

Union Calendar No. 44

114TH CONGRESS
1ST SESSION

H. R. 1560

[Report No. 114-63]

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 24, 2015

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

APRIL 13, 2015

Additional sponsors: Mr. KING of New York, Mr. LOBIONDO, Ms. SEWELL of Alabama, Mr. QUIGLEY, and Mr. MURPHY of Florida

APRIL 13, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italic*]

[For text of introduced bill, see copy of bill as introduced on March 24, 2015]

A BILL

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

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

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

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

6 (b) *TABLE OF CONTENTS.*—*The table of contents of this*
 7 *Act is as follows:*

Sec. 1. Short title; table of contents.

Sec. 2. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.

Sec. 3. Authorizations for preventing, detecting, analyzing, and mitigating cyber-security threats.

Sec. 4. Sharing of cyber threat indicators and defensive measures with appropriate Federal entities other than the Department of Defense or the National Security Agency.

Sec. 5. Federal Government liability for violations of privacy or civil liberties.

Sec. 6. Protection from liability.

Sec. 7. Oversight of Government activities.

Sec. 8. Report on cybersecurity threats.

Sec. 9. Construction and preemption.

Sec. 10. Conforming amendments.

Sec. 11. Definitions.

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

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

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

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

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

8 “(A) *the timely sharing of classified cyber*
9 *threat indicators in the possession of the Federal*
10 *Government with representatives of relevant non-*
11 *Federal entities with appropriate security clear-*
12 *ances;*

13 “(B) *the timely sharing with relevant non-*
14 *Federal entities of cyber threat indicators in the*
15 *possession of the Federal Government that may*
16 *be declassified and shared at an unclassified*
17 *level; and*

18 “(C) *the sharing with non-Federal entities,*
19 *if appropriate, of information in the possession*
20 *of the Federal Government about imminent or*
21 *ongoing cybersecurity threats to such entities to*
22 *prevent or mitigate adverse impacts from such*
23 *cybersecurity threats.*

1 “(2) *DEVELOPMENT OF PROCEDURES.*—*The pro-*
2 *cedures developed and promulgated under paragraph*
3 *(1) shall—*

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

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

14 “(C) *include procedures for notifying non-*
15 *Federal entities that have received a cyber threat*
16 *indicator from a Federal entity in accordance*
17 *with this Act that is known or determined to be*
18 *in error or in contravention of the requirements*
19 *of this section, the Protecting Cyber Networks*
20 *Act, or the amendments made by such Act or an-*
21 *other provision of Federal law or policy of such*
22 *error or contravention;*

23 “(D) *include requirements for Federal enti-*
24 *ties receiving a cyber threat indicator or defen-*
25 *sive measure to implement appropriate security*

1 *controls to protect against unauthorized access*
2 *to, or acquisition of, such cyber threat indicator*
3 *or defensive measure;*

4 “(E) include procedures that require Fed-
5 *eral entities, prior to the sharing of a cyber*
6 *threat indicator, to—*

7 “(i) review such cyber threat indicator
8 *to assess whether such cyber threat indi-*
9 *cator, in contravention of the requirement*
10 *under section 3(d)(2) of the Protecting*
11 *Cyber Networks Act, contains any informa-*
12 *tion that such Federal entity knows at the*
13 *time of sharing to be personal information*
14 *of or information identifying a specific per-*
15 *son not directly related to a cybersecurity*
16 *threat and remove such information; or*

17 “(ii) implement a technical capability
18 *configured to remove or exclude any per-*
19 *sonal information of or information identi-*
20 *fying a specific person not directly related*
21 *to a cybersecurity threat; and*

22 “(F) include procedures to promote the effi-
23 *cient granting of security clearances to appro-*
24 *priate representatives of non-Federal entities.*

1 “(b) *DEFINITIONS.*—*In this section, the terms ‘appropriate Federal entities’, ‘cyber threat indicator’, ‘defensive*
2 *measure’, ‘Federal entity’, and ‘non-Federal entity’ have the*
3 *meaning given such terms in section 11 of the Protecting*
4 *Cyber Networks Act.’”.*

6 (b) *SUBMITTAL TO CONGRESS.*—*Not later than 90*
7 *days after the date of the enactment of this Act, the Director*
8 *of National Intelligence, in consultation with the heads of*
9 *the other appropriate Federal entities, shall submit to Con-*
10 *gress the procedures required by section 111(a) of the Na-*
11 *tional Security Act of 1947, as inserted by subsection (a)*
12 *of this section.*

