (1) BIENNIAL REPORT FROM PRIVACY AND  
21           CIVIL LIBERTIES OVERSIGHT BOARD.—

22           (A) IN GENERAL.—Section 1061(e) of the  
23           Intelligence Reform and Terrorism Prevention  
24           Act of 2004 (42 U.S.C. 2000ee(e)) is amended

1 by adding at the end the following new para-  
2 graph:

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

5 “(A) REPORT REQUIRED.—The Privacy  
6 and Civil Liberties Oversight Board shall bien-  
7 nially submit to Congress and the President a  
8 report containing—

9 “(i) an assessment of the privacy and  
10 civil liberties impact of the activities car-  
11 ried out under the Protecting Cyber Net-  
12 works Act and the amendments made by  
13 such Act; and

14 “(ii) an assessment of the sufficiency  
15 of the policies, procedures, and guidelines  
16 established pursuant to section 4 of the  
17 Protecting Cyber Networks Act and the  
18 amendments made by such section 4 in ad-  
19 dressing privacy and civil liberties con-  
20 cerns.

21 “(B) RECOMMENDATIONS.—Each report  
22 submitted under this paragraph may include  
23 such recommendations as the Privacy and Civil  
24 Liberties Oversight Board may have for im-  
25 provements or modifications to the authorities

1 under the Protecting Cyber Networks Act or  
2 the amendments made by such Act.

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

6 “(D) PUBLIC AVAILABILITY OF RE-  
7 PORTS.—The Privacy and Civil Liberties Over-  
8 sight Board shall make publicly available the  
9 unclassified portion of each report required by  
10 subparagraph (A).”.

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

18 (2) BIENNIAL REPORT OF INSPECTORS GEN-  
19 ERAL.—

20 (A) IN GENERAL.—Not later than 2 years  
21 after the date of the enactment of this title and  
22 not less frequently than once every 2 years  
23 thereafter, the Inspector General of the Depart-  
24 ment of Homeland Security, the Inspector Gen-  
25 eral of the Intelligence Community, the Inspec-

1           tor General of the Department of Justice, and  
2           the Inspector General of the Department of De-  
3           fense, in consultation with the Council of In-  
4           spectors General on Financial Oversight, shall  
5           jointly submit to Congress a report on the re-  
6           ceipt, use, and dissemination of cyber threat in-  
7           dicators and defensive measures that have been  
8           shared with Federal entities under this title and  
9           the amendments made by this title.

10           (B) CONTENTS.—Each report submitted  
11           under subparagraph (A) shall include the fol-  
12           lowing:

13                   (i) A review of the types of cyber  
14                   threat indicators shared with Federal enti-  
15                   ties.

16                   (ii) A review of the actions taken by  
17                   Federal entities as a result of the receipt  
18                   of such cyber threat indicators.

19                   (iii) A list of Federal entities receiving  
20                   such cyber threat indicators.

21                   (iv) A review of the sharing of such  
22                   cyber threat indicators among Federal en-  
23                   tities to identify inappropriate barriers to  
24                   sharing information.

1                   (v) A review of the current procedures  
2                   pertaining to the sharing of information,  
3                   removal procedures for personal informa-  
4                   tion or information identifying a specific  
5                   person, and any incidents pertaining to the  
6                   improper treatment of such information.

7                   (C) RECOMMENDATIONS.—Each report  
8                   submitted under this paragraph may include  
9                   such recommendations as the Inspectors Gen-  
10                  eral referred to in subparagraph (A) may have  
11                  for improvements or modifications to the au-  
12                  thorities under this title or the amendments  
13                  made by this title.

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

17                  (E) PUBLIC AVAILABILITY OF REPORTS.—  
18                  The Inspector General of the Department of  
19                  Homeland Security, the Inspector General of  
20                  the Intelligence Community, the Inspector Gen-  
21                  eral of the Department of Justice, and the In-  
22                  spector General of the Department of Defense  
23                  shall make publicly available the unclassified  
24                  portion of each report required under subpara-  
25                  graph (A).

1 **SEC. 108. REPORT ON CYBERSECURITY THREATS.**

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

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

14 (1) An assessment of—

15 (A) the current intelligence sharing and co-  
16 operation relationships of the United States  
17 with other countries regarding cybersecurity  
18 threats (including cyber attacks, theft, and data  
19 breaches) directed against the United States  
20 that threaten the United States national secu-  
21 rity interests, economy, and intellectual prop-  
22 erty; and

23 (B) the relative utility of such relation-  
24 ships, which elements of the intelligence com-  
25 munity participate in such relationships, and



1           whether and how such relationships could be  
2           improved.

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

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

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

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

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

4 (d) PUBLIC AVAILABILITY OF REPORT.—The Direc-  
5 tor of National Intelligence shall make publicly available  
6 the unclassified portion of the report required by sub-  
7 section (a).

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

12 **SEC. 109. CONSTRUCTION AND PREEMPTION.**

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

18 (b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in  
19 this title or the amendments made by this title shall be  
20 construed to limit or prohibit—

21 (1) otherwise lawful disclosures of communica-  
22 tions, records, or other information, including re-  
23 porting of known or suspected criminal activity, by  
24 a non-Federal entity to any other non-Federal entity  
25 or the Federal Government; or

1           (2) any otherwise lawful use of such disclosures  
2           by any entity of the Federal Government, without  
3           regard to whether such otherwise lawful disclosures  
4           duplicate or replicate disclosures made under this  
5           title.

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

16          (d) PROTECTION OF SOURCES AND METHODS.—  
17          Nothing in this title or the amendments made by this title  
18          shall be construed—

19                 (1) as creating any immunity against, or other-  
20                 wise affecting, any action brought by the Federal  
21                 Government, or any department or agency thereof,  
22                 to enforce any law, Executive order, or procedure  
23                 governing the appropriate handling, disclosure, or  
24                 use of classified information;

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

3           (3) to modify the authority of the President or  
4           a department or agency of the Federal Government  
5           to protect and control the dissemination of classified  
6           information, intelligence sources and methods, and  
7           the national security of the United States.

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

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

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

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

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

23          (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS  
24          AND RIGHTS.—Nothing in this title or the amendments  
25          made by this title shall be construed—

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

6           (2) to abrogate trade secret or intellectual prop-  
7 erty rights of any non-Federal entity or Federal  
8 entity.

9           (h) ANTI-TASKING RESTRICTION.—Nothing in this  
10 title or the amendments made by this title shall be con-  
11 strued to permit the Federal Government—

12           (1) to require a non-Federal entity to provide  
13 information to the Federal Government;

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

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

21           (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-  
22 ing in this title or the amendments made by this title shall  
23 be construed to subject any non-Federal entity to liability  
24 for choosing not to engage in a voluntary activity author-  
25 ized in this title and the amendments made by this title.

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

9           (k) FEDERAL PREEMPTION.—

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

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

22           (3) STATE REGULATION OF UTILITIES.—Except  
23 as provided by section 103(d)(4)(B), nothing in this  
24 title or the amendments made by this title shall be  
25 construed to supersede any statute, regulation, or

1 other provision of law of a State or political subdivi-  
2 sion of a State relating to the regulation of a private  
3 entity performing utility services, except to the ex-  
4 tent such statute, regulation, or other provision of  
5 law restricts activity authorized under this title or  
6 the amendments made by this title.

7 (l) REGULATORY AUTHORITY.—Nothing in this title  
8 or the amendments made by this title shall be construed—

9 (1) to authorize the promulgation of any regu-  
10 lations not specifically authorized by this title or the  
11 amendments made by this title;

12 (2) to establish any regulatory authority not  
13 specifically established under this title or the amend-  
14 ments made by this title; or

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

19 **SEC. 110. DEFINITIONS.**

20 In this title:

21 (1) AGENCY.—The term “agency” has the  
22 meaning given the term in section 3502 of title 44,  
23 United States Code.

1           (2) APPROPRIATE FEDERAL ENTITIES.—The  
2 term “appropriate Federal entities” means the fol-  
3 lowing:

4           (A) The Department of Commerce.

5           (B) The Department of Defense.

6           (C) The Department of Energy.

7           (D) The Department of Homeland Secu-  
8 rity.

9           (E) The Department of Justice.

10          (F) The Department of the Treasury.

11          (G) The Office of the Director of National  
12 Intelligence.

13           (3) CYBERSECURITY PURPOSE.—The term “cy-  
14 bersecurity purpose” means the purpose of pro-  
15 tecting (including through the use of a defensive  
16 measure) an information system or information that  
17 is stored on, processed by, or transiting an informa-  
18 tion system from a cybersecurity threat or security  
19 vulnerability or identifying the source of a cyberse-  
20 curity threat.

21           (4) CYBERSECURITY THREAT.—

22           (A) IN GENERAL.—Except as provided in  
23 subparagraph (B), the term “cybersecurity  
24 threat” means an action, not protected by the  
25 first amendment to the Constitution of the



1 United States, on or through an information  
2 system that may result in an unauthorized ef-  
3 fort to adversely impact the security, confiden-  
4 tiality, integrity, or availability of an informa-  
5 tion system or information that is stored on,  
6 processed by, or transiting an information sys-  
7 tem.

8 (B) EXCLUSION.—The term “cybersecurity  
9 threat” does not include any action that solely  
10 involves a violation of a consumer term of serv-  
11 ice or a consumer licensing agreement.

12 (5) CYBER THREAT INDICATOR.—The term  
13 “cyber threat indicator” means information or a  
14 physical object that is necessary to describe or iden-  
15 tify—

16 (A) malicious reconnaissance, including  
17 anomalous patterns of communications that ap-  
18 pear to be transmitted for the purpose of gath-  
19 ering technical information related to a cyberse-  
20 curity threat or security vulnerability;

21 (B) a method of defeating a security con-  
22 trol or exploitation of a security vulnerability;

23 (C) a security vulnerability, including  
24 anomalous activity that appears to indicate the  
25 existence of a security vulnerability;

1 (D) a method of causing a user with legiti-  
2 mate access to an information system or infor-  
3 mation that is stored on, processed by, or  
4 transiting an information system to unwittingly  
5 enable the defeat of a security control or exploi-  
6 tation of a security vulnerability;

7 (E) malicious cyber command and control;

8 (F) the actual or potential harm caused by  
9 an incident, including a description of the infor-  
10 mation exfiltrated as a result of a particular cy-  
11 bersecurity threat; or

12 (G) any other attribute of a cybersecurity  
13 threat, if disclosure of such attribute is not oth-  
14 erwise prohibited by law.

15 (6) DEFENSIVE MEASURE.—The term “defen-  
16 sive measure” means an action, device, procedure,  
17 technique, or other measure executed on an informa-  
18 tion system or information that is stored on, proc-  
19 essed by, or transiting an information system that  
20 prevents or mitigates a known or suspected cyberse-  
21 curity threat or security vulnerability.