13 (c) *TABLE OF CONTENTS AMENDMENT.*—*The table of*
14 *contents in the first section of the National Security Act*
15 *of 1947 is amended by inserting after the item relating to*
16 *section 110 the following new item:*

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

17 **SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
18 **ANALYZING, AND MITIGATING CYBERSECURITY**
19 **THREATS.**

20 (a) *AUTHORIZATION FOR PRIVATE-SECTOR DEFEN-*
21 *SIVE MONITORING.*—

22 (1) *IN GENERAL.*—*Notwithstanding any other*
23 *provision of law, a private entity may, for a cyberse-*
24 *curity purpose, monitor—*

1 (A) an information system of such private
2 entity;

3 (B) an information system of a non-Federal
4 entity or a Federal entity, upon the written au-
5 thorization of such non-Federal entity or such
6 Federal entity; and

7 (C) information that is stored on, processed
8 by, or transiting an information system mon-
9 itored by the private entity under this para-
10 graph.

11 (2) CONSTRUCTION.—Nothing in this subsection
12 shall be construed to—

13 (A) authorize the monitoring of an informa-
14 tion system, or the use of any information ob-
15 tained through such monitoring, other than as
16 provided in this Act;

17 (B) authorize the Federal Government to
18 conduct surveillance of any person; or

19 (C) limit otherwise lawful activity.

20 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE
21 MEASURES.—

22 (1) IN GENERAL.—Except as provided in para-
23 graph (2) and notwithstanding any other provision of
24 law, a private entity may, for a cybersecurity pur-

1 *pose, operate a defensive measure that is operated on*
2 *and is limited to—*

3 *(A) an information system of such private*
4 *entity to protect the rights or property of the pri-*
5 *vate entity; and*

6 *(B) an information system of a non-Federal*
7 *entity or a Federal entity upon written author-*
8 *ization of such non-Federal entity or such Fed-*
9 *eral entity for operation of such defensive meas-*
10 *ure to protect the rights or property of such pri-*
11 *vate entity, such non-Federal entity, or such*
12 *Federal entity.*

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

21 *(A) the private entity operating such defen-*
22 *sive measure; or*

23 *(B) a non-Federal entity or a Federal enti-*
24 *ty that has provided written authorization to*
25 *that private entity for operation of such defen-*

1 *sive measure on the information system or infor-*
2 *mation of the entity in accordance with this sub-*
3 *section.*

4 (3) *CONSTRUCTION.*—*Nothing in this subsection*
5 *shall be construed—*

6 (A) *to authorize the use of a defensive meas-*
7 *ure other than as provided in this subsection; or*

8 (B) *to limit otherwise lawful activity.*

9 (c) *AUTHORIZATION FOR SHARING OR RECEIVING*
10 *CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.*—

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

19 (A) *share a lawfully obtained cyber threat*
20 *indicator or defensive measure with any other*
21 *non-Federal entity or an appropriate Federal*
22 *entity (other than the Department of Defense or*
23 *any component of the Department, including the*
24 *National Security Agency); and*

1 (B) receive a cyber threat indicator or de-
2 fensive measure from any other non-Federal enti-
3 ty or an appropriate Federal entity.

4 (2) *LAWFUL RESTRICTION.*—A non-Federal enti-
5 ty receiving a cyber threat indicator or defensive
6 measure from another non-Federal entity or a Federal
7 entity shall comply with otherwise lawful restrictions
8 placed on the sharing or use of such cyber threat indi-
9 cator or defensive measure by the sharing non-Federal
10 entity or Federal entity.

11 (3) *CONSTRUCTION.*—Nothing in this subsection
12 shall be construed to—

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

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

19 (C) prohibit any Federal entity from engag-
20 ing in formal or informal technical discussion
21 regarding cyber threat indicators or defensive
22 measures with a non-Federal entity or from pro-
23 viding technical assistance to address
24 vulnerabilities or mitigate threats at the request
25 of such an entity;

1 (D) limit otherwise lawful activity;

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

8 (F) authorize the Federal Government to
9 conduct surveillance of any person.

10 (d) *PROTECTION AND USE OF INFORMATION.*—

11 (1) *SECURITY OF INFORMATION.*—A non-Federal
12 entity monitoring an information system, operating a
13 defensive measure, or providing or receiving a cyber
14 threat indicator or defensive measure under this sec-
15 tion shall implement an appropriate security control
16 to protect against unauthorized access to, or acquisi-
17 tion of, such cyber threat indicator or defensive meas-
18 ure.

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

23 (A) review such cyber threat indicator to as-
24 sess whether such cyber threat indicator contains
25 any information that the non-Federal entity rea-

1 *sonably believes at the time of sharing to be per-*
2 *sonal information of or information identifying*
3 *a specific person not directly related to a cyber-*
4 *security threat and remove such information; or*

5 *(B) implement a technical capability con-*
6 *figured to remove any information contained*
7 *within such indicator that the non-Federal enti-*
8 *ty reasonably believes at the time of sharing to*
9 *be personal information of or information identi-*
10 *fying a specific person not directly related to a*
11 *cybersecurity threat.*

12 *(3) USE OF CYBER THREAT INDICATORS AND DE-*
13 *FENSIVE MEASURES BY NON-FEDERAL ENTITIES.—A*
14 *non-Federal entity may, for a cybersecurity pur-*
15 *pose—*

16 *(A) use a cyber threat indicator or defensive*
17 *measure shared or received under this section to*
18 *monitor or operate a defensive measure on—*

19 *(i) an information system of such non-*
20 *Federal entity; or*

21 *(ii) an information system of another*
22 *non-Federal entity or a Federal entity upon*
23 *the written authorization of that other non-*
24 *Federal entity or that Federal entity; and*

1 (B) otherwise use, retain, and further share
2 such cyber threat indicator or defensive measure
3 subject to—

4 (i) an otherwise lawful restriction
5 placed by the sharing non-Federal entity or
6 Federal entity on such cyber threat indi-
7 cator or defensive measure; or

8 (ii) an otherwise applicable provision
9 of law.

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

12 (A) *LAW ENFORCEMENT USE.—*A State,
13 tribal, or local government may use a cyber
14 threat indicator shared with such State, tribal,
15 or local government for the purposes described in
16 clauses (i), (ii), and (iii) of section 4(d)(5)(A).

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

21 (i) deemed voluntarily shared informa-
22 tion; and

23 (ii) exempt from disclosure under any
24 State, tribal, or local law requiring disclo-
25 sure of information or records, except as

1 *otherwise required by applicable State, trib-*
2 *al, or local law requiring disclosure in any*
3 *criminal prosecution.*

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

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

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

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

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

20 *(B) by inserting after subsection (a) the fol-*
21 *lowing new subsection:*

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

1 “(1) *ESTABLISHMENT.*—*The President shall de-*
2 *velop and submit to Congress policies and procedures*
3 *relating to the receipt of cyber threat indicators and*
4 *defensive measures by the Federal Government.*

5 “(2) *REQUIREMENTS CONCERNING POLICIES AND*
6 *PROCEDURES.*—*The policies and procedures required*
7 *under paragraph (1) shall—*

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

12 “(B) *ensure that—*

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

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

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

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

7 “(C) *ensure there—*

8 “(i) *is an audit capability; and*

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

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

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

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

4 (b) *PRIVACY AND CIVIL LIBERTIES.*—

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

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

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

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

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

9 *(i) a process for the prompt destruction*
10 *of such information that is known not to be*
11 *directly related to a use for a cybersecurity*
12 *purpose;*

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

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

19 *(C) include requirements to safeguard cyber*
20 *threat indicators containing personal informa-*
21 *tion of or identifying specific persons from un-*
22 *authorized access or acquisition, including ap-*
23 *propriate sanctions for activities by officers, em-*
24 *ployees, or agents of the Federal Government in*
25 *contravention of such guidelines;*

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

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

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

18 (3) SUBMISSION.—The Attorney General shall
19 submit to Congress—

20 (A) not later than 90 days after the date of
21 the enactment of this Act, interim guidelines re-
22 quired under paragraph (1); and

23 (B) not later than 180 days after such date,
24 final guidelines required under such paragraph.

1 (c) *NATIONAL CYBER THREAT INTELLIGENCE INTE-*
2 *GRATION CENTER.*—

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

7 (A) *by redesignating section 119B as section*
8 *119C; and*

9 (B) *by inserting after section 119A the fol-*
10 *lowing new section:*

11 **“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION**
12 **CENTER.**

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

16 “(b) *DIRECTOR.*—*There is a Director of the Cyber*
17 *Threat Intelligence Integration Center, who shall be the*
18 *head of the Cyber Threat Intelligence Integration Center,*
19 *and who shall be appointed by the Director of National In-*
20 *telligence.*

21 “(c) *PRIMARY MISSIONS.*—*The Cyber Threat Intel-*
22 *ligence Integration Center shall—*

23 “(1) *serve as the primary organization within*
24 *the Federal Government for analyzing and inte-*

1 *grating all intelligence possessed or acquired by the*
2 *United States pertaining to cyber threats;*