22 (7) FEDERAL ENTITY.—The term “Federal en-  
23 tity” means a department or agency of the United  
24 States or any component of such department or  
25 agency.

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

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

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

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

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

19          (11) MALICIOUS RECONNAISSANCE.—The term  
20          “malicious reconnaissance” means a method for ac-  
21          tively probing or passively monitoring an information  
22          system for the purpose of discerning security  
23          vulnerabilities of the information system, if such  
24          method is associated with a known or suspected cy-  
25          bersecurity threat.

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

5           (13) NON-FEDERAL ENTITY.—

6           (A) IN GENERAL.—Except as otherwise  
7           provided in this paragraph, the term “non-Fed-  
8           eral entity” means any private entity, non-Fed-  
9           eral Government department or agency, or  
10          State, tribal, or local government (including a  
11          political subdivision, department, officer, em-  
12          ployee, or agent thereof).

13          (B) INCLUSIONS.—The term “non-Federal  
14          entity” includes a government department or  
15          agency (including an officer, employee, or agent  
16          thereof) of the District of Columbia, the Com-  
17          monwealth of Puerto Rico, the Virgin Islands,  
18          Guam, American Samoa, the Northern Mariana  
19          Islands, and any other territory or possession of  
20          the United States.

21          (C) EXCLUSION.—The term “non-Federal  
22          entity” does not include a foreign power or  
23          known agent of a foreign power, as both terms  
24          are defined in section 101 of the Foreign Intel-

1           ligence Surveillance Act of 1978 (50 U.S.C.  
2           1801).

3           (14) PRIVATE ENTITY.—

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

11                (B) INCLUSION.—The term “private enti-  
12          ty” includes a component of a State, tribal, or  
13          local government performing utility services.

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

18                (15) REAL TIME; REAL-TIME.—The terms “real  
19          time” and “real-time” mean a process by which an  
20          automated, machine-to-machine system processes  
21          cyber threat indicators such that the time in which  
22          the occurrence of an event and the reporting or re-  
23          cording of it are as simultaneous as technologically  
24          and operationally practicable.

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

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

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

15 **SEC. 111. COMPTROLLER GENERAL REPORT ON REMOVAL**  
16 **OF PERSONAL IDENTIFYING INFORMATION.**

17           (a) REPORT.—Not later than 3 years after the date  
18 of the enactment of this title, the Comptroller General of  
19 the United States shall submit to Congress a report on  
20 the actions taken by the Federal Government to remove  
21 personal information from cyber threat indicators pursu-  
22 ant to section 104(b).

23           (b) FORM.—The report under subsection (a) shall be  
24 submitted in unclassified form, but may include a classi-  
25 fied annex.

1 **SEC. 112. SUNSET.**

2 This title and the amendments made by this title  
3 shall terminate on the date that is 7 years after the date  
4 of the enactment of this title.

5 **TITLE II—NATIONAL CYBERSE-**  
6 **CURITY PROTECTION AD-**  
7 **VANCEMENT ACT**

8 **SEC. 201. SHORT TITLE.**

9 This title may be cited as the “National Cybersecu-  
10 rity Protection Advancement Act of 2015”.

11 **SEC. 202. NATIONAL CYBERSECURITY AND COMMUNICA-**  
12 **TIONS INTEGRATION CENTER.**

13 (a) IN GENERAL.—Subsection (a) of the second sec-  
14 tion 226 of the Homeland Security Act of 2002 (6 U.S.C.  
15 148; relating to the National Cybersecurity and Commu-  
16 nications Integration Center) is amended—

17 (1) by amending paragraph (1) to read as fol-  
18 lows:

19 “(1)(A) except as provided in subparagraph  
20 (B), the term ‘cybersecurity risk’ means threats to  
21 and vulnerabilities of information or information sys-  
22 tems and any related consequences caused by or re-  
23 sulting from unauthorized access, use, disclosure,  
24 degradation, disruption, modification, or destruction  
25 of such information or information systems, includ-

1 ing such related consequences caused by an act of  
2 terrorism;

3 “(B) such term does not include any action that  
4 solely involves a violation of a consumer term of  
5 service or a consumer licensing agreement;”.

6 (2) by amending paragraph (2) to read as fol-  
7 lows:

8 “(2) the term ‘incident’ means an occurrence  
9 that actually or imminently jeopardizes, without law-  
10 ful authority, the integrity, confidentiality, or avail-  
11 ability of information on an information system, or  
12 actually or imminently jeopardizes, without lawful  
13 authority, an information system;”.

14 (3) in paragraph (3), by striking “and” at the  
15 end;

16 (4) in paragraph (4), by striking the period at  
17 the end and inserting “; and”; and

18 (5) by adding at the end the following new  
19 paragraphs:

20 “(5) the term ‘cyber threat indicator’ means  
21 technical information that is necessary to describe or  
22 identify—

23 “(A) a method for probing, monitoring,  
24 maintaining, or establishing network awareness  
25 of an information system for the purpose of dis-



1 cerning technical vulnerabilities of such infor-  
2 mation system, if such method is known or rea-  
3 sonably suspected of being associated with a  
4 known or suspected cybersecurity risk, includ-  
5 ing communications that reasonably appear to  
6 be transmitted for the purpose of gathering  
7 technical information related to a cybersecurity  
8 risk;

9 “(B) a method for defeating a technical or  
10 security control of an information system;

11 “(C) a technical vulnerability, including  
12 anomalous technical behavior that may become  
13 a vulnerability;

14 “(D) a method of causing a user with le-  
15 gitimate access to an information system or in-  
16 formation that is stored on, processed by, or  
17 transiting an information system to inadvert-  
18 ently enable the defeat of a technical or oper-  
19 ational control;

20 “(E) a method for unauthorized remote  
21 identification of, access to, or use of an infor-  
22 mation system or information that is stored on,  
23 processed by, or transiting an information sys-  
24 tem that is known or reasonably suspected of

1 being associated with a known or suspected cy-  
2 bersecurity risk;

3 “(F) the actual or potential harm caused  
4 by a cybersecurity risk, including a description  
5 of the information exfiltrated as a result of a  
6 particular cybersecurity risk;

7 “(G) any other attribute of a cybersecurity  
8 risk that cannot be used to identify specific per-  
9 sons reasonably believed to be unrelated to such  
10 cybersecurity risk, if disclosure of such at-  
11 tribute is not otherwise prohibited by law; or

12 “(H) any combination of subparagraphs  
13 (A) through (G);

14 “(6) the term ‘cybersecurity purpose’ means the  
15 purpose of protecting an information system or in-  
16 formation that is stored on, processed by, or  
17 transiting an information system from a cybersecu-  
18 rity risk or incident, or the purpose of identifying  
19 the source of a cybersecurity risk or incident;

20 “(7)(A) except as provided in subparagraph  
21 (B), the term ‘defensive measure’ means an action,  
22 device, procedure, signature, technique, or other  
23 measure applied to an information system or infor-  
24 mation that is stored on, processed by, or transiting  
25 an information system that detects, prevents, or

1 mitigates a known or suspected cybersecurity risk or  
2 incident, or any attribute of hardware, software,  
3 process, or procedure that could enable or facilitate  
4 the defeat of a security control;

5 “(B) such term does not include a measure that  
6 destroys, renders unusable, or substantially harms  
7 an information system or data on an information  
8 system not belonging to—

9 “(i) the non-Federal entity, not including a  
10 State, local, or tribal government, operating  
11 such measure; or

12 “(ii) another Federal entity or non-Federal  
13 entity that is authorized to provide consent and  
14 has provided such consent to the non-Federal  
15 entity referred to in clause (i);

16 “(8) the term ‘network awareness’ means to  
17 scan, identify, acquire, monitor, log, or analyze in-  
18 formation that is stored on, processed by, or  
19 transiting an information system;

20 “(9)(A) the term ‘private entity’ means a non-  
21 Federal entity that is an individual or private group,  
22 organization, proprietorship, partnership, trust, co-  
23 operative, corporation, or other commercial or non-  
24 profit entity, including an officer, employee, or agent  
25 thereof;

1           “(B) such term includes a component of a  
2           State, local, or tribal government performing utility  
3           services or an entity performing utility services;

4           “(10) the term ‘security control’ means the  
5           management, operational, and technical controls  
6           used to protect against an unauthorized effort to ad-  
7           versely affect the confidentiality, integrity, or avail-  
8           ability of an information system or information that  
9           is stored on, processed by, or transiting an informa-  
10          tion system; and

11          “(11) the term ‘sharing’ (including all conjuga-  
12          tions thereof) means providing, receiving, and dis-  
13          seminating (including all conjugations of each of  
14          such terms).”.

15          (b) AMENDMENT.—Subparagraph (B) of subsection  
16          (d)(1) of such second section 226 of the Homeland Secu-  
17          rity Act of 2002 is amended—

18                 (1) in clause (i), by striking “and local” and in-  
19                 serting “, local, and tribal”;

20                 (2) in clause (ii)—

21                         (A) by inserting “, including information  
22                         sharing and analysis centers” before the semi-  
23                         colon; and

24                         (B) by striking “and” at the end;

1           (3) in clause (iii), by inserting “and” after the  
2           semicolon at the end; and

3           (4) by adding at the end the following new  
4           clause:

5                           “(iv) private entities;”.

6   **SEC. 203. INFORMATION SHARING STRUCTURE AND PROC-**  
7                           **ESSES.**

8           The second section 226 of the Homeland Security Act  
9   of 2002 (6 U.S.C. 148; relating to the National Cyberse-  
10   curity and Communications Integration Center) is amend-  
11   ed—

12           (1) in subsection (c)—

13                   (A) in paragraph (1)—

14                           (i) by striking “a Federal civilian  
15                           interface” and inserting “the lead Federal  
16                           civilian interface”; and

17                           (ii) by striking “cybersecurity risks,”  
18                           and inserting “cyber threat indicators, de-  
19                           fensive measures, cybersecurity risks,”;

20                   (B) in paragraph (3), by striking “cyberse-  
21                   curity risks” and inserting “cyber threat indica-  
22                   tors, defensive measures, cybersecurity risks,”;

23                   (C) in paragraph (5)(A), by striking “cy-  
24                   bersecurity risks” and inserting “cyber threat

1 indicators, defensive measures, cybersecurity  
2 risks,”;

3 (D) in paragraph (6)—

4 (i) by striking “cybersecurity risks”  
5 and inserting “cyber threat indicators, de-  
6 fensive measures, cybersecurity risks,”;  
7 and

8 (ii) by striking “and” at the end;

9 (E) in paragraph (7)—

10 (i) in subparagraph (A), by striking  
11 “and” at the end;

12 (ii) in subparagraph (B), by striking  
13 the period at the end and inserting “;  
14 and”; and

15 (iii) by adding at the end the fol-  
16 lowing new subparagraph:

17 “(C) sharing cyber threat indicators and  
18 defensive measures;”; and

19 (F) by adding at the end the following new  
20 paragraphs:

21 “(8) engaging with international partners, in  
22 consultation with other appropriate agencies, to—

23 “(A) collaborate on cyber threat indicators,  
24 defensive measures, and information related to  
25 cybersecurity risks and incidents; and

1           “(B) enhance the security and resilience of  
2           global cybersecurity;

3           “(9) sharing cyber threat indicators, defensive  
4           measures, and other information related to cyberse-  
5           curity risks and incidents with Federal and non-Fed-  
6           eral entities, including across sectors of critical in-  
7           frastructure and with State and major urban area  
8           fusion centers, as appropriate;

9           “(10) promptly notifying the Secretary and the  
10          Committee on Homeland Security of the House of  
11          Representatives and the Committee on Homeland  
12          Security and Governmental Affairs of the Senate of  
13          any significant violations of the policies and proce-  
14          dures specified in subsection (i)(6)(A);

15          “(11) promptly notifying non-Federal entities  
16          that have shared cyber threat indicators or defensive  
17          measures that are known or determined to be in  
18          error or in contravention of the requirements of this  
19          section; and

20          “(12) participating, as appropriate, in exercises  
21          run by the Department’s National Exercise Pro-  
22          gram.”;

23          (2) in subsection (d)(1)—

24                  (A) in subparagraph (D), by striking  
25                  “and” at the end;

1 (B) by redesignating subparagraph (E) as  
2 subparagraph (J); and

3 (C) by inserting after subparagraph (D)  
4 the following new subparagraphs:

5 “(E) an entity that collaborates with State  
6 and local governments on cybersecurity risks  
7 and incidents, and has entered into a voluntary  
8 information sharing relationship with the Cen-  
9 ter;

10 “(F) a United States Computer Emer-  
11 gency Readiness Team that coordinates infor-  
12 mation related to cybersecurity risks and inci-  
13 dents, proactively and collaboratively addresses  
14 cybersecurity risks and incidents to the United  
15 States, collaboratively responds to cybersecurity  
16 risks and incidents, provides technical assist-  
17 ance, upon request, to information system own-  
18 ers and operators, and shares cyber threat indi-  
19 cators, defensive measures, analysis, or infor-  
20 mation related to cybersecurity risks and inci-  
21 dents in a timely manner;

22 “(G) the Industrial Control System Cyber  
23 Emergency Response Team that—

24 “(i) coordinates with industrial con-  
25 trol systems owners and operators;



1           “(ii) provides training, upon request,  
2           to Federal entities and non-Federal enti-  
3           ties on industrial control systems cyberse-  
4           curity;

5           “(iii) collaboratively addresses cyber-  
6           security risks and incidents to industrial  
7           control systems;

8           “(iv) provides technical assistance,  
9           upon request, to Federal entities and non-  
10          Federal entities relating to industrial con-  
11          trol systems cybersecurity;

12          “(v) shares cyber threat indicators,  
13          defensive measures, or information related  
14          to cybersecurity risks and incidents of in-  
15          dustrial control systems in a timely fash-  
16          ion; and

17          “(vi) remains current on industrial  
18          control system innovation; industry adop-  
19          tion of new technologies, and industry best  
20          practices;

21          “(H) a National Coordinating Center for  
22          Communications that coordinates the protec-  
23          tion, response, and recovery of emergency com-  
24          munications;

1           “(I) an entity that coordinates with small  
2 and medium-sized businesses; and”;

3           (3) in subsection (e)—

4           (A) in paragraph (1)—

5           (i) in subparagraph (A), by inserting  
6 “cyber threat indicators, defensive meas-  
7 ures, and” before “information”;

8           (ii) in subparagraph (B), by inserting  
9 “cyber threat indicators, defensive meas-  
10 ures, and” before “information” the first  
11 place it appears;

12           (iii) in subparagraph (F), by striking  
13 “cybersecurity risks” and inserting “cyber  
14 threat indicators, defensive measures, cy-  
15 bersecurity risks,”;

16           (iv) in subparagraph (F), by striking  
17 “and” at the end;

18           (v) in subparagraph (G), by striking  
19 “cybersecurity risks” and inserting “cyber  
20 threat indicators, defensive measures, cy-  
21 bersecurity risks,”; and

22           (vi) by adding at the end the fol-  
23 lowing:

24           “(H) the Center ensures that it shares in-  
25 formation relating to cybersecurity risks and in-

1           idents with small and medium-sized busi-  
2           nesses, as appropriate, and, to the extent prac-  
3           ticable, make self-assessment tools available to  
4           such businesses to determine their levels of pre-  
5           vention of cybersecurity risks; and

6           “(I) the Center designates an agency con-  
7           tact for non-Federal entities;”;

8           (B) in paragraph (2)—

9           (i) by striking “cybersecurity risks”  
10           and inserting “cyber threat indicators, de-  
11           fensive measures, cybersecurity risks;”;  
12           and

13           (ii) by inserting “or disclosure” before  
14           the semicolon at the end; and

15           (C) in paragraph (3), by inserting before  
16           the period at the end the following: “, including  
17           by working with the Chief Privacy Officer ap-  
18           pointed under section 222 to ensure that the  
19           Center follows the policies and procedures speci-  
20           fied in subsection (i)(6)(A)”;

21           (4) by adding at the end the following new sub-  
22           sections:

23           “(g) RAPID AUTOMATED SHARING.—

24           “(1) IN GENERAL.—The Under Secretary for  
25           Cybersecurity and Infrastructure Protection, in co-

1 ordination with industry and other stakeholders,  
2 shall develop capabilities making use of existing in-  
3 formation technology industry standards and best  
4 practices, as appropriate, that support and rapidly  
5 advance the development, adoption, and implementa-  
6 tion of automated mechanisms for the timely sharing  
7 of cyber threat indicators and defensive measures to  
8 and from the Center and with each Federal agency  
9 designated as the ‘Sector Specific Agency’ for each  
10 critical infrastructure sector in accordance with sub-  
11 section (h).

12 “(2) BIENNIAL REPORT.—The Under Sec-  
13 retary for Cybersecurity and Infrastructure Protec-  
14 tion shall submit to the Committee on Homeland Se-  
15 curity of the House of Representatives and the Com-  
16 mittee on Homeland Security and Governmental Af-  
17 fairs of the Senate a biannual report on the status  
18 and progress of the development of the capability de-  
19 scribed in paragraph (1). Such reports shall be re-  
20 quired until such capability is fully implemented.

21 “(h) SECTOR SPECIFIC AGENCIES.—The Secretary,  
22 in collaboration with the relevant critical infrastructure  
23 sector and the heads of other appropriate Federal agen-  
24 cies, shall recognize the Federal agency designated as of  
25 March 25, 2015, as the ‘Sector Specific Agency’ for each

1 critical infrastructure sector designated in the Depart-  
2 ment’s National Infrastructure Protection Plan. If the  
3 designated Sector Specific Agency for a particular critical  
4 infrastructure sector is the Department, for purposes of  
5 this section, the Secretary is deemed to be the head of  
6 such Sector Specific Agency and shall carry out this sec-  
7 tion. The Secretary, in coordination with the heads of each  
8 such Sector Specific Agency, shall—

9           “(1) support the security and resilience actives  
10       of the relevant critical infrastructure sector in ac-  
11       cordance with this section;

12           “(2) provide institutional knowledge, specialized  
13       expertise, and technical assistance upon request to  
14       the relevant critical infrastructure sector; and

15           “(3) support the timely sharing of cyber threat  
16       indicators and defensive measures with the relevant  
17       critical infrastructure sector with the Center in ac-  
18       cordance with this section.

19       “(i) VOLUNTARY INFORMATION SHARING PROCE-  
20 DURES.—

21           “(1) PROCEDURES.—

22           “(A) IN GENERAL.—The Center may enter  
23       into a voluntary information sharing relation-  
24       ship with any consenting non-Federal entity for  
25       the sharing of cyber threat indicators and de-

1           fensive measures for cybersecurity purposes in  
2           accordance with this section. Nothing in this  
3           section may be construed to require any non-  
4           Federal entity to enter into any such informa-  
5           tion sharing relationship with the Center or any  
6           other entity. The Center may terminate a vol-  
7           untary information sharing relationship under  
8           this subsection, at the sole and unreviewable  
9           discretion of the Secretary, acting through the  
10          Under Secretary for Cybersecurity and Infra-  
11          structure Protection, if the Center determines  
12          that the non-Federal entity with which the Cen-  
13          ter has entered into such a relationship has,  
14          after repeated notice, repeatedly violated the  
15          terms of this subsection.

16                 “(B) NATIONAL SECURITY.—The Sec-  
17          retary may decline to enter into a voluntary in-  
18          formation sharing relationship under this sub-  
19          section, at the sole and unreviewable discretion  
20          of the Secretary, acting through the Under Sec-  
21          retary for Cybersecurity and Infrastructure  
22          Protection, if the Secretary determines that  
23          such is appropriate for national security.

24                 “(2) VOLUNTARY INFORMATION SHARING RELA-  
25          TIONSHPIS.—A voluntary information sharing rela-

1        tionship under this subsection may be characterized  
2        as an agreement described in this paragraph.

3                “(A) STANDARD AGREEMENT.—For the  
4                use of a non-Federal entity, the Center shall  
5                make available a standard agreement, con-  
6                sistent with this section, on the Department’s  
7                website.

8                “(B) NEGOTIATED AGREEMENT.—At the  
9                request of a non-Federal entity, and if deter-  
10              mined appropriate by the Center, at the sole  
11              and unreviewable discretion of the Secretary,  
12              acting through the Under Secretary for Cyber-  
13              security and Infrastructure Protection, the De-  
14              partment shall negotiate a non-standard agree-  
15              ment, consistent with this section.

16              “(C) EXISTING AGREEMENTS.—An agree-  
17              ment between the Center and a non-Federal en-  
18              tity that is entered into before the date of the  
19              enactment of this section, or such an agreement  
20              that is in effect before such date, shall be  
21              deemed in compliance with the requirements of  
22              this subsection, notwithstanding any other pro-  
23              vision or requirement of this subsection. An  
24              agreement under this subsection shall include  
25              the relevant privacy protections as in effect

1 under the Cooperative Research and Develop-  
2 ment Agreement for Cybersecurity Information  
3 Sharing and Collaboration, as of December 31,  
4 2014. Nothing in this subsection may be con-  
5 strued to require a non-Federal entity to enter  
6 into either a standard or negotiated agreement  
7 to be in compliance with this subsection.