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

8 *“(3) disseminate cyber threat analysis to the*
9 *President, the appropriate departments and agencies*
10 *of the Federal Government, and the appropriate com-*
11 *mittees of Congress;*

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

15 *“(5) conduct strategic cyber threat intelligence*
16 *planning for the Federal Government.*

17 *“(d) LIMITATIONS.—The Cyber Threat Intelligence In-*
18 *tegration Center shall—*

19 *“(1) have not more than 50 permanent positions;*

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

1 “(3) be located in a building owned or operated
2 by an element of the intelligence community as of the
3 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 2 of this
7 Act, is further amended by striking the item relating
8 to section 119B and inserting the following new
9 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 Act 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 section 3(c)(2), a cyber threat indicator or defen-*
20 *sive measure provided by a non-Federal entity to the*
21 *Federal Government under this Act shall be consid-*
22 *ered the commercial, financial, and proprietary infor-*
23 *mation 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 enti-*
2 *ty or a non-Federal entity acting in accordance with*
3 *the written authorization of the non-Federal entity*
4 *that is the originator of such cyber threat indicator*
5 *or defensive measure.*

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

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

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

22 (4) *EX PARTE COMMUNICATIONS.—The provision*
23 *of a cyber threat indicator or defensive measure to the*
24 *Federal Government under this Act shall not be sub-*
25 *ject to a rule of any Federal department or agency or*

1 *any judicial doctrine regarding ex parte communica-*
2 *tions with a decision-making official.*

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

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

12 (i) *a cybersecurity purpose;*

13 (ii) *the purpose of responding to, pros-*
14 *ecuting, or otherwise preventing or miti-*
15 *gating a threat of death or serious bodily*
16 *harm or an offense arising out of such a*
17 *threat;*

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

22 (iv) *the purpose of preventing, inves-*
23 *tigating, disrupting, or prosecuting any of*
24 *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 to
5 the Federal Government under this Act shall not
6 be disclosed to, retained by, or used by any Fed-
7 eral department or agency for any use not per-
8 mitted 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 Act
12 shall be retained, used, and disseminated by the
13 Federal Government in accordance with—

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

20 (ii) the privacy and civil liberties
21 guidelines required by subsection (b).

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

24 (a) *IN GENERAL.*—If a department or agency of the
25 Federal Government intentionally or willfully violates the

1 *privacy and civil liberties guidelines issued by the Attorney*
2 *General under section 4(b), the United States shall be liable*
3 *to a person injured by such violation in an amount equal*
4 *to the sum of—*

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

8 (2) *reasonable attorney fees as determined by the*
9 *court and other litigation costs reasonably incurred*
10 *in any case under this subsection in which the com-*
11 *plainant has substantially prevailed.*

12 (b) *VENUE.—An action to enforce liability created*
13 *under this section may be brought in the district court of*
14 *the United States in—*

15 (1) *the district in which the complainant resides;*

16 (2) *the district in which the principal place of*
17 *business of the complainant is located;*

18 (3) *the district in which the department or agen-*
19 *cy of the Federal Government that violated such pri-*
20 *vacy and civil liberties guidelines is located; or*

21 (4) *the District of Columbia.*

22 (c) *STATUTE OF LIMITATIONS.—No action shall lie*
23 *under this subsection unless such action is commenced not*
24 *later than two years after the date of the violation of the*

1 *privacy and civil liberties guidelines issued by the Attorney*
2 *General under section 4(b) that is the basis for the action.*

3 (d) *EXCLUSIVE CAUSE OF ACTION.*—*A cause of action*
4 *under this subsection shall be the exclusive means available*
5 *to a complainant seeking a remedy for a violation by a*
6 *department or agency of the Federal Government under this*
7 *Act.*

8 **SEC. 6. PROTECTION FROM LIABILITY.**

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

16 (b) *SHARING OR RECEIPT OF CYBER THREAT INDICA-*
17 *TORS.*—*No cause of action shall lie or be maintained in*
18 *any court against any non-Federal entity, and such action*
19 *shall be promptly dismissed, for the sharing or receipt of*
20 *a cyber threat indicator or defensive measure under section*
21 *3(c), or a good faith failure to act based on such sharing*
22 *or receipt, if such sharing or receipt is conducted in good*
23 *faith in accordance with this Act and the amendments made*
24 *by this Act.*

25 (c) *WILLFUL MISCONDUCT.*—

1 (1) *RULE OF CONSTRUCTION.*—*Nothing in this*
2 *section shall be construed—*

3 (A) *to require dismissal of a cause of action*
4 *against a non-Federal entity (including a pri-*
5 *ivate entity) that has engaged in willful mis-*
6 *conduct in the course of conducting activities au-*
7 *thorized by this Act or the amendments made by*
8 *this Act; or*

9 (B) *to undermine or limit the availability*
10 *of otherwise applicable common law or statutory*
11 *defenses.*

12 (2) *PROOF OF WILLFUL MISCONDUCT.*—*In any*
13 *action claiming that subsection (a) or (b) does not*
14 *apply due to willful misconduct described in para-*
15 *graph (1), the plaintiff shall have the burden of prov-*
16 *ing by clear and convincing evidence the willful mis-*
17 *conduct by each non-Federal entity subject to such*
18 *claim and that such willful misconduct proximately*
19 *caused injury to the plaintiff.*

20 (3) *WILLFUL MISCONDUCT DEFINED.*—*In this*
21 *subsection, the term “willful misconduct” means an*
22 *act or omission that is taken—*

23 (A) *intentionally to achieve a wrongful pur-*
24 *pose;*

1 (B) knowingly without legal or factual jus-
2 tification; and

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

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

7 (a) *BIENNIAL REPORT ON IMPLEMENTATION.*—

8 (1) *IN GENERAL.*—Section 111 of the National
9 Security Act of 1947, as added by section 2(a) and
10 amended by section 4(a) of this Act, is further amend-
11 ed—

12 (A) by redesignating subsection (c) (as re-
13 designated by such section 4(a)) as subsection
14 (d); and

15 (B) by inserting after subsection (b) (as in-
16 serted by such section 4(a)) the following new
17 subsection:

18 “(c) *BIENNIAL REPORT ON IMPLEMENTATION.*—

19 “(1) *IN GENERAL.*—Not less frequently than once
20 every two years, the Director of National Intelligence,
21 in consultation with the heads of the other appro-
22 priate Federal entities, shall submit to Congress a re-
23 port concerning the implementation of this section
24 and the Protecting Cyber Networks Act.

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

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

9 “(B) *An assessment of whether the proce-*
10 *dures developed under section 3 of such Act com-*
11 *ply with the goals described in subparagraphs*
12 *(A), (B), and (C) of subsection (a)(1).*

13 “(C) *An assessment of whether cyber threat*
14 *indicators have been properly classified and an*
15 *accounting of the number of security clearances*
16 *authorized by the Federal Government for the*
17 *purposes of this section and such Act.*

18 “(D) *A review of the type of cyber threat in-*
19 *dicators shared with the Federal Government*
20 *under this section and such Act, including the*
21 *following:*

22 “(i) *The degree to which such informa-*
23 *tion may impact the privacy and civil lib-*
24 *erties of specific persons.*

1 “(ii) *A quantitative and qualitative*
2 *assessment of the impact of the sharing of*
3 *such cyber threat indicators with the Fed-*
4 *eral Government on privacy and civil lib-*
5 *erties of specific persons.*

6 “(iii) *The adequacy of any steps taken*
7 *by the Federal Government to reduce such*
8 *impact.*

9 “(E) *A review of actions taken by the Fed-*
10 *eral Government based on cyber threat indicators*
11 *shared with the Federal Government under this*
12 *section or such Act, including the appropriate-*
13 *ness of any subsequent use or dissemination of*
14 *such cyber threat indicators by a Federal entity*
15 *under this section or section 4 of such Act.*

16 “(F) *A description of any significant viola-*
17 *tions of the requirements of this section or such*
18 *Act by the Federal Government—*

19 “(i) *an assessment of all reports of offi-*
20 *cers, employees, and agents of the Federal*
21 *Government misusing information provided*
22 *to the Federal Government under the Pro-*
23 *tecting Cyber Networks Act or this section,*
24 *without regard to whether the misuse was*
25 *knowing or wilful; and*

1 “(ii) an assessment of all disciplinary
2 actions taken against such officers, employ-
3 ees, and agents.

4 “(G) A summary of the number and type of
5 non-Federal entities that received classified cyber
6 threat indicators from the Federal Government
7 under this section or such Act and an evaluation
8 of the risks and benefits of sharing such cyber
9 threat indicators.

10 “(H) An assessment of any personal infor-
11 mation of or information identifying a specific
12 person not directly related to a cybersecurity
13 threat that—

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

17 “(ii) was shared within the Federal
18 Government under this Act in contravention
19 of the guidelines required by section 4(b).

20 “(3) *RECOMMENDATIONS.*—Each report sub-
21 mitted under paragraph (1) may include such rec-
22 ommendations as the heads of the appropriate Federal
23 entities may have for improvements or modifications
24 to the authorities and processes under this section or
25 such Act.