8 “(3) INFORMATION SHARING AUTHORIZA-  
9 TION.—

10 “(A) IN GENERAL.—Except as provided in  
11 subparagraph (B), and notwithstanding any  
12 other provision of law, a non-Federal entity  
13 may, for cybersecurity purposes, share cyber  
14 threat indicators or defensive measures ob-  
15 tained on its own information system, or on an  
16 information system of another Federal entity or  
17 non-Federal entity, upon written consent of  
18 such other Federal entity or non-Federal entity  
19 or an authorized representative of such other  
20 Federal entity or non-Federal entity in accord-  
21 ance with this section with—

22 “(i) another non-Federal entity; or

23 “(ii) the Center, as provided in this  
24 section.



1           “(B) **LAWFUL RESTRICTION.**—A non-Fed-  
2           eral entity receiving a cyber threat indicator or  
3           defensive measure from another Federal entity  
4           or non-Federal entity shall comply with other-  
5           wise lawful restrictions placed on the sharing or  
6           use of such cyber threat indicator or defensive  
7           measure by the sharing Federal entity or non-  
8           Federal entity.

9           “(C) **REMOVAL OF INFORMATION UNRE-**  
10           **LATED TO CYBERSECURITY RISKS OR INCI-**  
11           **DENTS.**—Federal entities and non-Federal enti-  
12           ties shall, prior to such sharing, take reasonable  
13           efforts to remove or exclude information that  
14           can be used to identify specific persons and is  
15           reasonably believed at the time of sharing to be  
16           unrelated to a cybersecurity risk or incident and  
17           to safeguard information that can be used to  
18           identify specific persons from unintended disclo-  
19           sure or unauthorized access or acquisition.

20           “(D) **RULE OF CONSTRUCTION.**—Nothing  
21           in this paragraph may be construed to—

22                   “(i) limit or modify an existing infor-  
23                   mation sharing relationship;

24                   “(ii) prohibit a new information shar-  
25                   ing relationship;

1           “(iii) require a new information shar-  
2           ing relationship between any non-Federal  
3           entity and a Federal entity;

4           “(iv) limit otherwise lawful activity; or

5           “(v) in any manner impact or modify  
6           procedures in existence as of the date of  
7           the enactment of this section for reporting  
8           known or suspected criminal activity to ap-  
9           propriate law enforcement authorities or  
10          for participating voluntarily or under legal  
11          requirement in an investigation.

12          “(E) COORDINATED VULNERABILITY DIS-  
13          CLOSURE.—The Under Secretary for Cyberse-  
14          curity and Infrastructure Protection, in coordi-  
15          nation with industry and other stakeholders,  
16          shall develop, publish, and adhere to policies  
17          and procedures for coordinating vulnerability  
18          disclosures, to the extent practicable, consistent  
19          with international standards in the information  
20          technology industry.

21          “(4) NETWORK AWARENESS AUTHORIZATION.—

22                 “(A) IN GENERAL.—Notwithstanding any  
23                 other provision of law, a non-Federal entity, not  
24                 including a State, local, or tribal government,

1           may, for cybersecurity purposes, conduct net-  
2           work awareness of—

3                   “(i) an information system of such  
4                   non-Federal entity to protect the rights or  
5                   property of such non-Federal entity;

6                   “(ii) an information system of another  
7                   non-Federal entity, upon written consent  
8                   of such other non-Federal entity for con-  
9                   ducting such network awareness to protect  
10                  the rights or property of such other non-  
11                  Federal entity;

12                  “(iii) an information system of a Fed-  
13                  eral entity, upon written consent of an au-  
14                  thorized representative of such Federal en-  
15                  tity for conducting such network awareness  
16                  to protect the rights or property of such  
17                  Federal entity; or

18                  “(iv) information that is stored on,  
19                  processed by, or transiting an information  
20                  system described in this subparagraph.

21                  “(B) RULE OF CONSTRUCTION.—Nothing  
22                  in this paragraph may be construed to—

23                   “(i) authorize conducting network  
24                   awareness of an information system, or the  
25                   use of any information obtained through

1           such conducting of network awareness,  
2           other than as provided in this section; or

3           “(ii) limit otherwise lawful activity.

4           “(5) DEFENSIVE MEASURE AUTHORIZATION.—

5           “(A) IN GENERAL.—Except as provided in  
6           subparagraph (B) and notwithstanding any  
7           other provision of law, a non-Federal entity, not  
8           including a State, local, or tribal government,  
9           may, for cybersecurity purposes, operate a de-  
10          fensive measure that is applied to—

11           “(i) an information system of such  
12          non-Federal entity to protect the rights or  
13          property of such non-Federal entity;

14           “(ii) an information system of another  
15          non-Federal entity upon written consent of  
16          such other non-Federal entity for operation  
17          of such defensive measure to protect the  
18          rights or property of such other non-Fed-  
19          eral entity;

20           “(iii) an information system of a Fed-  
21          eral entity upon written consent of an au-  
22          thorized representative of such Federal en-  
23          tity for operation of such defensive meas-  
24          ure to protect the rights or property of  
25          such Federal entity; or

1           “(iv) information that is stored on,  
2           processed by, or transiting an information  
3           system described in this subparagraph.

4           “(B) RULE OF CONSTRUCTION.—Nothing  
5           in this paragraph may be construed to—

6           “(i) authorize the use of a defensive  
7           measure other than as provided in this sec-  
8           tion; or

9           “(ii) limit otherwise lawful activity.

10          “(6) PRIVACY AND CIVIL LIBERTIES PROTEC-  
11          TIONS.—

12          “(A) POLICIES AND PROCEDURES.—

13               “(i) IN GENERAL.—The Under Sec-  
14               retary for Cybersecurity and Infrastructure  
15               Protection shall, in coordination with the  
16               Chief Privacy Officer and the Chief Civil  
17               Rights and Civil Liberties Officer of the  
18               Department, establish and annually review  
19               policies and procedures governing the re-  
20               ceipt, retention, use, and disclosure of  
21               cyber threat indicators, defensive meas-  
22               ures, and information related to cybersecu-  
23               rity risks and incidents shared with the  
24               Center in accordance with this section.  
25               Such policies and procedures shall apply

1           only to the Department, consistent with  
2           the need to protect information systems  
3           from cybersecurity risks and incidents and  
4           mitigate cybersecurity risks and incidents  
5           in a timely manner, and shall—

6                     “(I) be consistent with the De-  
7                     partment’s Fair Information Practice  
8                     Principles developed pursuant to sec-  
9                     tion 552a of title 5, United States  
10                    Code (commonly referred to as the  
11                    ‘Privacy Act of 1974’ or the ‘Privacy  
12                    Act’), and subject to the Secretary’s  
13                    authority under subsection (a)(2) of  
14                    section 222 of this Act;

15                    “(II) reasonably limit, to the  
16                    greatest extent practicable, the re-  
17                    ceipt, retention, use, and disclosure of  
18                    cyber threat indicators and defensive  
19                    measures associated with specific per-  
20                    sons that is not necessary, for cyber-  
21                    security purposes, to protect a net-  
22                    work or information system from cy-  
23                    bersecurity risks or mitigate cyberse-  
24                    curity risks and incidents in a timely  
25                    manner;

1           “(III) minimize any impact on  
2 privacy and civil liberties;

3           “(IV) provide data integrity  
4 through the prompt removal and de-  
5 struction of obsolete or erroneous  
6 names and personal information that  
7 is unrelated to the cybersecurity risk  
8 or incident information shared and re-  
9 tained by the Center in accordance  
10 with this section;

11           “(V) include requirements to  
12 safeguard cyber threat indicators and  
13 defensive measures retained by the  
14 Center, including information that is  
15 proprietary or business-sensitive, or  
16 that may be used to identify specific  
17 persons from unauthorized access or  
18 acquisition;

19           “(VI) protect the confidentiality  
20 of cyber threat indicators and defen-  
21 sive measures associated with specific  
22 persons to the greatest extent prac-  
23 ticable; and

1                   “(VII) ensure all relevant con-  
2                   stitutional, legal, and privacy protec-  
3                   tions are observed.

4                   “(ii) SUBMISSION TO CONGRESS.—  
5                   Not later than 180 days after the date of  
6                   the enactment of this section and annually  
7                   thereafter, the Chief Privacy Officer and  
8                   the Officer for Civil Rights and Civil Lib-  
9                   erties of the Department, in consultation  
10                  with the Privacy and Civil Liberties Over-  
11                  sight Board (established pursuant to sec-  
12                  tion 1061 of the Intelligence Reform and  
13                  Terrorism Prevention Act of 2004 (42  
14                  U.S.C. 2000ee)), shall submit to the Com-  
15                  mittee on Homeland Security of the House  
16                  of Representatives and the Committee on  
17                  Homeland Security and Governmental Af-  
18                  fairs of the Senate the policies and proce-  
19                  dures governing the sharing of cyber threat  
20                  indicators, defensive measures, and infor-  
21                  mation related to cybersecurity risks and  
22                  incidents described in clause (i) of sub-  
23                  paragraph (A).

24                  “(iii) PUBLIC NOTICE AND ACCESS.—  
25                  The Under Secretary for Cybersecurity



1 and Infrastructure Protection, in consulta-  
2 tion with the Chief Privacy Officer and the  
3 Chief Civil Rights and Civil Liberties Offi-  
4 cer of the Department, and the Privacy  
5 and Civil Liberties Oversight Board (estab-  
6 lished pursuant to section 1061 of the In-  
7 telligence Reform and Terrorism Preven-  
8 tion Act of 2004 (42 U.S.C. 2000ee)),  
9 shall ensure there is public notice of, and  
10 access to, the policies and procedures gov-  
11 erning the sharing of cyber threat indica-  
12 tors, defensive measures, and information  
13 related to cybersecurity risks and inci-  
14 dents.

15 “(iv) CONSULTATION.—The Under  
16 Secretary for Cybersecurity and Infrastruc-  
17 ture Protection when establishing policies  
18 and procedures to support privacy and civil  
19 liberties may consult with the National In-  
20 stitute of Standards and Technology.

21 “(B) IMPLEMENTATION.—The Chief Pri-  
22 vacy Officer of the Department, on an ongoing  
23 basis, shall—

24 “(i) monitor the implementation of  
25 the policies and procedures governing the

1 sharing of cyber threat indicators and de-  
2 fensive measures established pursuant to  
3 clause (i) of subparagraph (A);

4 “(ii) regularly review and update pri-  
5 vacy impact assessments, as appropriate,  
6 to ensure all relevant constitutional, legal,  
7 and privacy protections are being followed;

8 “(iii) work with the Under Secretary  
9 for Cybersecurity and Infrastructure Pro-  
10 tection to carry out paragraphs (10) and  
11 (11) of subsection (c);

12 “(iv) annually submit to the Com-  
13 mittee on Homeland Security of the House  
14 of Representatives and the Committee on  
15 Homeland Security and Governmental Af-  
16 fairs of the Senate a report that contains  
17 a review of the effectiveness of such poli-  
18 cies and procedures to protect privacy and  
19 civil liberties; and

20 “(v) ensure there are appropriate  
21 sanctions in place for officers, employees,  
22 or agents of the Department who inten-  
23 tionally or willfully conduct activities under  
24 this section in an unauthorized manner.