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

4 “(5) *PUBLIC AVAILABILITY OF REPORTS.*—The
5 Director of National Intelligence shall make publicly
6 available the unclassified portion of each report re-
7 quired by paragraph (1).”.

8 (2) *INITIAL REPORT.*—The first report required
9 under subsection (c) of section 111 of the National Se-
10 curity Act of 1947, as inserted by paragraph (1) of
11 this subsection, shall be submitted not later than one
12 year after the date of the enactment of this Act.

13 (b) *REPORTS ON PRIVACY AND CIVIL LIBERTIES.*—

14 (1) *BIENNIAL REPORT FROM PRIVACY AND CIVIL*
15 *LIBERTIES OVERSIGHT BOARD.*—

16 (A) *IN GENERAL.*—Section 1061(e) of the
17 *Intelligence Reform and Terrorism Prevention*
18 *Act of 2004 (42 U.S.C. 2000ee(e)) is amended by*
19 *adding at the end the following new paragraph:*

20 “(3) *BIENNIAL REPORT ON CERTAIN CYBER AC-*
21 *TIVITIES.*—

22 “(A) *REPORT REQUIRED.*—The *Privacy*
23 *and Civil Liberties Oversight Board shall bienni-*
24 *ally submit to Congress and the President a re-*
25 *port containing—*

1 “(i) *an assessment of the privacy and*
2 *civil liberties impact of the activities car-*
3 *ried out under the Protecting Cyber Net-*
4 *works Act and the amendments made by*
5 *such Act; and*

6 “(ii) *an assessment of the sufficiency of*
7 *the policies, procedures, and guidelines es-*
8 *tablished pursuant to section 4 of the Pro-*
9 *tecting Cyber Networks Act and the amend-*
10 *ments made by such section 4 in addressing*
11 *privacy and civil liberties concerns.*

12 “(B) *RECOMMENDATIONS.—Each report*
13 *submitted under this paragraph may include*
14 *such recommendations as the Privacy and Civil*
15 *Liberties Oversight Board may have for improve-*
16 *ments or modifications to the authorities under*
17 *the Protecting Cyber Networks Act or the amend-*
18 *ments made by such Act.*

19 “(C) *FORM.—Each report required under*
20 *this paragraph shall be submitted in unclassified*
21 *form, but may include a classified annex.*

22 “(D) *PUBLIC AVAILABILITY OF REPORTS.—*
23 *The Privacy and Civil Liberties Oversight Board*
24 *shall make publicly available the unclassified*

1 portion of each report required by subparagraph
2 (A).”.

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

10 (2) *BIENNIAL REPORT OF INSPECTORS GEN-*
11 *ERAL.*—

12 (A) *IN GENERAL.*—Not later than 2 years
13 after the date of the enactment of this Act and
14 not less frequently than once every 2 years there-
15 after, the *Inspector General of the Department of*
16 *Homeland Security, the Inspector General of the*
17 *Intelligence Community, the Inspector General of*
18 *the Department of Justice, and the Inspector*
19 *General of the Department of Defense, in con-*
20 *sultation with the Council of Inspectors General*
21 *on Financial Oversight, shall jointly submit to*
22 *Congress a report on the receipt, use, and dis-*
23 *semination of cyber threat indicators and defen-*
24 *sive measures that have been shared with Federal*

1 *entities under this Act and the amendments*
2 *made by this Act.*

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

6 (i) *A review of the types of cyber threat*
7 *indicators shared with Federal entities.*

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

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

13 (iv) *A review of the sharing of such*
14 *cyber threat indicators among Federal enti-*
15 *ties to identify inappropriate barriers to*
16 *sharing information.*

17 (C) *RECOMMENDATIONS.*—*Each report sub-*
18 *mitted under this paragraph may include such*
19 *recommendations as the Inspectors General re-*
20 *ferred to in subparagraph (A) may have for im-*
21 *provements or modifications to the authorities*
22 *under this Act or the amendments made by this*
23 *Act.*

1 (D) *FORM.*—Each report required under
2 this paragraph shall be submitted in unclassified
3 form, but may include a classified annex.

4 (E) *PUBLIC AVAILABILITY OF REPORTS.*—
5 The Inspector General of the Department of
6 Homeland Security, the Inspector General of the
7 Intelligence Community, the Inspector General of
8 the Department of Justice, and the Inspector
9 General of the Department of Defense shall make
10 publicly available the unclassified portion of
11 each report required under subparagraph (A).

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

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

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

23 (1) *An assessment of—*

24 (A) *the current intelligence sharing and co-*
25 *operation relationships of the United States with*

1 *other countries regarding cybersecurity threats*
2 *(including cyber attacks, theft, and data*
3 *breaches) directed against the United States that*
4 *threaten the United States national security in-*
5 *terests, economy, and intellectual property; and*

6 *(B) the relative utility of such relationships,*
7 *which elements of the intelligence community*
8 *participate in such relationships, and whether*
9 *and how such relationships could be improved.*

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

16 *(3) A description of the extent to which the capa-*
17 *bilities of the United States Government to respond to*
18 *or prevent cybersecurity threats (including cyber at-*
19 *tacks, theft, or data breaches) directed against the*
20 *United States private sector are degraded by a delay*
21 *in the prompt notification by private entities of such*
22 *threats or cyber attacks, theft, and breaches.*

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

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

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

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

10 *(d) PUBLIC AVAILABILITY OF REPORT.—The Director*
11 *of National Intelligence shall make publicly available the*
12 *unclassified portion of the report required by subsection (a).*

13 *(e) INTELLIGENCE COMMUNITY DEFINED.—In this sec-*
14 *tion, the term “intelligence community” has the meaning*
15 *given that term in section 3 of the National Security Act*
16 *of 1947 (50 U.S.C. 3003).*

17 **SEC. 9. CONSTRUCTION AND PREEMPTION.**

18 *(a) PROHIBITION OF SURVEILLANCE.—Nothing in this*
19 *Act or the amendments made by this Act shall be construed*
20 *to authorize the Department of Defense or the National Se-*
21 *curity Agency or any other element of the intelligence com-*
22 *munity to target a person for surveillance.*

23 *(b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in*
24 *this Act or the amendments made by this Act shall be con-*
25 *strued to limit or prohibit—*

1 (1) *otherwise lawful disclosures of communica-*
2 *tions, records, or other information, including report-*
3 *ing of known or suspected criminal activity, by a*
4 *non-Federal entity to any other non-Federal entity or*
5 *the Federal Government; or*

6 (2) *any otherwise lawful use of such disclosures*
7 *by any entity of the Federal government, without re-*
8 *gard to whether such otherwise lawful disclosures du-*
9 *PLICATE or replicate disclosures made under this Act.*

10 (c) *WHISTLE BLOWER PROTECTIONS.—Nothing in*
11 *this Act or the amendments made by this Act shall be con-*
12 *strued to prohibit or limit the disclosure of information pro-*
13 *tected under section 2302(b)(8) of title 5, United States*
14 *Code (governing disclosures of illegality, waste, fraud,*
15 *abuse, or public health or safety threats), section 7211 of*
16 *title 5, United States Code (governing disclosures to Con-*
17 *gress), section 1034 of title 10, United States Code (gov-*
18 *erning disclosure to Congress by members of the military),*
19 *or any similar provision of Federal or State law..*

20 (d) *PROTECTION OF SOURCES AND METHODS.—Noth-*
21 *ing in this Act or the amendments made by this Act shall*
22 *be construed—*

23 (1) *as creating any immunity against, or other-*
24 *wise affecting, any action brought by the Federal*
25 *Government, or any department or agency thereof, to*

1 enforce any law, executive order, or procedure gov-
2 erning the appropriate handling, disclosure, or use of
3 classified information;

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

6 (3) to modify the authority of the President or
7 a department or agency of the Federal Government to
8 protect and control the dissemination of classified in-
9 formation, intelligence sources and methods, and the
10 national security of the United States.

11 (e) *RELATIONSHIP TO OTHER LAWS.*—Nothing in this
12 Act or the amendments made by this Act shall be construed
13 to affect any requirement under any other provision of law
14 for a non-Federal entity to provide information to the Fed-
15 eral Government.

16 (f) *INFORMATION SHARING RELATIONSHIPS.*—Nothing
17 in this Act or the amendments made by this Act shall be
18 construed—

19 (1) to limit or modify an existing information-
20 sharing relationship;

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

23 (3) to require a new information-sharing rela-
24 tionship between any non-Federal entity and the Fed-
25 eral Government.