1           “(C) INSPECTOR GENERAL REPORT.—The  
2           Inspector General of the Department, in con-  
3           sultation with the Privacy and Civil Liberties  
4           Oversight Board and the Inspector General of  
5           each Federal agency that receives cyber threat  
6           indicators or defensive measures shared with  
7           the Center under this section, shall, not later  
8           than two years after the date of the enactment  
9           of this subsection and periodically thereafter  
10          submit to the Committee on Homeland Security  
11          of the House of Representatives and the Com-  
12          mittee on Homeland Security and Govern-  
13          mental Affairs of the Senate a report con-  
14          taining a review of the use of cybersecurity risk  
15          information shared with the Center, including  
16          the following:

17                   “(i) A report on the receipt, use, and  
18                   dissemination of cyber threat indicators  
19                   and defensive measures that have been  
20                   shared with Federal entities under this  
21                   section.

22                   “(ii) Information on the use by the  
23                   Center of such information for a purpose  
24                   other than a cybersecurity purpose.

1           “(iii) A review of the type of informa-  
2           tion shared with the Center under this sec-  
3           tion.

4           “(iv) A review of the actions taken by  
5           the Center based on such information.

6           “(v) The appropriate metrics that  
7           exist to determine the impact, if any, on  
8           privacy and civil liberties as a result of the  
9           sharing of such information with the Cen-  
10          ter.

11          “(vi) A list of other Federal agencies  
12          receiving such information.

13          “(vii) A review of the sharing of such  
14          information within the Federal Govern-  
15          ment to identify inappropriate stove piping  
16          of such information.

17          “(viii) Any recommendations of the  
18          Inspector General of the Department for  
19          improvements or modifications to informa-  
20          tion sharing under this section.

21          “(D) PRIVACY AND CIVIL LIBERTIES OFFI-  
22          CERS REPORT.—The Chief Privacy Officer and  
23          the Chief Civil Rights and Civil Liberties Offi-  
24          cer of the Department, in consultation with the  
25          Privacy and Civil Liberties Oversight Board,

1 the Inspector General of the Department, and  
2 the senior privacy and civil liberties officer of  
3 each Federal agency that receives cyber threat  
4 indicators and defensive measures shared with  
5 the Center under this section, shall biennially  
6 submit to the appropriate congressional com-  
7 mittees a report assessing the privacy and civil  
8 liberties impact of the activities under this  
9 paragraph. Each such report shall include any  
10 recommendations the Chief Privacy Officer and  
11 the Chief Civil Rights and Civil Liberties Offi-  
12 cer of the Department consider appropriate to  
13 minimize or mitigate the privacy and civil lib-  
14 erties impact of the sharing of cyber threat in-  
15 dicators and defensive measures under this sec-  
16 tion.

17 “(E) FORM.—Each report required under  
18 subparagraphs (C) and (D) shall be submitted  
19 in unclassified form, but may include a classi-  
20 fied annex.

21 “(7) USES AND PROTECTION OF INFORMA-  
22 TION.—

23 “(A) NON-FEDERAL ENTITIES.—A non-  
24 Federal entity, not including a State, local, or  
25 tribal government, that shares cyber threat in-

1 indicators or defensive measures through the Cen-  
2 ter or otherwise under this section—

3 “(i) may use, retain, or further dis-  
4 close such cyber threat indicators or defen-  
5 sive measures solely for cybersecurity pur-  
6 poses;

7 “(ii) shall, prior to such sharing, take  
8 reasonable efforts to remove or exclude in-  
9 formation that can be used to identify spe-  
10 cific persons and is reasonably believed at  
11 the time of sharing to be unrelated to a cy-  
12 bersecurity risk or incident, and to safe-  
13 guard information that can be used to  
14 identify specific persons from unintended  
15 disclosure or unauthorized access or acqui-  
16 sition;

17 “(iii) shall comply with appropriate  
18 restrictions that a Federal entity or non-  
19 Federal entity places on the subsequent  
20 disclosure or retention of cyber threat indi-  
21 cators and defensive measures that it dis-  
22 closes to other Federal entities or non-Fed-  
23 eral entities;

1           “(iv) shall be deemed to have volun-  
2           tarily shared such cyber threat indicators  
3           or defensive measures;

4           “(v) shall implement and utilize a se-  
5           curity control to protect against unauthor-  
6           ized access to or acquisition of such cyber  
7           threat indicators or defensive measures;  
8           and

9           “(vi) may not use such information to  
10          gain an unfair competitive advantage to  
11          the detriment of any non-Federal entity.

12          “(B) FEDERAL ENTITIES.—

13                 “(i) USES OF INFORMATION.—A Fed-  
14                 eral entity that receives cyber threat indi-  
15                 cators or defensive measures shared  
16                 through the Center or otherwise under this  
17                 section from another Federal entity or a  
18                 non-Federal entity—

19                         “(I) may use, retain, or further  
20                         disclose such cyber threat indicators  
21                         or defensive measures solely for cyber-  
22                         security purposes;

23                         “(II) shall, prior to such sharing,  
24                         take reasonable efforts to remove or  
25                         exclude information that can be used

1 to identify specific persons and is rea-  
2 sonably believed at the time of sharing  
3 to be unrelated to a cybersecurity risk  
4 or incident, and to safeguard informa-  
5 tion that can be used to identify spe-  
6 cific persons from unintended diselo-  
7 sure or unauthorized access or acqui-  
8 sition;

9 “(III) shall be deemed to have  
10 voluntarily shared such cyber threat  
11 indicators or defensive measures;

12 “(IV) shall implement and utilize  
13 a security control to protect against  
14 unauthorized access to or acquisition  
15 of such cyber threat indicators or de-  
16 fensive measures; and

17 “(V) may not use such cyber  
18 threat indicators or defensive meas-  
19 ures to engage in surveillance or other  
20 collection activities for the purpose of  
21 tracking an individual’s personally  
22 identifiable information, except for  
23 purposes authorized in this section.



1           “(ii) PROTECTIONS FOR INFORMA-  
2           TION.—The cyber threat indicators and de-  
3           fensive measures referred to in clause (i)—

4                   “(I) are exempt from disclosure  
5                   under section 552 of title 5, United  
6                   States Code, and withheld, without  
7                   discretion, from the public under sub-  
8                   section (b)(3)(B) of such section;

9                   “(II) may not be used by the  
10                  Federal Government for regulatory  
11                  purposes;

12                  “(III) may not constitute a waiv-  
13                  er of any applicable privilege or pro-  
14                  tection provided by law, including  
15                  trade secret protection;

16                  “(IV) shall be considered the  
17                  commercial, financial, and proprietary  
18                  information of the non-Federal entity  
19                  referred to in clause (i) when so des-  
20                  ignated by such non-Federal entity;  
21                  and

22                  “(V) may not be subject to a rule  
23                  of any Federal entity or any judicial  
24                  doctrine regarding ex parte commu-

1                   communications with a decisionmaking offi-  
2                   cial.

3                   “(C) STATE, LOCAL, OR TRIBAL GOVERN-  
4                   MENT.—

5                   “(i) USES OF INFORMATION.—A  
6                   State, local, or tribal government that re-  
7                   ceives cyber threat indicators or defensive  
8                   measures from the Center from a Federal  
9                   entity or a non-Federal entity—

10                   “(I) may use, retain, or further  
11                   disclose such cyber threat indicators  
12                   or defensive measures solely for cyber-  
13                   security purposes;

14                   “(II) shall, prior to such sharing,  
15                   take reasonable efforts to remove or  
16                   exclude information that can be used  
17                   to identify specific persons and is rea-  
18                   sonably believed at the time of sharing  
19                   to be unrelated to a cybersecurity risk  
20                   or incident, and to safeguard informa-  
21                   tion that can be used to identify spe-  
22                   cific persons from unintended disclo-  
23                   sure or unauthorized access or acqui-  
24                   sition;

1           “(III) shall consider such infor-  
2           mation the commercial, financial, and  
3           proprietary information of such Fed-  
4           eral entity or non-Federal entity if so  
5           designated by such Federal entity or  
6           non-Federal entity;

7           “(IV) shall be deemed to have  
8           voluntarily shared such cyber threat  
9           indicators or defensive measures; and

10           “(V) shall implement and utilize  
11           a security control to protect against  
12           unauthorized access to or acquisition  
13           of such cyber threat indicators or de-  
14           fensive measures.

15           “(ii) PROTECTIONS FOR INFORMA-  
16           TION.—The cyber threat indicators and de-  
17           fensive measures referred to in clause (i)—

18           “(I) shall be exempt from disclo-  
19           sure under any State, local, or tribal  
20           law or regulation that requires public  
21           disclosure of information or records  
22           by a public or quasi-public entity; and

23           “(II) may not be used by any  
24           State, local, or tribal government to

1 regulate a lawful activity of a non-  
2 Federal entity.

3 “(8) LIABILITY EXEMPTIONS.—

4 “(A) NETWORK AWARENESS.—No cause of  
5 action shall lie or be maintained in any court,  
6 and such action shall be promptly dismissed,  
7 against any non-Federal entity that, for cyber-  
8 security purposes, conducts network awareness  
9 under paragraph (4), if such network awareness  
10 is conducted in accordance with such paragraph  
11 and this section.

12 “(B) INFORMATION SHARING.—No cause  
13 of action shall lie or be maintained in any  
14 court, and such action shall be promptly dis-  
15 missed, against any non-Federal entity that, for  
16 cybersecurity purposes, shares cyber threat in-  
17 dicators or defensive measures under paragraph  
18 (3), or in good faith fails to act based on such  
19 sharing, if such sharing is conducted in accord-  
20 ance with such paragraph and this section.

21 “(C) WILLFUL MISCONDUCT.—

22 “(i) RULE OF CONSTRUCTION.—Noth-  
23 ing in this section may be construed to—

24 “(I) require dismissal of a cause  
25 of action against a non-Federal entity

1 that has engaged in willful misconduct  
2 in the course of conducting activities  
3 authorized by this section; or

4 “(II) undermine or limit the  
5 availability of otherwise applicable  
6 common law or statutory defenses.

7 “(ii) PROOF OF WILLFUL MIS-  
8 CONDUCT.—In any action claiming that  
9 subparagraph (A) or (B) does not apply  
10 due to willful misconduct described in  
11 clause (i), the plaintiff shall have the bur-  
12 den of proving by clear and convincing evi-  
13 dence the willful misconduct by each non-  
14 Federal entity subject to such claim and  
15 that such willful misconduct proximately  
16 caused injury to the plaintiff.

17 “(iii) WILLFUL MISCONDUCT DE-  
18 FINED.—In this subsection, the term ‘will-  
19 ful misconduct’ means an act or omission  
20 that is taken—

21 “(I) intentionally to achieve a  
22 wrongful purpose;

23 “(II) knowingly without legal or  
24 factual justification; and

1                   “(III) in disregard of a known or  
2                   obvious risk that is so great as to  
3                   make it highly probable that the harm  
4                   will outweigh the benefit.

5                   “(D) EXCLUSION.—The term ‘non-Federal  
6                   entity’ as used in this paragraph shall not in-  
7                   clude a State, local, or tribal government.

8                   “(9) FEDERAL GOVERNMENT LIABILITY FOR  
9                   VIOLATIONS OF RESTRICTIONS ON THE USE AND  
10                  PROTECTION OF VOLUNTARILY SHARED INFORMA-  
11                  TION.—

12                  “(A) IN GENERAL.—If a department or  
13                  agency of the Federal Government intentionally  
14                  or willfully violates the restrictions specified in  
15                  paragraph (3), (6), or (7)(B) on the use and  
16                  protection of voluntarily shared cyber threat in-  
17                  dicators or defensive measures, or any other  
18                  provision of this section, the Federal Govern-  
19                  ment shall be liable to a person injured by such  
20                  violation in an amount equal to the sum of—

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

24                         “(ii) reasonable attorney fees as deter-  
25                         mined by the court and other litigation

1 costs reasonably occurred in any case  
2 under this subsection in which the com-  
3 plainant has substantially prevailed.

4 “(B) VENUE.—An action to enforce liabil-  
5 ity under this subsection may be brought in the  
6 district court of the United States in—

7 “(i) the district in which the com-  
8 plainant resides;

9 “(ii) the district in which the principal  
10 place of business of the complainant is lo-  
11 cated;

12 “(iii) the district in which the depart-  
13 ment or agency of the Federal Government  
14 that disclosed the information is located; or

15 “(iv) the District of Columbia.

16 “(C) STATUTE OF LIMITATIONS.—No ac-  
17 tion shall lie under this subsection unless such  
18 action is commenced not later than two years  
19 after the date on which the cause of action  
20 arises.

21 “(D) EXCLUSIVE CAUSE OF ACTION.—A  
22 cause of action under this subsection shall be  
23 the exclusive means available to a complainant  
24 seeking a remedy for a violation of any restric-

1           tion specified in paragraph (3), (6), or 7(B) or  
2           any other provision of this section.

3           “(10) ANTI-TRUST EXEMPTION.—

4                   “(A) IN GENERAL.—Except as provided in  
5           subparagraph (C), it shall not be considered a  
6           violation of any provision of antitrust laws for  
7           two or more non-Federal entities to share a  
8           cyber threat indicator or defensive measure, or  
9           assistance relating to the prevention, investiga-  
10          tion, or mitigation of a cybersecurity risk or in-  
11          cident, for cybersecurity purposes under this  
12          Act.

13                   “(B) APPLICABILITY.—Subparagraph (A)  
14          shall apply only to information that is shared or  
15          assistance that is provided in order to assist  
16          with—

17                           “(i) facilitating the prevention, inves-  
18                           tigation, or mitigation of a cybersecurity  
19                           risk or incident to an information system  
20                           or information that is stored on, processed  
21                           by, or transiting an information system; or

22                           “(ii) communicating or disclosing a  
23                           cyber threat indicator or defensive measure  
24                           to help prevent, investigate, or mitigate the  
25                           effect of a cybersecurity risk or incident to



1           an information system or information that  
2           is stored on, processed by, or transiting an  
3           information system.

4           “(11) CONSTRUCTION AND PREEMPTION.—

5           “(A) OTHERWISE LAWFUL DISCLO-  
6           SURES.—Nothing in this section may be con-  
7           strued to limit or prohibit otherwise lawful dis-  
8           closures of communications, records, or other  
9           information, including reporting of known or  
10          suspected criminal activity or participating vol-  
11          untarily or under legal requirement in an inves-  
12          tigation, by a non-Federal to any other non-  
13          Federal entity or Federal entity under this sec-  
14          tion.

15          “(B) WHISTLE BLOWER PROTECTIONS.—  
16          Nothing in this section may be construed to  
17          prohibit or limit the disclosure of information  
18          protected under section 2302(b)(8) of title 5,  
19          United States Code (governing disclosures of il-  
20          legality, waste, fraud, abuse, or public health or  
21          safety threats), section 7211 of title 5, United  
22          States Code (governing disclosures to Con-  
23          gress), section 1034 of title 10, United States  
24          Code (governing disclosure to Congress by  
25          members of the military), section 1104 of the

1 National Security Act of 1947 (50 U.S.C.  
2 3234) (governing disclosure by employees of  
3 elements of the intelligence community), or any  
4 similar provision of Federal or State law.

5 “(C) RELATIONSHIP TO OTHER LAWS.—  
6 Nothing in this section may be construed to af-  
7 fect any requirement under any other provision  
8 of law for a non-Federal entity to provide infor-  
9 mation to a Federal entity.

10 “(D) PRESERVATION OF CONTRACTUAL  
11 OBLIGATIONS AND RIGHTS.—Nothing in this  
12 section may be construed to—

13 “(i) amend, repeal, or supersede any  
14 current or future contractual agreement,  
15 terms of service agreement, or other con-  
16 tractual relationship between any non-Fed-  
17 eral entities, or between any non-Federal  
18 entity and a Federal entity; or

19 “(ii) abrogate trade secret or intellec-  
20 tual property rights of any non-Federal en-  
21 tity or Federal entity.

22 “(E) ANTI-TASKING RESTRICTION.—Noth-  
23 ing in this section may be construed to permit  
24 a Federal entity to—

1           “(i) require a non-Federal entity to  
2           provide information to a Federal entity;

3           “(ii) condition the sharing of cyber  
4           threat indicators or defensive measures  
5           with a non-Federal entity on such non-  
6           Federal entity’s provision of cyber threat  
7           indicators or defensive measures to a Fed-  
8           eral entity; or

9           “(iii) condition the award of any Fed-  
10          eral grant, contract, or purchase on the  
11          sharing of cyber threat indicators or defen-  
12          sive measures with a Federal entity.

13          “(F) NO LIABILITY FOR NON-PARTICIPA-  
14          TION.—Nothing in this section may be con-  
15          strued to subject any non-Federal entity to li-  
16          ability for choosing to not engage in the vol-  
17          untary activities authorized under this section.

18          “(G) USE AND RETENTION OF INFORMA-  
19          TION.—Nothing in this section may be con-  
20          strued to authorize, or to modify any existing  
21          authority of, a department or agency of the  
22          Federal Government to retain or use any infor-  
23          mation shared under this section for any use  
24          other than permitted in this section.

1           “(H) VOLUNTARY SHARING.—Nothing in  
2 this section may be construed to restrict or con-  
3 dition a non-Federal entity from sharing, for  
4 cybersecurity purposes, cyber threat indicators,  
5 defensive measures, or information related to  
6 cybersecurity risks or incidents with any other  
7 non-Federal entity, and nothing in this section  
8 may be construed as requiring any non-Federal  
9 entity to share cyber threat indicators, defen-  
10 sive measures, or information related to cyber-  
11 security risks or incidents with the Center.

12           “(I) PROHIBITED CONDUCT.—Nothing in  
13 this section may be construed to permit price-  
14 fixing, allocating a market between competitors,  
15 monopolizing or attempting to monopolize a  
16 market, or exchanges of price or cost informa-  
17 tion, customer lists, or information regarding  
18 future competitive planning.

19           “(J) FEDERAL PREEMPTION.—This sec-  
20 tion supersedes any statute or other provision  
21 of law of a State or political subdivision of a  
22 State that restricts or otherwise expressly regu-  
23 lates an activity authorized under this section.

24           “(j) DIRECT REPORTING.—The Secretary shall de-  
25 velop policies and procedures for direct reporting to the

1 Secretary by the Director of the Center regarding signifi-  
2 cant cybersecurity risks and incidents.

3 “(k) ADDITIONAL RESPONSIBILITIES.—The Sec-  
4 retary shall build upon existing mechanisms to promote  
5 a national awareness effort to educate the general public  
6 on the importance of securing information systems.

7 “(l) REPORTS ON INTERNATIONAL COOPERATION.—  
8 Not later than 180 days after the date of the enactment  
9 of this subsection and periodically thereafter, the Sec-  
10 retary of Homeland Security shall submit to the Com-  
11 mittee on Homeland Security of the House of Representa-  
12 tives and the Committee on Homeland Security and Gov-  
13 ernmental Affairs of the Senate a report on the range of  
14 efforts underway to bolster cybersecurity collaboration  
15 with relevant international partners in accordance with  
16 subsection (e)(8).

17 “(m) OUTREACH.—Not later than 60 days after the  
18 date of the enactment of this subsection, the Secretary,  
19 acting through the Under Secretary for Cybersecurity and  
20 Infrastructure Protection, shall—

21 “(1) disseminate to the public information  
22 about how to voluntarily share cyber threat indica-  
23 tors and defensive measures with the Center; and

24 “(2) enhance outreach to critical infrastructure  
25 owners and operators for purposes of such sharing.”.

1 **SEC. 204. INFORMATION SHARING AND ANALYSIS ORGANI-**  
2 **ZATIONS.**

3 Section 212 of the Homeland Security Act of 2002  
4 (6 U.S.C. 131) is amended—

5 (1) in paragraph (5)—

6 (A) in subparagraph (A)—

7 (i) by inserting “and information re-  
8 lated to cybersecurity risks and incidents  
9 and” after “critical infrastructure informa-  
10 tion”; and

11 (ii) by striking “related to critical in-  
12 frastructure” and inserting “related to cy-  
13 bersecurity risks, incidents, critical infra-  
14 structure, and”;

15 (B) in subparagraph (B)—

16 (i) by striking “disclosing critical in-  
17 frastructure information” and inserting  
18 “disclosing cybersecurity risks, incidents,  
19 and critical infrastructure information”;  
20 and

21 (ii) by striking “related to critical in-  
22 frastructure or” and inserting “related to  
23 cybersecurity risks, incidents, critical infra-  
24 structure, or” and

25 (C) in subparagraph (C), by striking “dis-  
26 seminating critical infrastructure information”

1 and inserting “disseminating cybersecurity  
2 risks, incidents, and critical infrastructure in-  
3 formation”; and

4 (2) by adding at the end the following new  
5 paragraph:

6 “(8) CYBERSECURITY RISK; INCIDENT.—The  
7 terms ‘cybersecurity risk’ and ‘incident’ have the  
8 meanings given such terms in the second section 226  
9 (relating to the National Cybersecurity and Commu-  
10 nications Integration Center).”.

11 **SEC. 205. STREAMLINING OF DEPARTMENT OF HOMELAND**  
12 **SECURITY CYBERSECURITY AND INFRA-**  
13 **STRUCTURE PROTECTION ORGANIZATION.**

14 (a) CYBERSECURITY AND INFRASTRUCTURE PRO-  
15 TECTION.—The National Protection and Programs Direc-  
16 torate of the Department of Homeland Security shall,  
17 after the date of the enactment of this title, be known and  
18 designated as the “Cybersecurity and Infrastructure Pro-  
19 tection”. Any reference to the National Protection and  
20 Programs Directorate of the Department in any law, regu-  
21 lation, map, document, record, or other paper of the  
22 United States shall be deemed to be a reference to the  
23 Cybersecurity and Infrastructure Protection of the De-  
24 partment.

1 (b) SENIOR LEADERSHIP OF CYBERSECURITY AND  
2 INFRASTRUCTURE PROTECTION.—

3 (1) IN GENERAL.—Subsection (a) of section  
4 103 of the Homeland Security Act of 2002 (6  
5 U.S.C. 113) is amended—

6 (A) in paragraph (1)—

7 (i) by amending subparagraph (H) to  
8 read as follows:

9 “(H) An Under Secretary for Cyber-  
10 security and Infrastructure Protection.”;

11 and

12 (ii) by adding at the end the following  
13 new subparagraphs:

14 “(K) A Deputy Under Secretary for  
15 Cybersecurity.

16 “(L) A Deputy Under Secretary for  
17 Infrastructure Protection.”; and

18 (B) by adding at the end the following new  
19 paragraph:

20 “(3) DEPUTY UNDER SECRETARIES.—The Dep-  
21 uty Under Secretaries referred to in subparagraphs  
22 (K) and (L) of paragraph (1) shall be appointed by  
23 the President without the advice and consent of the  
24 Senate.”.



1           (2) CONTINUATION IN OFFICE.—The individ-  
2           uals who hold the positions referred in subpara-  
3           graphs (H), (K), and (L) of paragraph (1) of section  
4           103(a) the Homeland Security Act of 2002 (as  
5           amended and added by paragraph (1) of this sub-  
6           section) as of the date of the enactment of this title  
7           may continue to hold such positions.

8           (c) REPORT.—Not later than 90 days after the date  
9           of the enactment of this title, the Under Secretary for Cy-  
10          bersecurity and Infrastructure Protection of the Depart-  
11          ment of Homeland Security shall submit to the Committee  
12          on Homeland Security of the House of Representatives  
13          and the Committee on Homeland Security and Govern-  
14          mental Affairs of the Senate a report on the feasibility  
15          of becoming an operational component, including an anal-  
16          ysis of alternatives, and if a determination is rendered that  
17          becoming an operational component is the best option for  
18          achieving the mission of Cybersecurity and Infrastructure  
19          Protection, a legislative proposal and implementation plan  
20          for becoming such an operational component. Such report  
21          shall also include plans to more effectively carry out the  
22          cybersecurity mission of Cybersecurity and Infrastructure  
23          Protection, including expediting information sharing  
24          agreements.

1 **SEC. 206. CYBER INCIDENT RESPONSE PLANS.**

2 (a) IN GENERAL.—Section 227 of the Homeland Se-  
3 curity Act of 2002 (6 U.S.C. 149) is amended—

4 (1) in the heading, by striking “**PLAN**” and in-  
5 serting “**PLANS**”;

6 (2) by striking “The Under Secretary appointed  
7 under section 103(a)(1)(H) shall” and inserting the  
8 following:

9 “(a) IN GENERAL.—The Under Secretary for Cyber-  
10 security and Infrastructure Protection shall”; and

11 (3) by adding at the end the following new sub-  
12 section:

13 “(b) UPDATES TO THE CYBER INCIDENT ANNEX TO  
14 THE NATIONAL RESPONSE FRAMEWORK.—The Secretary,  
15 in coordination with the heads of other appropriate Fed-  
16 eral departments and agencies, and in accordance with the  
17 National Cybersecurity Incident Response Plan required  
18 under subsection (a), shall regularly update, maintain, and  
19 exercise the Cyber Incident Annex to the National Re-  
20 sponse Framework of the Department.”.

21 (b) CLERICAL AMENDMENT.—The table of contents  
22 of the Homeland Security Act of 2002 is amended by  
23 amending the item relating to section 227 to read as fol-  
24 lows:

“Sec. 227. Cyber incident response plans.”.

1 **SEC. 207. SECURITY AND RESILIENCY OF PUBLIC SAFETY**  
2 **COMMUNICATIONS; CYBERSECURITY AWARE-**  
3 **NESS CAMPAIGN.**

4 (a) IN GENERAL.—Subtitle C of title II of the Home-  
5 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-  
6 ed by adding at the end the following new sections:

7 **“SEC. 230. SECURITY AND RESILIENCY OF PUBLIC SAFETY**  
8 **COMMUNICATIONS.**

9 “The National Cybersecurity and Communications  
10 Integration Center, in coordination with the Office of  
11 Emergency Communications of the Department, shall as-  
12 sess and evaluate consequence, vulnerability, and threat  
13 information regarding cyber incidents to public safety  
14 communications to help facilitate continuous improve-  
15 ments to the security and resiliency of such communica-  
16 tions.

17 **“SEC. 231. CYBERSECURITY AWARENESS CAMPAIGN.**

18 “(a) IN GENERAL.—The Under Secretary for Cyber-  
19 security and Infrastructure Protection shall develop and  
20 implement an ongoing and comprehensive cybersecurity  
21 awareness campaign regarding cybersecurity risks and vol-  
22 untary best practices for mitigating and responding to  
23 such risks. Such campaign shall, at a minimum, publish  
24 and disseminate, on an ongoing basis, the following:

25 “(1) Public service announcements targeted at  
26 improving awareness among State, local, and tribal

1 governments, the private sector, academia, and  
2 stakeholders in specific audiences, including the el-  
3 derly, students, small businesses, members of the  
4 Armed Forces, and veterans.

5 “(2) Vendor and technology-neutral voluntary  
6 best practices information.

7 “(b) CONSULTATION.—The Under Secretary for Cy-  
8 bersecurity and Infrastructure Protection shall consult  
9 with a wide range of stakeholders in government, industry,  
10 academia, and the non-profit community in carrying out  
11 this section.

12 **“SEC. 232. NATIONAL CYBERSECURITY PREPAREDNESS**  
13 **CONSORTIUM.**

14 “(a) IN GENERAL.—The Secretary may establish a  
15 consortium to be known as the ‘National Cybersecurity  
16 Preparedness Consortium’ (in this section referred to as  
17 the ‘Consortium’).

18 “(b) FUNCTIONS.—The Consortium may—

19 “(1) provide training to State and local first re-  
20 sponders and officials specifically for preparing and  
21 responding to cyber attacks;

22 “(2) develop and update a curriculum utilizing  
23 the National Protection and Programs Directorate  
24 of the Department sponsored Community Cyber Se-

1 security Maturity Model (CCSMM) for State and local  
2 first responders and officials;

3 “(3) provide technical assistance services to  
4 build and sustain capabilities in support of cyberse-  
5 curity preparedness and response;

6 “(4) conduct cybersecurity training and simula-  
7 tion exercises to defend from and respond to cyber-  
8 attacks;

9 “(5) coordinate with the National Cybersecurity  
10 and Communications Integration Center to help  
11 States and communities develop cybersecurity infor-  
12 mation sharing programs; and

13 “(6) coordinate with the National Domestic  
14 Preparedness Consortium to incorporate cybersecu-  
15 rity emergency responses into existing State and  
16 local emergency management functions.

17 “(c) MEMBERS.—The Consortium shall consist of  
18 academic, nonprofit, and government partners that de-  
19 velop, update, and deliver cybersecurity training in sup-  
20 port of homeland security. Members shall have prior expe-  
21 rience conducting cybersecurity training and exercises for  
22 State and local entities.”.

23 (b) CLERICAL AMENDMENT.—The table of contents  
24 of the Homeland Security Act of 2002 is amended by in-  
25 serting after the item relating to section 226 (relating to

1 cybersecurity recruitment and retention) the following new  
2 items:

“Sec. 230. Security and resiliency of public safety communications.

“Sec. 231. Cybersecurity awareness campaign.

“Sec. 232. National Cybersecurity Preparedness Consortium.”.

3 **SEC. 208. CRITICAL INFRASTRUCTURE PROTECTION RE-**  
4 **SEARCH AND DEVELOPMENT.**

5 (a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSOR-  
6 TIUMS.—Title III of the Homeland Security Act of 2002  
7 (6 U.S.C. 181 et seq.) is amended by adding at the end  
8 the following new section:

9 **“SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR**  
10 **CRITICAL INFRASTRUCTURE PROTECTION.**

11 “(a) IN GENERAL.—Not later than 180 days after  
12 the date of enactment of this section, the Secretary, acting  
13 through the Under Secretary for Science and Technology,  
14 shall submit to Congress a strategic plan to guide the  
15 overall direction of Federal physical security and cyberse-  
16 curity technology research and development efforts for  
17 protecting critical infrastructure, including against all  
18 threats. Such plan shall be updated and submitted to Con-  
19 gress every two years.

20 “(b) CONTENTS OF PLAN.—The strategic plan, in-  
21 cluding biennial updates, required under subsection (a)  
22 shall include the following:

1           “(1) An identification of critical infrastructure  
2 security risks and any associated security technology  
3 gaps, that are developed following:

4                   “(A) Consultation with stakeholders, in-  
5 cluding critical infrastructure Sector Coordi-  
6 nating Councils.

7                   “(B) Performance by the Department of a  
8 risk and gap analysis that considers informa-  
9 tion received in such consultations.

10           “(2) A set of critical infrastructure security  
11 technology needs that—

12                   “(A) is prioritized based on the risks and  
13 gaps identified under paragraph (1);

14                   “(B) emphasizes research and development  
15 of technologies that need to be accelerated due  
16 to rapidly evolving threats or rapidly advancing  
17 infrastructure technology; and

18                   “(C) includes research, development, and  
19 acquisition roadmaps with clearly defined objec-  
20 tives, goals, and measures.

21           “(3) An identification of laboratories, facilities,  
22 modeling, and simulation capabilities that will be re-  
23 quired to support the research, development, dem-  
24 onstration, testing, evaluation, and acquisition of the  
25 security technologies described in paragraph (2).

1           “(4) An identification of current and planned  
2           programmatic initiatives for fostering the rapid ad-  
3           vancement and deployment of security technologies  
4           for critical infrastructure protection, including a  
5           consideration of opportunities for public-private  
6           partnerships, intragovernment collaboration, univer-  
7           sity centers of excellence, and national laboratory  
8           technology transfer.

9           “(5) A description of progress made with re-  
10          spect to each critical infrastructure security risk, as-  
11          sociated security technology gap, and critical infra-  
12          structure technology need identified in the preceding  
13          strategic plan required under subsection (a).

14          “(c) COORDINATION.—In carrying out this section,  
15          the Under Secretary for Science and Technology shall co-  
16          ordinate with the Under Secretary for the National Pro-  
17          tection and Programs Directorate.

18          “(d) CONSULTATION.—In carrying out this section,  
19          the Under Secretary for Science and Technology shall con-  
20          sult with—

21                 “(1) critical infrastructure Sector Coordinating  
22                 Councils;

23                 “(2) to the extent practicable, subject matter  
24                 experts on critical infrastructure protection from



1 universities, colleges, national laboratories, and pri-  
2 vate industry;

3 “(3) the heads of other relevant Federal depart-  
4 ments and agencies that conduct research and devel-  
5 opment relating to critical infrastructure protection;  
6 and

7 “(4) State, local, and tribal governments, as ap-  
8 propriate.”.

9 (b) CLERICAL AMENDMENT.—The table of contents  
10 of the Homeland Security Act of 2002 is amended by in-  
11 serting after the item relating to section 317 the following  
12 new item:

“Sec. 318. Research and development strategy for critical infrastructure protec-  
tion.”.

13 **SEC. 209. REPORT ON REDUCING CYBERSECURITY RISKS IN**  
14 **DHS DATA CENTERS.**

15 Not later than 1 year after the date of the enactment  
16 of this title, the Secretary of Homeland Security shall sub-  
17 mit to the Committee on Homeland Security of the House  
18 of Representatives and the Committee on Homeland Secu-  
19 rity and Governmental Affairs of the Senate a report on  
20 the feasibility of the Department of Homeland Security  
21 creating an environment for the reduction in cybersecurity  
22 risks in Department data centers, including by increasing  
23 compartmentalization between systems, and providing a  
24 mix of security controls between such compartments.

1 **SEC. 210. ASSESSMENT.**

2 Not later than 2 years after the date of the enact-  
3 ment of this title, the Comptroller General of the United  
4 States shall submit to the Committee on Homeland Secu-  
5 rity of the House of Representatives and the Committee  
6 on Homeland Security and Governmental Affairs of the  
7 Senate a report that contains an assessment of the imple-  
8 mentation by the Secretary of Homeland Security of this  
9 title and the amendments made by this title and, to the  
10 extent practicable, findings regarding increases in the  
11 sharing of cyber threat indicators, defensive measures,  
12 and information relating to cybersecurity risks and inci-  
13 dents at the National Cybersecurity and Communications  
14 Integration Center and throughout the United States.

15 **SEC. 211. CONSULTATION.**

16 The Under Secretary for Cybersecurity and Infra-  
17 structure Protection shall produce a report on the feasi-  
18 bility of creating a risk-informed prioritization plan should  
19 multiple critical infrastructures experience cyber incidents  
20 simultaneously.

21 **SEC. 212. TECHNICAL ASSISTANCE.**

22 The Inspector General of the Department of Home-  
23 land Security shall review the operations of the United  
24 States Computer Emergency Readiness Team (US-  
25 CERT) and the Industrial Control Systems Cyber Emer-  
26 gency Response Team (ICS-CERT) to assess the capacity

1 to provide technical assistance to non-Federal entities and  
2 to adequately respond to potential increases in requests  
3 for technical assistance.

4 **SEC. 213. PROHIBITION ON NEW REGULATORY AUTHORITY.**

5       Nothing in this title or the amendments made by this  
6 title may be construed to grant the Secretary of Homeland  
7 Security any authority to promulgate regulations or set  
8 standards relating to the cybersecurity of non-Federal en-  
9 tities, not including State, local, and tribal governments,  
10 that was not in effect on the day before the date of the  
11 enactment of this title.

12 **SEC. 214. SUNSET.**

13       Any requirements for reports required by this title  
14 or the amendments made by this title shall terminate on  
15 the date that is 7 years after the date of the entitlement  
16 of this title.

17 **SEC. 215. PROHIBITION ON NEW FUNDING.**

18       No funds are authorized to be appropriated to carry  
19 out this title and the amendments made by this title. This  
20 title and such amendments shall be carried out using  
21 amounts appropriated or otherwise made available for  
22 such purposes.

1 **SEC. 216. PROTECTION OF FEDERAL INFORMATION SYS-**  
2 **TEMS.**

3 (a) IN GENERAL.—Subtitle C of title II of the Home-  
4 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-  
5 ed by adding at the end the following new section:

6 **“SEC. 233. AVAILABLE PROTECTION OF FEDERAL INFORMA-**  
7 **TION SYSTEMS.**

8 “(a) IN GENERAL.—The Secretary shall deploy and  
9 operate, to make available for use by any Federal agency,  
10 with or without reimbursement, capabilities to protect  
11 Federal agency information and information systems, in-  
12 cluding technologies to continuously diagnose, detect, pre-  
13 vent, and mitigate against cybersecurity risks (as such  
14 term is defined in the second section 226) involving Fed-  
15 eral agency information or information systems.

16 “(b) ACTIVITIES.—In carrying out this section, the  
17 Secretary may—

18 “(1) access, and Federal agency heads may dis-  
19 close to the Secretary or a private entity providing  
20 assistance to the Secretary under paragraph (2), in-  
21 formation traveling to or from or stored on a Fed-  
22 eral agency information system, regardless of from  
23 where the Secretary or a private entity providing as-  
24 sistance to the Secretary under paragraph (2) ac-  
25 cesses such information, notwithstanding any other  
26 provision of law that would otherwise restrict or pre-

1 vent Federal agency heads from disclosing such in-  
2 formation to the Secretary or a private entity pro-  
3 viding assistance to the Secretary under paragraph  
4 (2);

5 “(2) enter into contracts or other agreements,  
6 or otherwise request and obtain the assistance of,  
7 private entities to deploy and operate technologies in  
8 accordance with subsection (a); and

9 “(3) retain, use, and disclose information ob-  
10 tained through the conduct of activities authorized  
11 under this section only to protect Federal agency in-  
12 formation and information systems from cybersecu-  
13 rity risks, or, with the approval of the Attorney Gen-  
14 eral and if disclosure of such information is not oth-  
15 erwise prohibited by law, to law enforcement only to  
16 investigate, prosecute, disrupt, or otherwise respond  
17 to—

18 “(A) a violation of section 1030 of title 18,  
19 United States Code;

20 “(B) an imminent threat of death or seri-  
21 ous bodily harm;

22 “(C) a serious threat to a minor, including  
23 sexual exploitation or threats to physical safety;

24 or

1           “(D) an attempt, or conspiracy, to commit  
2           an offense described in any of subparagraphs  
3           (A) through (C).

4           “(c) CONDITIONS.—Contracts or other agreements  
5           under subsection (b)(2) shall include appropriate provi-  
6           sions barring—

7           “(1) the disclosure of information to any entity  
8           other than the Department or the Federal agency  
9           disclosing information in accordance with subsection  
10          (b)(1) that can be used to identify specific persons  
11          and is reasonably believed to be unrelated to a cy-  
12          bersecurity risk; and

13          “(2) the use of any information to which such  
14          private entity gains access in accordance with this  
15          section for any purpose other than to protect Fed-  
16          eral agency information and information systems  
17          against cybersecurity risks or to administer any such  
18          contract or other agreement.

19          “(d) LIMITATION.—No cause of action shall lie  
20          against a private entity for assistance provided to the Sec-  
21          retary in accordance with this section and a contract or  
22          agreement under subsection (b)(2).”.

23          (b) CLERICAL AMENDMENT.—The table of contents  
24          of the Homeland Security Act of 2002 is amended by in-  
25          serting after the item relating to section 226 (relating to

1 cybersecurity recruitment and retention) the following new  
2 item:

“Sec. 233. Available protection of Federal information systems.”.

3 **SEC. 217. SUNSET.**

4 This title and the amendments made by this title  
5 shall terminate on the date that is 7 years after the date  
6 of the enactment of this title.

7 **SEC. 218. REPORT ON CYBERSECURITY VULNERABILITIES**  
8 **OF UNITED STATES PORTS.**

9 Not later than 180 days after the date of the enact-  
10 ment of this title, the Secretary of Homeland Security  
11 shall submit to the Committee on Homeland Security and  
12 the Committee on Transportation and Infrastructure of  
13 the House of Representatives and the Committee on  
14 Homeland Security and Governmental Affairs and the  
15 Committee on Commerce, Science and Transportation of  
16 the Senate a report on cybersecurity vulnerabilities for the  
17 ten United States ports that the Secretary determines are  
18 at greatest risk of a cybersecurity incident and provide  
19 recommendations to mitigate such vulnerabilities.

20 **SEC. 219. REPORT ON CYBERSECURITY AND CRITICAL IN-**  
21 **FRASTRUCTURE.**

22 The Secretary of Homeland Security may consult  
23 with sector specific agencies, businesses, and stakeholders  
24 to produce and submit to the Committee on Homeland Se-  
25 curity of the House of Representatives and the Committee

1 on Homeland Security and Governmental Affairs of the  
2 Senate a report on how best to align federally funded cy-  
3 bersecurity research and development activities with pri-  
4 vate sector efforts to protect privacy and civil liberties  
5 while assuring security and resilience of the Nation's crit-  
6 ical infrastructure, including—

7           (1) promoting research and development to en-  
8           able the secure and resilient design and construction  
9           of critical infrastructure and more secure accom-  
10          panying cyber technology;

11          (2) enhancing modeling capabilities to deter-  
12          mine potential impacts on critical infrastructure of  
13          incidents or threat scenarios, and cascading effects  
14          on other sectors; and

15          (3) facilitating initiatives to incentivize cyberse-  
16          curity investments and the adoption of critical infra-  
17          structure design features that strengthen cybersecu-  
18          rity and resilience.

19 **SEC. 220. GAO REPORT ON IMPACT PRIVACY AND CIVIL LIB-**  
20 **ERTIES.**

21           Not later than 60 months after the date of the enact-  
22          ment of this title, the Comptroller General of the United  
23          States shall submit to the Committee on Homeland Secu-  
24          rity of the House of Representatives and the Committee  
25          on Homeland Security and Governmental Affairs of the



- 1 Senate an assessment on the impact on privacy and civil
- 2 liberties limited to the work of the National Cybersecurity
- 3 and Communications Integration Center.

Passed the House of Representatives April 22, 2015.

Attest:

KAREN L. HAAS,

*Clerk.*