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

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

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

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

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

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

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

24 (i) *NO LIABILITY FOR NON-PARTICIPATION.*—*Nothing*
25 *in this Act or the amendments made by this Act shall be*

1 *construed to subject any non-Federal entity to liability for*
2 *choosing not to engage in a voluntary activity authorized*
3 *in this Act and the amendments made by this Act.*

4 (j) *USE AND RETENTION OF INFORMATION.*—*Nothing*
5 *in this Act or the amendments made by this Act shall be*
6 *construed to authorize, or to modify any existing authority*
7 *of, a department or agency of the Federal Government to*
8 *retain or use any information shared under this Act or the*
9 *amendments made by this Act for any use other than per-*
10 *mitted in this Act or the amendments made by this Act.*

11 (k) *FEDERAL PREEMPTION.*—

12 (1) *IN GENERAL.*—*This Act and the amendments*
13 *made by this Act supersede any statute or other pro-*
14 *vision of law of a State or political subdivision of a*
15 *State that restricts or otherwise expressly regulates an*
16 *activity authorized under this Act or the amendments*
17 *made by this Act.*

18 (2) *STATE LAW ENFORCEMENT.*—*Nothing in this*
19 *Act or the amendments made by this Act shall be con-*
20 *strued to supersede any statute or other provision of*
21 *law of a State or political subdivision of a State con-*
22 *cerning the use of authorized law enforcement prac-*
23 *tices and procedures.*

24 (l) *REGULATORY AUTHORITY.*—*Nothing in this Act or*
25 *the amendments made by this Act shall be construed—*

1 (1) to authorize the promulgation of any regula-
2 tions not specifically authorized by this Act or the
3 amendments made by this Act;

4 (2) to establish any regulatory authority not spe-
5 cifically established under this Act or the amendments
6 made by this Act; or

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

11 **SEC. 10. CONFORMING AMENDMENTS.**

12 Section 552(b) of title 5, United States Code, is amend-
13 *ed—*

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

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

18 (3) by inserting after paragraph (9) the fol-
19 lowing:

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

23 **SEC. 11. DEFINITIONS.**

24 In this Act:

1 (1) *AGENCY.*—*The term “agency” has the mean-*
2 *ing given the term in section 3502 of title 44, United*
3 *States Code.*

4 (2) *APPROPRIATE FEDERAL ENTITIES.*—*The*
5 *term “appropriate Federal entities” means the fol-*
6 *lowing:*

7 (A) *The Department of Commerce.*

8 (B) *The Department of Defense.*

9 (C) *The Department of Energy.*

10 (D) *The Department of Homeland Security.*

11 (E) *The Department of Justice.*

12 (F) *The Department of the Treasury.*

13 (G) *The Office of the Director of National*
14 *Intelligence.*

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

22 (4) *CYBERSECURITY THREAT.*—

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

1 *first amendment to the Constitution of the*
2 *United States, on or through an information sys-*
3 *tem that may result in an unauthorized effort to*
4 *adversely impact the security, confidentiality,*
5 *integrity, or availability of an information sys-*
6 *tem or information that is stored on, processed*
7 *by, or transiting an information system.*

8 (B) *EXCLUSION.—The term “cybersecurity*
9 *threat” does not include any action that solely*
10 *involves a violation of a consumer term of service*
11 *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 control*
22 *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 other-
14 wise prohibited by law.

15 (6) *DEFENSIVE MEASURE*.—The term “defensive
16 measure” means an action, device, procedure, tech-
17 nique, or other measure executed on an information
18 system or information that is stored on, processed by,
19 or transiting an information system that prevents or
20 mitigates a known or suspected cybersecurity threat
21 or security vulnerability.

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

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 gov-*
10 *ernment” means any borough, city, county, parish,*
11 *town, township, village, or other political subdivision*
12 *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 by,*
18 *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 informa-*
22 *tion system for the purpose of discerning security*
23 *vulnerabilities of the information system, if such*
24 *method is associated with a known or suspected cyber-*
25 *security 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 pro-*
7 *vided in this paragraph, the term “non-Federal*
8 *entity” means any private entity, non-Federal*
9 *government department or agency, or State, trib-*
10 *al, or local government (including a political*
11 *subdivision, department, officer, employee, or*
12 *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 pro-*
5 *vided in this paragraph, the term “private enti-*
6 *ty” means any person or private group, organi-*
7 *zation, proprietorship, partnership, trust, cooper-*
8 *ative, corporation, or other commercial or non-*
9 *profit entity, including an officer, employee, or*
10 *agent thereof.*

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

14 (C) *EXCLUSION.*—*The term “private entity”*
15 *does not include a foreign power as defined in*
16 *section 101 of the Foreign Intelligence Surveil-*
17 *lance 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 *coding 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 infor-*
6 *mation system or its information.*

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

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

Union Calendar No. 44

114TH CONGRESS
1ST Session

H. R. 1560

[Report No. 114-63]

A BILL

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

APRIL 13, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed