

## Union Calendar No. 61

114<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

# H. R. 1731

**[Report No. 114–83]**

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.

---

### IN THE HOUSE OF REPRESENTATIVES

APRIL 13, 2015

Mr. McCAUL (for himself and Mr. RATCLIFFE) introduced the following bill;  
which was referred to the Committee on Homeland Security

APRIL 17, 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 *italie*]

[For text of introduced bill, see copy of bill as introduced on April 13, 2015]

# **A BILL**

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. SHORT TITLE.**

4 *This Act may be cited as the “National Cybersecurity*  
5 *Protection Advancement Act of 2015”.*

6 **SEC. 2. NATIONAL CYBERSECURITY AND COMMUNICATIONS**

7 **INTEGRATION CENTER.**

8 *(a) DEFINITIONS.—*

9 *(1) IN GENERAL.—Subsection (a) of the second*  
10 *section 226 of the Homeland Security Act of 2002 (6*  
11 *U.S.C. 148; relating to the National Cybersecurity*  
12 *and Communications Integration Center) is amend-*  
13 *ed—*

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

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

18 *(C) 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 informa-*  
2            *tion system, if such method is known or reason-*  
3            *ably suspected of being associated with a known*  
4            *or suspected cybersecurity risk, including com-*  
5            *munications that reasonably appear to be trans-*  
6            *mitted for the purpose of gathering technical in-*  
7            *formation related to a cybersecurity risk;*

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

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

13           *“(D) a method of causing a user with legiti-*  
14           *mate access to an information system or infor-*  
15           *mation that is stored on, processed by, or*  
16           *transiting an information system to inadvert-*  
17           *ently enable the defeat of a technical or oper-*  
18           *ational control;*

19           *“(E) a method for unauthorized remote*  
20           *identification of, access to, or use of an informa-*  
21           *tion system or information that is stored on,*  
22           *processed by, or transiting an information sys-*  
23           *tem that is known or reasonably suspected of*  
24           *being associated with a known or suspected cy-*  
25           *bersecurity risk;*

1           “(F) the actual or potential harm caused by  
2           a cybersecurity risk, including a description of  
3           the information exfiltrated as a result of a par-  
4           ticular cybersecurity risk;

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

10           “(H) any combination of subparagraphs  
11           (A) through (G);

12           “(6) the term ‘cybersecurity purpose’ means the  
13           purpose of protecting an information system or infor-  
14           mation that is stored on, processed by, or transiting  
15           an information system from a cybersecurity risk or  
16           incident;

17           “(7)(A) except as provided in subparagraph (B),  
18           the term ‘defensive measure’ means an action, device,  
19           procedure, signature, technique, or other measure ap-  
20           plied to an information system or information that is  
21           stored on, processed by, or transiting an information  
22           system that detects, prevents, or mitigates a known or  
23           suspected cybersecurity risk or incident, or any at-  
24           tribute of hardware, software, process, or procedure

1       *that could enable or facilitate the defeat of a security*  
2       *control;*

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

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

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

14              “(8) *the term ‘network awareness’ means to scan,*  
15       *identify, acquire, monitor, log, or analyze informa-*  
16       *tion that is stored on, processed by, or transiting an*  
17       *information system;*

18              “(9)(A) *the term ‘private entity’ means a non-*  
19       *Federal entity that is an individual or private group,*  
20       *organization, proprietorship, partnership, trust, coop-*  
21       *erative, corporation, or other commercial or non-prof-*  
22       *it entity, including an officer, employee, or agent*  
23       *thereof;*

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

4           “(10) the term ‘security control’ means the man-  
5           agement, operational, and technical controls used to  
6           protect against an unauthorized effort to adversely af-  
7           fect the confidentiality, integrity, or availability of an  
8           information system or information that is stored on,  
9           processed by, or transiting an information system;  
10          and

11          “(11) the term ‘sharing’ means providing, receiv-  
12          ing, and disseminating.”.

13          (b) *AMENDMENT.*—Subparagraph (B) of subsection  
14          (d)(1) of such second section 226 of the *Homeland Security*  
15          *Act of 2002* is amended—

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

18                 (2) in clause (ii)—

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

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

23                 (3) in clause (iii), by striking the period at the  
24                 end and inserting “; and”; and

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

3                           “(iv) private entities.”.

4 **SEC. 3. INFORMATION SHARING STRUCTURE AND PROC-**  
5 **ESSES.**

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

10                   (1) in subsection (c)—

11                           (A) in paragraph (1)—

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

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

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

21                           (C) in paragraph (5)(A), by striking “cy-  
22 bersecurity risks” and inserting “cyber threat in-  
23 dicators, defensive measures, cybersecurity  
24 risks,”;

25                           (D) in paragraph (6)—



1           (i) by striking “cybersecurity risks”  
2           and inserting “cyber threat indicators, de-  
3           fensive measures, cybersecurity risks,”; and

4           (ii) by striking “and” at the end;

5           (E) in paragraph (7)—

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

8           (ii) in subparagraph (B), by striking  
9           the period at the end and inserting “; and”;  
10          and

11          (iii) by adding at the end the following  
12          new subparagraph:

13          “(C) sharing cyber threat indicators and de-  
14          fensive measures;” and

15          (F) by adding at the end the following new  
16          paragraphs

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

19                “(A) collaborate on cyber threat indicators,  
20                defensive measures, and information related to  
21                cybersecurity risks and incidents; and

22                “(B) enhance the security and resilience of  
23                global cybersecurity;

24                “(9) sharing cyber threat indicators, defensive  
25                measures, and other information related to cybersecu-

1        *city risks and incidents with Federal and non-Fed-*  
2        *eral entities, including across sectors of critical infra-*  
3        *structure and with State and major urban area fu-*  
4        *sion centers, as appropriate;*

5                *“(10) promptly notifying the Secretary and the*  
6        *Committee on Homeland Security of the House of*  
7        *Representatives and the Committee on Homeland Se-*  
8        *curity and Governmental Affairs of the Senate of any*  
9        *significant violations of the policies and procedures*  
10        *specified in subsection (i)(6)(A);*

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

16                *“(12) participating, as appropriate, in exercises*  
17        *run by the Department’s National Exercise Pro-*  
18        *gram.”;*

19                *(2) in subsection (d)—*

20                        *(A) in subparagraph (D), by striking “and”*  
21                        *at the end;*

22                        *(B) by redesignating subparagraph (E) as*  
23                        *subparagraph (J); and*

24                        *(C) by inserting after subparagraph (D) the*  
25                        *following new subparagraphs:*

1           “(E) an entity that collaborates with State  
2           and local governments on cybersecurity risks and  
3           incidents, and has entered into a voluntary in-  
4           formation sharing relationship with the Center;

5           “(F) a United States Computer Emergency  
6           Readiness Team that coordinates information re-  
7           lated to cybersecurity risks and incidents,  
8           proactively and collaboratively addresses cyberse-  
9           curity risks and incidents to the United States,  
10          collaboratively responds to cybersecurity risks  
11          and incidents, provides technical assistance,  
12          upon request, to information system owners and  
13          operators, and shares cyber threat indicators, de-  
14          fensive measures, analysis, or information re-  
15          lated to cybersecurity risks and incidents in a  
16          timely manner;

17          “(G) the Industrial Control System Cyber  
18          Emergency Response Team that—

19                  “(i) coordinates with industrial control  
20                  systems owners and operators;

21                  “(ii) provides training, upon request,  
22                  to Federal entities and non-Federal entities  
23                  on industrial control systems cybersecurity;

1           “(iii) collaboratively addresses cyberse-  
2           curity risks and incidents to industrial con-  
3           trol systems;

4           “(iv) provides technical assistance,  
5           upon request, to Federal entities and non-  
6           Federal entities relating to industrial con-  
7           trol systems cybersecurity; and

8           “(v) shares cyber threat indicators, de-  
9           fensive measures, or information related to  
10          cybersecurity risks and incidents of indus-  
11          trial control systems in a timely fashion;

12          “(H) a National Coordinating Center for  
13          Communications that coordinates the protection,  
14          response, and recovery of emergency communica-  
15          tions;

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

18          (3) in subsection (e)—

19                  (A) in paragraph (1)—

20                          (i) in subparagraph (A), by inserting  
21                          “cyber threat indicators, defensive measures,  
22                          and” before “information”;

23                          (ii) in subparagraph (B), by inserting  
24                          “cyber threat indicators, defensive measures,  
25                          and” before “information”;

1           (iii) in subparagraph (F), by striking  
2           “cybersecurity risks” and inserting “cyber  
3           threat indicators, defensive measures, cyber-  
4           security risks,”;

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

7           (v) in subparagraph (G), by striking  
8           “cybersecurity risks” and inserting “cyber  
9           threat indicators, defensive measures, cyber-  
10          security risks,”; and

11          (vi) by adding at the end the following:

12          “(H) the Center ensures that it shares infor-  
13          mation relating to cybersecurity risks and inci-  
14          dents with small and medium-sized businesses,  
15          as appropriate; and

16          “(I) the Center designates an agency contact  
17          for non-Federal entities;”;

18          (B) in paragraph (2)—

19               (i) by striking “cybersecurity risks”  
20               and inserting “cyber threat indicators, de-  
21               fensive measures, cybersecurity risks,”; and

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

24          (C) in paragraph (3), by inserting before  
25          the period at the end the following: “, including

1           *by working with the Chief Privacy Officer ap-*  
2           *pointed under section 222 to ensure that the Cen-*  
3           *ter follows the policies and procedures specified*  
4           *in subsection (i)(6)(A)”; and*

5           *(4) by adding at the end the following new sub-*  
6           *sections:*

7           “*(g) RAPID AUTOMATED SHARING.—*

8                 “*(1) IN GENERAL.—The Under Secretary for Cy-*  
9                 *bersecurity and Infrastructure Protection, in coordi-*  
10                *nation with industry and other stakeholders, shall de-*  
11                *velop capabilities making use of existing information*  
12                *technology industry standards and best practices, as*  
13                *appropriate, that support and rapidly advance the*  
14                *development, adoption, and implementation of auto-*  
15                *mated mechanisms for the timely sharing of cyber*  
16                *threat indicators and defensive measures to and from*  
17                *the Center and with each Federal agency designated*  
18                *as the ‘Sector Specific Agency’ for each critical infra-*  
19                *structure sector in accordance with subsection (h).*

20                “*(2) BIENNIAL REPORT.—The Under Secretary*  
21                *for Cybersecurity and Infrastructure Protection shall*  
22                *submit to the Committee on Homeland Security of the*  
23                *House of Representatives and the Committee on*  
24                *Homeland Security and Governmental Affairs of the*  
25                *Senate a biennial report on the status and progress*

1       *of the development of the capability described in*  
2       *paragraph (1). Such reports shall be required until*  
3       *such capability is fully implemented.*

4       “(h) *SECTOR SPECIFIC AGENCIES.—The Secretary, in*  
5       *collaboration with the relevant critical infrastructure sector*  
6       *and the heads of other appropriate Federal agencies, shall*  
7       *recognize the Federal agency designated as of March 25,*  
8       *2015, as the ‘Sector Specific Agency’ for each critical infra-*  
9       *structure sector designated in the Department’s National*  
10       *Infrastructure Protection Plan. If the designated Sector*  
11       *Specific Agency for a particular critical infrastructure sec-*  
12       *tor is the Department, for purposes of this section, the Sec-*  
13       *retary is deemed to be the head of such Sector Specific Agen-*  
14       *cy and shall carry out this section. The Secretary, in co-*  
15       *ordination with the heads of each such Sector Specific Agen-*  
16       *cy, shall—*

17               “(1) *support the security and resilience actives of*  
18       *the relevant critical infrastructure sector in accord-*  
19       *ance with this section;*

20               “(2) *provide institutional knowledge, specialized*  
21       *expertise, and technical assistance upon request to the*  
22       *relevant critical infrastructure sector; and*

23               “(3) *support the timely sharing of cyber threat*  
24       *indicators and defensive measures with the relevant*

1       *critical infrastructure sector with the Center in ac-*  
2       *cordance with this section.*

3       “(i) *VOLUNTARY INFORMATION SHARING PROCE-*  
4       *DURES.—*

5               “(1) *PROCEDURES.—*

6                       “(A) *IN GENERAL.—The Center may enter*  
7                       *into a voluntary information sharing relation-*  
8                       *ship with any consenting non-Federal entity for*  
9                       *the sharing of cyber threat indicators and defen-*  
10                      *sive measures for cybersecurity purposes in ac-*  
11                      *cordance with this section. Nothing in this sec-*  
12                      *tion may be construed to require any non-Fed-*  
13                      *eral entity to enter into any such information*  
14                      *sharing relationship with the Center or any*  
15                      *other entity. The Center may terminate a vol-*  
16                      *untary information sharing relationship under*  
17                      *this subsection if the Center determines that the*  
18                      *non-Federal entity with which the Center has en-*  
19                      *tered into such a relationship has, after repeated*  
20                      *notice, repeatedly violated the terms of this sub-*  
21                      *section.*

22                      “(B) *NATIONAL SECURITY.—The Secretary*  
23                      *may decline to enter into a voluntary informa-*  
24                      *tion sharing relationship under this subsection if*



1           *the Secretary determines that such is appro-*  
2           *priate for national security.*

3           “(2) *VOLUNTARY INFORMATION SHARING RELA-*  
4           *TIONSHIPS.—A voluntary information sharing rela-*  
5           *tionship under this subsection may be characterized*  
6           *as an agreement described in this paragraph.*

7           “(A) *STANDARD AGREEMENT.—For the use*  
8           *of a non-Federal entity, the Center shall make*  
9           *available a standard agreement, consistent with*  
10          *this section, on the Department’s website.*

11          “(B) *NEGOTIATED AGREEMENT.—At the re-*  
12          *quest of a non-Federal entity, and if determined*  
13          *appropriate by the Center, the Department shall*  
14          *negotiate a non-standard agreement, consistent*  
15          *with this section.*

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

1           *ative Research and Development Agreement for*  
2           *Cybersecurity Information Sharing and Collabo-*  
3           *ration, as of December 31, 2014. Nothing in this*  
4           *subsection may be construed to require a non-*  
5           *Federal entity to enter into either a standard or*  
6           *negotiated agreement to be in compliance with*  
7           *this subsection.*

8           “(3) *INFORMATION SHARING AUTHORIZATION.*—

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

21                           “(i) *another non-Federal entity; or*

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

24                   “(B) *LAWFUL RESTRICTION.*—*A non-Fed-*  
25           *eral entity receiving a cyber threat indicator or*

1           *defensive measure from another Federal entity or*  
2           *non-Federal entity shall comply with otherwise*  
3           *lawful restrictions placed on the sharing or use*  
4           *of such cyber threat indicator or defensive meas-*  
5           *ure by the sharing Federal entity or non-Federal*  
6           *entity.*

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

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

20                  “(i) *limit or modify an existing infor-*  
21                  *mation sharing relationship;*

22                  “(ii) *prohibit a new information shar-*  
23                  *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 the  
7           enactment of this section for reporting  
8           known or suspected criminal activity to ap-  
9           propriate law enforcement authorities or for  
10          participating voluntarily or under legal re-  
11          quirement in an investigation.

12          “(E) COORDINATED VULNERABILITY DIS-  
13          CLOSURE.—The Under Secretary for Cybersecu-  
14          rity and Infrastructure Protection, in coordina-  
15          tion with industry and other stakeholders, shall  
16          develop, publish, and adhere to policies and pro-  
17          cedures for coordinating vulnerability disclo-  
18          sures, to the extent practicable, consistent with  
19          international standards in the information tech-  
20          nology 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 network*  
2           *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 of*  
8                   *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 enti-*  
15                   *ty for conducting such network awareness to*  
16                   *protect the rights or property of such Fed-*  
17                   *eral 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 in*  
22                   *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, other*  
2           *than as provided in this section; or*

3           “(i) *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 defen-*  
10          *sive 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-Federal*  
19           *entity;*

20           “(iii) *an information system of a Fed-*  
21           *eral entity upon written consent of an au-*  
22           *thorized representative of such Federal enti-*  
23           *ty for operation of such defensive measure*  
24           *to protect the rights or property of such*  
25           *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 in  
5           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 De-  
18          partment, establish and annually review  
19          policies and procedures governing the re-  
20          ceipt, retention, use, and disclosure of cyber  
21          threat indicators, defensive measures, and  
22          information related to cybersecurity risks  
23          and incidents shared with the Center in ac-  
24          cordance with this section. Such policies  
25          and procedures shall apply only to the De-

1            *partment, consistent with the need to pro-*  
2            *tect information systems from cybersecurity*  
3            *risks and incidents and mitigate cybersecu-*  
4            *rity risks and incidents in a timely man-*  
5            *ner, 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 Code*  
10                   *(commonly referred to as the ‘Privacy*  
11                   *Act of 1974’ or the ‘Privacy Act’), and*  
12                   *subject to the Secretary’s authority*  
13                   *under subsection (a)(2) of section 222*  
14                   *of this Act;*

15                   *“(II) reasonably limit, to the*  
16                   *greatest extent practicable, the receipt,*  
17                   *retention, use, and disclosure of cyber*  
18                   *threat indicators and defensive meas-*  
19                   *ures associated with specific persons*  
20                   *that is not necessary, for cybersecurity*  
21                   *purposes, to protect a network or infor-*  
22                   *mation system from cybersecurity risks*  
23                   *or mitigate cybersecurity risks and in-*  
24                   *cidents in a timely 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 or  
8           incident information shared and re-  
9           tained by the Center in accordance  
10          with this section;

11          “(V) include requirements to safe-  
12          guard cyber threat indicators and de-  
13          fensive measures retained by the Cen-  
14          ter, including information that is pro-  
15          prietary or business-sensitive that may  
16          be used to identify specific persons  
17          from unauthorized access or acquisi-  
18          tion;

19          “(VI) protect the confidentiality of  
20          cyber threat indicators and defensive  
21          measures associated with specific per-  
22          sons to the greatest extent practicable;  
23          and

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

4                   “(ii) *SUBMISSION TO CONGRESS.*—Not  
5                   later than 180 days after the date of the en-  
6                   actment of this section and annually there-  
7                   after, the Chief Privacy Officer and the Of-  
8                   ficer for Civil Rights and Civil Liberties of  
9                   the Department, in consultation with the  
10                  Privacy and Civil Liberties Oversight  
11                  Board (established pursuant to section 1061  
12                  of the Intelligence Reform and Terrorism  
13                  Prevention Act of 2004 (42 U.S.C. 2000ee)),  
14                  shall submit to the Committee on Homeland  
15                  Security of the House of Representatives  
16                  and the Committee on Homeland Security  
17                  and Governmental Affairs of the Senate the  
18                  policies and procedures governing the shar-  
19                  ing of cyber threat indicators, defensive  
20                  measures, and information related to  
21                  cybersecurity risks and incidents described  
22                  in clause (i) of subparagraph (A).

23                  “(iii) *PUBLIC NOTICE AND ACCESS.*—  
24                  The Under Secretary for Cybersecurity and  
25                  Infrastructure Protection, in consultation

1           *with the Chief Privacy Officer and the Chief*  
2           *Civil Rights and Civil Liberties Officer of*  
3           *the Department, and the Privacy and Civil*  
4           *Liberties Oversight Board (established pur-*  
5           *suant to section 1061 of the Intelligence Re-*  
6           *form and Terrorism Prevention Act of 2004*  
7           *(42 U.S.C. 2000ee)), shall ensure there is*  
8           *public notice of, and access to, the policies*  
9           *and procedures governing the sharing of*  
10          *cyber threat indicators, defensive measures,*  
11          *and information related to cybersecurity*  
12          *risks and incidents.*

13           “(iv) *CONSULTATION.—The Under Sec-*  
14          *retary for Cybersecurity and Infrastructure*  
15          *Protection when establishing policies and*  
16          *procedures to support privacy and civil lib-*  
17          *erties may consult with the National Insti-*  
18          *tute of Standards and Technology.*

19           “(B) *IMPLEMENTATION.—The Chief Privacy*  
20          *Officer of the Department, on an ongoing basis,*  
21          *shall—*

22           “(i) *monitor the implementation of the*  
23          *policies and procedures governing the shar-*  
24          *ing of cyber threat indicators and defensive*

1           *measures established pursuant to clause (i)*  
2           *of subparagraph (A);*

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

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

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

19          “(v) *ensure there are appropriate sanc-*  
20          *tions in place for officers, employees, or*  
21          *agents of the Department who intentionally*  
22          *or willfully conduct activities under this*  
23          *section in an unauthorized manner.*

24          “(C) *INSPECTOR GENERAL REPORT.—The*  
25          *Inspector General of the Department, in con-*

1           *sultation with the Privacy and Civil Liberties*  
2           *Oversight Board and the Inspector General of*  
3           *each Federal agency that receives cyber threat*  
4           *indicators or defensive measures shared with the*  
5           *Center under this section, shall, not later than*  
6           *two years after the date of the enactment of this*  
7           *subsection and periodically thereafter submit to*  
8           *the Committee on Homeland Security of the*  
9           *House of Representatives and the Committee on*  
10           *Homeland Security and Governmental Affairs of*  
11           *the Senate a report containing a review of the*  
12           *use of cybersecurity risk information shared with*  
13           *the Center, including the following:*

14                   “(i) *A report on the receipt, use, and*  
15                   *dissemination of cyber threat indicators and*  
16                   *defensive measures that have been shared*  
17                   *with Federal entities under this section.*

18                   “(ii) *Information on the use by the*  
19                   *Center of such information for a purpose*  
20                   *other than a cybersecurity purpose.*

21                   “(iii) *A review of the type of informa-*  
22                   *tion shared with the Center under this sec-*  
23                   *tion.*

24                   “(iv) *A review of the actions taken by*  
25                   *the Center based on such information.*

1           “(v) *The appropriate metrics that exist*  
2           *to determine the impact, if any, on privacy*  
3           *and civil liberties as a result of the sharing*  
4           *of such information with the Center.*

5           “(vi) *A list of other Federal agencies*  
6           *receiving such information.*

7           “(vii) *A review of the sharing of such*  
8           *information within the Federal Government*  
9           *to identify inappropriate stove piping of*  
10           *such information.*

11           “(viii) *Any recommendations of the In-*  
12           *spector General of the Department for im-*  
13           *provements or modifications to information*  
14           *sharing under this section.*

15           “(D) *PRIVACY AND CIVIL LIBERTIES OFFI-*  
16           *CERS REPORT.—The Chief Privacy Officer and*  
17           *the Chief Civil Rights and Civil Liberties Officer*  
18           *of the Department, in consultation with the Pri-*  
19           *vacancy and Civil Liberties Oversight Board, the*  
20           *Inspector General of the Department, and the*  
21           *senior privacy and civil liberties officer of each*  
22           *Federal agency that receives cyber threat indica-*  
23           *tors and defensive measures shared with the Cen-*  
24           *ter under this section, shall biennially submit to*  
25           *the appropriate congressional committees a re-*

1            *port assessing the privacy and civil liberties im-*  
2            *port of the activities under this paragraph. Each*  
3            *such report shall include any recommendations*  
4            *the Chief Privacy Officer and the Chief Civil*  
5            *Rights and Civil Liberties Officer of the Depart-*  
6            *ment consider appropriate to minimize or miti-*  
7            *gate the privacy and civil liberties impact of the*  
8            *sharing of cyber threat indicators and defensive*  
9            *measures under this section.*

10            *“(E) FORM.—Each report required under*  
11            *paragraphs (C) and (D) shall be submitted in*  
12            *unclassified form, but may include a classified*  
13            *annex.*

14            *“(7) USES AND PROTECTION OF INFORMATION.—*

15            *“(A) NON-FEDERAL ENTITIES.—A non-Fed-*  
16            *eral entity, not including a State, local, or tribal*  
17            *government, that shares cyber threat indicators*  
18            *or defensive measures through the Center or oth-*  
19            *erwise under this section—*

20            *“(i) may use, retain, or further disclose*  
21            *such cyber threat indicators or defensive*  
22            *measures solely for cybersecurity purposes;*

23            *“(ii) shall, prior to such sharing, take*  
24            *reasonable efforts to remove information*  
25            *that can be used to identify specific persons*

1           *and is reasonably believed at the time of*  
2           *sharing to be unrelated to a cybersecurity*  
3           *risk or incident, and to safeguard informa-*  
4           *tion that can be used to identify specific*  
5           *persons from unintended disclosure or un-*  
6           *authorized access or acquisition;*

7           *“(iii) shall comply with appropriate*  
8           *restrictions that a Federal entity or non-*  
9           *Federal entity places on the subsequent dis-*  
10          *closure or retention of cyber threat indica-*  
11          *tors and defensive measures that it discloses*  
12          *to other Federal entities or non-Federal en-*  
13          *tities;*

14          *“(iv) shall be deemed to have volun-*  
15          *tarily shared such cyber threat indicators or*  
16          *defensive measures;*

17          *“(v) shall implement and utilize a se-*  
18          *curity control to protect against unauthor-*  
19          *ized access to or acquisition of such cyber*  
20          *threat indicators or defensive measures; and*

21          *“(vi) may not use such information to*  
22          *gain an unfair competitive advantage to the*  
23          *detriment of any non-Federal entity.*

24          *“(B) FEDERAL ENTITIES.—*



1           “(i) *USES OF INFORMATION.*—A *Fed-*  
2           *eral entity that receives cyber threat indica-*  
3           *tors or defensive measures shared through*  
4           *the Center or otherwise under this section*  
5           *from another Federal entity or a non-Fed-*  
6           *eral entity—*

7                   “(I) *may use, retain, or further*  
8                   *disclose such cyber threat indicators or*  
9                   *defensive measures solely for cybersecu-*  
10                  *rity purposes;*

11                  “(II) *shall, prior to such sharing,*  
12                  *take reasonable efforts to remove infor-*  
13                  *mation that can be used to identify*  
14                  *specific persons and is reasonably be-*  
15                  *lieved at the time of sharing to be un-*  
16                  *related to a cybersecurity risk or inci-*  
17                  *dent, and to safeguard information*  
18                  *that can be used to identify specific*  
19                  *persons from unintended disclosure or*  
20                  *unauthorized access or acquisition;*

21                  “(III) *shall be deemed to have vol-*  
22                  *untarily shared such cyber threat indi-*  
23                  *cators or defensive measures;*

24                  “(IV) *shall implement and utilize*  
25                  *a security control to protect against*

1 *unauthorized access to or acquisition of*  
2 *such cyber threat indicators or defen-*  
3 *sive measures; and*

4 “(V) *may not use such cyber*  
5 *threat indicators or defensive measures*  
6 *to engage in surveillance or other col-*  
7 *lection activities for the purpose of*  
8 *tracking an individual’s personally*  
9 *identifiable information.*

10 “(ii) *PROTECTIONS FOR INFORMA-*  
11 *TION.—The cyber threat indicators and de-*  
12 *fensive measures referred to in clause (i)—*

13 “(I) *are exempt from disclosure*  
14 *under section 552 of title 5, United*  
15 *States Code, and withheld, without dis-*  
16 *cretion, from the public under sub-*  
17 *section (b)(3)(B) of such section;*

18 “(II) *may not be used by the Fed-*  
19 *eral Government for regulatory pur-*  
20 *poses;*

21 “(III) *may not constitute a waiv-*  
22 *er of any applicable privilege or pro-*  
23 *tection provided by law, including*  
24 *trade secret protection;*

1           “(IV) shall be considered the com-  
2           mercial, financial, and proprietary in-  
3           formation of the non-Federal entity re-  
4           ferred to in clause (i) when so des-  
5           ignated by such non-Federal entity;  
6           and

7           “(V) may not be subject to a rule  
8           of any Federal entity or any judicial  
9           doctrine regarding *ex parte* commu-  
10          nications with a decisionmaking offi-  
11          cial.

12           “(C) STATE, LOCAL, OR TRIBAL GOVERN-  
13          MENT.—

14           “(i) USES OF INFORMATION.—A State,  
15          local, or tribal government that receives  
16          cyber threat indicators or defensive meas-  
17          ures from the Center from a Federal entity  
18          or a non-Federal entity—

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

23           “(II) shall, prior to such sharing,  
24          take reasonable efforts to remove infor-  
25          mation that can be used to identify

1           *specific persons and is reasonably be-*  
2           *lieved at the time of sharing to be un-*  
3           *related to a cybersecurity risk or inci-*  
4           *dent, and to safeguard information*  
5           *that can be used to identify specific*  
6           *persons from unintended disclosure or*  
7           *unauthorized access or acquisition;*

8           *“(III) shall consider such infor-*  
9           *mation the commercial, financial, and*  
10          *proprietary information of such Fed-*  
11          *eral entity or non-Federal entity if so*  
12          *designated by such Federal entity or*  
13          *non-Federal entity;*

14          *“(IV) shall be deemed to have vol-*  
15          *untarily shared such cyber threat indi-*  
16          *cators or defensive measures; and*

17          *“(V) shall implement and utilize*  
18          *a security control to protect against*  
19          *unauthorized access to or acquisition of*  
20          *such cyber threat indicators or defen-*  
21          *sive measures.*

22          *“(i) PROTECTIONS FOR INFORMA-*  
23          *TION.—The cyber threat indicators and de-*  
24          *fensive measures referred to in clause (i)—*

1                   “(I) shall be exempt from disclo-  
2                   sure under any State, local, or tribal  
3                   law or regulation that requires public  
4                   disclosure of information or records by  
5                   a public or quasi-public entity; and

6                   “(II) may not be used by any  
7                   State, local, or tribal government to  
8                   regulate a lawful activity of a non-  
9                   Federal entity.

10                   “(8) *LIABILITY EXEMPTIONS.*—

11                   “(A) *NETWORK AWARENESS.*—No cause of  
12                   action shall lie or be maintained in any court,  
13                   and such action shall be promptly dismissed,  
14                   against any non-Federal entity that, for cyberse-  
15                   curity purposes, conducts network awareness  
16                   under paragraph (4), if such network awareness  
17                   is conducted in accordance with such paragraph  
18                   and this section.

19                   “(B) *INFORMATION SHARING.*—No cause of  
20                   action shall lie or be maintained in any court,  
21                   and such action shall be promptly dismissed,  
22                   against any non-Federal entity that, for cyberse-  
23                   curity purposes, shares cyber threat indicators or  
24                   defensive measures under paragraph (3), or fails  
25                   to act based on such sharing, if such sharing is

1           *conducted in accordance with such paragraph*  
2           *and this section.*

3           “(C) *WILLFUL MISCONDUCT.*—

4                   “(i) *RULE OF CONSTRUCTION.*—*Noth-*  
5                   *ing in this section may be construed to—*

6                           “(I) *require dismissal of a cause*  
7                           *of action against a non-Federal entity*  
8                           *that has engaged in willful misconduct*  
9                           *in the course of conducting activities*  
10                           *authorized by this section; or*

11                           “(II) *undermine or limit the*  
12                           *availability of otherwise applicable*  
13                           *common law or statutory defenses.*

14                   “(ii) *PROOF OF WILLFUL MIS-*  
15                   *CONDUCT.*—*In any action claiming that*  
16                   *subparagraph (A) or (B) does not apply due*  
17                   *to willful misconduct described in clause (i),*  
18                   *the plaintiff shall have the burden of prov-*  
19                   *ing by clear and convincing evidence the*  
20                   *willful misconduct by each non-Federal en-*  
21                   *tity subject to such claim and that such*  
22                   *willful misconduct proximately caused in-*  
23                   *jury to the plaintiff.*

24                   “(iii) *WILLFUL MISCONDUCT DE-*  
25                   *FINED.*—*In this subsection, the term ‘willful*

1                    *misconduct’ means an act or omission that*  
2                    *is taken—*

3                    *“(I) intentionally to achieve a*  
4                    *wrongful purpose;*

5                    *“(II) knowingly without legal or*  
6                    *factual justification; and*

7                    *“(III) in disregard of a known or*  
8                    *obvious risk that is so great as to make*  
9                    *it highly probable that the harm will*  
10                   *outweigh the benefit.*

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

14                   *“(9) FEDERAL GOVERNMENT LIABILITY FOR VIO-*  
15                   *LATIONS OF RESTRICTIONS ON THE USE AND PROTEC-*  
16                   *TION OF VOLUNTARILY SHARED INFORMATION.—*

17                   *“(A) IN GENERAL.—If a department or*  
18                   *agency of the Federal Government intentionally*  
19                   *or willfully violates the restrictions specified in*  
20                   *paragraph (3), (6), or (7)(B) on the use and pro-*  
21                   *tection of voluntarily shared cyber threat indica-*  
22                   *tors or defensive measures, or any other provi-*  
23                   *sion of this section, the Federal Government shall*  
24                   *be liable to a person injured by such violation in*  
25                   *an amount equal to the sum of—*

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

4           “(ii) reasonable attorney fees as deter-  
5           mined by the court and other litigation  
6           costs reasonably occurred in any case under  
7           this subsection in which the complainant  
8           has substantially prevailed.

9           “(B) VENUE.—An action to enforce liability  
10          under this subsection may be brought in the dis-  
11          trict court of the United States in—

12           “(i) the district in which the complain-  
13          ant resides;

14           “(ii) the district in which the prin-  
15          cipal place of business of the complainant is  
16          located;

17           “(iii) the district in which the depart-  
18          ment or agency of the Federal Government  
19          that disclosed the information is located; or

20           “(iv) the District of Columbia.

21          “(C) STATUTE OF LIMITATIONS.—No action  
22          shall lie under this subsection unless such action  
23          is commenced not later than two years after the  
24          date of the violation of any restriction specified  
25          in paragraph (3), (6), or 7(B), or any other pro-



1 *vision of this section, that is the basis for such*  
2 *action.*

3 “(D) *EXCLUSIVE CAUSE OF ACTION.*—A  
4 *cause of action under this subsection shall be the*  
5 *exclusive means available to a complainant seek-*  
6 *ing a remedy for a violation of any restriction*  
7 *specified in paragraph (3), (6), or 7(B) or any*  
8 *other provision of this section.*

9 “(10) *ANTI-TRUST EXEMPTION.*—

10 “(A) *IN GENERAL.*—*Except as provided in*  
11 *subparagraph (C), it shall not be considered a*  
12 *violation of any provision of antitrust laws for*  
13 *two or more non-Federal entities to share a cyber*  
14 *threat indicator or defensive measure, or assist-*  
15 *ance relating to the prevention, investigation, or*  
16 *mitigation of a cybersecurity risk or incident, for*  
17 *cybersecurity purposes under this Act.*

18 “(B) *APPLICABILITY.*—*Subparagraph (A)*  
19 *shall apply only to information that is shared or*  
20 *assistance that is provided in order to assist*  
21 *with—*

22 “(i) *facilitating the prevention, inves-*  
23 *tigation, or mitigation of a cybersecurity*  
24 *risk or incident to an information system*

1           or information that is stored on, processed  
2           by, or transiting an information system; or  
3           “(ii) communicating or disclosing a  
4           cyber threat indicator or defensive measure  
5           to help prevent, investigate, or mitigate the  
6           effect of a cybersecurity risk or incident to  
7           an information system or information that  
8           is stored on, processed by, or transiting an  
9           information system.

10           “(C) *PROHIBITED CONDUCT.*—Nothing in  
11           this section may be construed to permit price-fix-  
12           ing, allocating a market between competitors,  
13           monopolizing or attempting to monopolize a  
14           market, or exchanges of price or cost informa-  
15           tion, customer lists, or information regarding fu-  
16           ture competitive planning.

17           “(11) *CONSTRUCTION AND PREEMPTION.*—

18           “(A) *OTHERWISE LAWFUL DISCLOSURES.*—  
19           Nothing in this section may be construed to limit  
20           or prohibit otherwise lawful disclosures of com-  
21           munications, records, or other information, in-  
22           cluding reporting of known or suspected criminal  
23           activity or participating voluntarily or under  
24           legal requirement in an investigation, by a non-

1           *Federal to any other non-Federal entity or Fed-*  
2           *eral entity under this section.*

3           “(B) *WHISTLE BLOWER PROTECTIONS.*—  
4           *Nothing in this section may be construed to pro-*  
5           *hibit or limit the disclosure of information pro-*  
6           *tected under section 2302(b)(8) of title 5, United*  
7           *States Code (governing disclosures of illegality,*  
8           *waste, fraud, abuse, or public health or safety*  
9           *threats), section 7211 of title 5, United States*  
10           *Code (governing disclosures to Congress), section*  
11           *1034 of title 10, United States Code (governing*  
12           *disclosure to Congress by members of the mili-*  
13           *tary), section 1104 of the National Security Act*  
14           *of 1947 (50 U.S.C. 3234) (governing disclosure*  
15           *by employees of elements of the intelligence com-*  
16           *munity), or any similar provision of Federal or*  
17           *State law.*

18           “(C) *RELATIONSHIP TO OTHER LAWS.*—  
19           *Nothing in this section may be construed to af-*  
20           *fect any requirement under any other provision*  
21           *of law for a non-Federal entity to provide infor-*  
22           *mation to a Federal entity.*

23           “(D) *PRESERVATION OF CONTRACTUAL OB-*  
24           *LIGATIONS AND RIGHTS.*—*Nothing in this section*  
25           *may be construed to—*

1           “(i) amend, repeal, or supersede any  
2           current or future contractual agreement,  
3           terms of service agreement, or other contrac-  
4           tual relationship between any non-Federal  
5           entities, or between any non-Federal entity  
6           and a Federal entity; or

7           “(ii) abrogate trade secret or intellec-  
8           tual property rights of any non-Federal en-  
9           tity or Federal entity.

10          “(E) ANTI-TASKING RESTRICTION.—Nothing  
11          in this section may be construed to permit a  
12          Federal entity to—

13               “(i) require a non-Federal entity to  
14               provide information to a Federal entity;

15               “(ii) condition the sharing of cyber  
16               threat indicators or defensive measures with  
17               a non-Federal entity on such non-Federal  
18               entity’s provision of cyber threat indicators  
19               or defensive measures to a Federal entity; or

20               “(iii) condition the award of any Fed-  
21               eral grant, contract, or purchase on the  
22               sharing of cyber threat indicators or defen-  
23               sive measures with a Federal entity.

24          “(F) NO LIABILITY FOR NON-PARTICIPA-  
25          TION.—Nothing in this section may be construed

1           to subject any non-Federal entity to liability for  
2           choosing to not engage in the voluntary activities  
3           authorized under this section.

4           “(G) *USE AND RETENTION OF INFORMA-*  
5           *TION.—Nothing in this section may be construed*  
6           *to authorize, or to modify any existing authority*  
7           *of, a department or agency of the Federal Gov-*  
8           *ernment to retain or use any information shared*  
9           *under this section for any use other than per-*  
10          *mitted in this section.*

11          “(H) *VOLUNTARY SHARING.—Nothing in*  
12          *this section may be construed to restrict or con-*  
13          *dition a non-Federal entity from sharing, for cy-*  
14          *bersecurity purposes, cyber threat indicators, de-*  
15          *fensive measures, or information related to cy-*  
16          *bersecurity risks or incidents with any other*  
17          *non-Federal entity, and nothing in this section*  
18          *may be construed as requiring any non-Federal*  
19          *entity to share cyber threat indicators, defensive*  
20          *measures, or information related to cybersecurity*  
21          *risks or incidents with the Center.*

22          “(I) *FEDERAL PREEMPTION.—This section*  
23          *supersedes any statute or other provision of law*  
24          *of a State or political subdivision of a State that*

1           *restricts or otherwise expressly regulates an ac-*  
2           *tivity authorized under this section.*

3           “(j) *DIRECT REPORTING.*—*The Secretary shall develop*  
4           *policies and procedures for direct reporting to the Secretary*  
5           *by the Director of the Center regarding significant cyberse-*  
6           *curity risks and incidents.*

7           “(k) *ADDITIONAL RESPONSIBILITIES.*—*The Secretary*  
8           *shall build upon existing mechanisms to promote a national*  
9           *awareness effort to educate the general public on the impor-*  
10          *tance of securing information systems.*

11          “(l) *REPORTS ON INTERNATIONAL COOPERATION.*—  
12          *Not later than 180 days after the date of the enactment of*  
13          *this subsection and periodically thereafter, the Secretary of*  
14          *Homeland Security shall submit to the Committee on*  
15          *Homeland Security of the House of Representatives and the*  
16          *Committee on Homeland Security and Governmental Af-*  
17          *airs of the Senate a report on the range of efforts underway*  
18          *to bolster cybersecurity collaboration with relevant inter-*  
19          *national partners in accordance with subsection (c)(8).*

20          “(m) *OUTREACH.*—*Not later than 60 days after the*  
21          *date of the enactment of this subsection, the Secretary, act-*  
22          *ing through the Under Secretary for Cybersecurity and In-*  
23          *frastructure Protection, shall—*

1           “(1) disseminate to the public information about  
2           how to voluntarily share cyber threat indicators and  
3           defensive measures with the Center; and

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

6   **SEC. 4. INFORMATION SHARING AND ANALYSIS ORGANIZA-**  
7                                   **TIONS.**

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

10           (1) in paragraph (5)—

11                   (A) in subparagraph (A)—

12                               (i) by inserting “information related to  
13                               cybersecurity risks and incidents and” after  
14                               “critical infrastructure information”; and

15                               (ii) by striking “related to critical in-  
16                               frastructure” and inserting “related to cy-  
17                               bersecurity risks, incidents, critical infra-  
18                               structure, and”;

19                   (B) in subparagraph (B)—

20                               (i) by striking “disclosing critical in-  
21                               frastructure information” and inserting  
22                               “disclosing cybersecurity risks, incidents,  
23                               and critical infrastructure information”;  
24                               and

1                   (ii) by striking “related to critical in-  
2                   frastructure or” and inserting “related to  
3                   cybersecurity risks, incidents, critical infra-  
4                   structure, or” and

5                   (C) in subparagraph (C), by striking “dis-  
6                   seminating critical infrastructure information”  
7                   and inserting “disseminating cybersecurity risks,  
8                   incidents, and critical infrastructure informa-  
9                   tion”; and

10                  (2) by adding at the end the following new para-  
11                  graph:

12                  “(8) *CYBERSECURITY RISK; INCIDENT.*—The  
13                  terms ‘cybersecurity risk’ and ‘incident’ have the  
14                  meanings given such terms in the second section 226  
15                  (relating to the National Cybersecurity and Commu-  
16                  nications Integration Center).”.

17 **SEC. 5. STREAMLINING OF DEPARTMENT OF HOMELAND SE-**  
18 **CURITY CYBERSECURITY AND INFRASTRUC-**  
19 **TURE PROTECTION ORGANIZATION.**

20                  (a) *CYBERSECURITY AND INFRASTRUCTURE PROTEC-*  
21 *TION.*—The National Protection and Programs Directorate  
22 of the Department of Homeland Security shall, after the  
23 date of the enactment of this Act, be known and designated  
24 as the “Cybersecurity and Infrastructure Protection”. Any  
25 reference to the National Protection and Programs Direc-



1 *torate of the Department in any law, regulation, map, doc-*  
2 *ument, record, or other paper of the United States shall be*  
3 *deemed to be a reference to the Cybersecurity and Infra-*  
4 *structure Protection of the Department.*

5 *(b) SENIOR LEADERSHIP OF CYBERSECURITY AND IN-*  
6 *FRAStructure PROTECTION.—*

7 *(1) IN GENERAL.—Subsection (a) of section 103*  
8 *of the Homeland Security Act of 2002 (6 U.S.C. 113)*  
9 *is amended—*

10 *(A) in paragraph (1)—*

11 *(i) by amending subparagraph (H) to*  
12 *read as follows:*

13 *“(H) An Under Secretary for Cybersecurity*  
14 *and Infrastructure Protection.”; and*

15 *(ii) by adding at the end the following*  
16 *new subparagraphs:*

17 *“(K) A Deputy Under Secretary for Cyber-*  
18 *security.*

19 *“(L) A Deputy Under Secretary for Infra-*  
20 *structure Protection.”; and*

21 *(B) by adding at the end the following new*  
22 *paragraph:*

23 *“(3) DEPUTY UNDER SECRETARIES.—The Dep-*  
24 *uty Under Secretaries referred to in subparagraphs*  
25 *(K) and (L) of paragraph (1) shall be appointed by*

1        *the President without the advice and consent of the*  
2        *Senate.”.*

3            (2) *CONTINUATION IN OFFICE.—The individuals*  
4        *who hold the positions referred in subparagraphs (H),*  
5        *(K), and (L) of paragraph (1) of section 103(a) the*  
6        *Homeland Security Act of 2002 (as amended and*  
7        *added by paragraph (1) of this subsection) as of the*  
8        *date of the enactment of this Act may continue to*  
9        *hold such positions.*

10          (c) *REPORT.—Not later than 90 days after the date*  
11        *of the enactment of this Act, the Under Secretary for Cyber-*  
12        *security and Infrastructure Protection of the Department*  
13        *of Homeland Security shall submit to the Committee on*  
14        *Homeland Security of the House of Representatives and the*  
15        *Committee on Homeland Security and Governmental Af-*  
16        *airs of the Senate a report on the feasibility of becoming*  
17        *an operational component, including an analysis of alter-*  
18        *natives, and if a determination is rendered that becoming*  
19        *an operational component is the best option for achieving*  
20        *the mission of Cybersecurity and Infrastructure Protection,*  
21        *a legislative proposal and implementation plan for becom-*  
22        *ing such an operational component. Such report shall also*  
23        *include plans to more effectively carry out the cybersecurity*  
24        *mission of Cybersecurity and Infrastructure Protection, in-*  
25        *cluding expediting information sharing agreements.*

1 **SEC. 6. CYBER INCIDENT RESPONSE PLANS.**

2 (a) *IN GENERAL.*—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 149) is amended—

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

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

8 “(a) *IN GENERAL.*—The Under Secretary for Cybersecurity and Infrastructure Protection shall”; and

11 (3) *by adding at the end the following new subsection:*

13 “(b) *UPDATES TO THE CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.*—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (a), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.”.

21 (b) *CLERICAL AMENDMENT.*—The table of contents of the Homeland Security Act of 2002 is amended by amending the item relating to section 227 to read as follows:

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

1 **SEC. 7. 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 amended*  
6 *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 In-*  
10 *tegration Center, in coordination with the Office of Emer-*  
11 *gency Communications of the Department, shall assess and*  
12 *evaluate consequence, vulnerability, and threat information*  
13 *regarding cyber incidents to public safety communications*  
14 *to help facilitate continuous improvements to the security*  
15 *and resiliency of such communications.*

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

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

24 “(1) *Public service announcements targeted at*  
25 *improving awareness among State, local, and tribal*  
26 *governments, the private sector, academia, and stake-*

1       *holders in specific audiences, including the elderly,*  
 2       *students, small businesses, members of the Armed*  
 3       *Forces, and veterans.*

4               “(2) *Vendor and technology-neutral voluntary*  
 5       *best practices information.*”

6       “(b) *CONSULTATION.—The Under Secretary for Cyber-*  
 7       *security and Infrastructure Protection shall consult with a*  
 8       *wide range of stakeholders in government, industry, aca-*  
 9       *demia, and the non-profit community in carrying out this*  
 10       *section.*”.

11       “(b) *CLERICAL AMENDMENT.—The table of contents of*  
 12       *the Homeland Security Act of 2002 is amended by inserting*  
 13       *after the item relating to section 226 (relating to cybersecu-*  
 14       *rity recruitment and retention) the following new items:*

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

      “*Sec. 231. Cybersecurity awareness campaign.*”.

15       **SEC. 8. CRITICAL INFRASTRUCTURE PROTECTION RE-**  
 16               **SEARCH AND DEVELOPMENT.**

17       “(a) *STRATEGIC PLAN; PUBLIC-PRIVATE CONSOR-*  
 18       *TIUMS.—Title III of the Homeland Security Act of 2002*  
 19       *(6 U.S.C. 181 et seq.) is amended by adding at the end*  
 20       *the following new section:*

21       **“SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR**  
 22               **CRITICAL INFRASTRUCTURE PROTECTION.**

23       “(a) *IN GENERAL.—Not later than 180 days after the*  
 24       *date of enactment of this section, the Secretary, acting*

1 *through the Under Secretary for Science and Technology,*  
2 *shall submit to Congress a strategic plan to guide the overall*  
3 *direction of Federal physical security and cybersecurity*  
4 *technology research and development efforts for protecting*  
5 *critical infrastructure, including against all threats. Such*  
6 *plan shall be updated and submitted to Congress every two*  
7 *years.*

8       “(b) *CONTENTS OF PLAN.*—*The strategic plan, includ-*  
9 *ing biennial updates, required under subsection (a) shall*  
10 *include the following:*

11               “(1) *An identification of critical infrastructure*  
12 *security risks and any associated security technology*  
13 *gaps, that are developed following—*

14                       “(A) *consultation with stakeholders, includ-*  
15 *ing critical infrastructure Sector Coordinating*  
16 *Councils; and*

17                       “(B) *performance by the Department of a*  
18 *risk and gap analysis that considers information*  
19 *received in such consultations.*

20               “(2) *A set of critical infrastructure security tech-*  
21 *nology needs that—*

22                       “(A) *is prioritized based on the risks and*  
23 *gaps identified under paragraph (1);*

24                       “(B) *emphasizes research and development*  
25 *of technologies that need to be accelerated due to*

1           *rapidly evolving threats or rapidly advancing*  
2           *infrastructure technology; and*

3           “(C) *includes research, development, and*  
4           *acquisition roadmaps with clearly defined objec-*  
5           *tives, goals, and measures.*

6           “(3) *An identification of laboratories, facilities,*  
7           *modeling, and simulation capabilities that will be re-*  
8           *quired to support the research, development, dem-*  
9           *onstration, testing, evaluation, and acquisition of the*  
10          *security technologies described in paragraph (2).*

11          “(4) *An identification of current and planned*  
12          *programmatic initiatives for fostering the rapid ad-*  
13          *vancement and deployment of security technologies for*  
14          *critical infrastructure protection, including a consid-*  
15          *eration of opportunities for public-private partner-*  
16          *ships, intragovernment collaboration, university cen-*  
17          *ters of excellence, and national laboratory technology*  
18          *transfer.*

19          “(5) *A description of progress made with respect*  
20          *to each critical infrastructure security risk, associated*  
21          *security technology gap, and critical infrastructure*  
22          *technology need identified in the preceding strategic*  
23          *plan required under subsection (a).*

24          “(c) *COORDINATION.—In carrying out this section, the*  
25          *Under Secretary for Science and Technology shall coordi-*

1 *nate with the Under Secretary for the National Protection*  
 2 *and Programs Directorate.*

3 “(d) *CONSULTATION.*—*In carrying out this section, the*  
 4 *Under Secretary for Science and Technology shall consult*  
 5 *with—*

6 “(1) *critical infrastructure Sector Coordinating*  
 7 *Councils;*

8 “(2) *to the extent practicable, subject matter ex-*  
 9 *erts on critical infrastructure protection from uni-*  
 10 *versities, colleges, national laboratories, and private*  
 11 *industry;*

12 “(3) *the heads of other relevant Federal depart-*  
 13 *ments and agencies that conduct research and devel-*  
 14 *opment relating to critical infrastructure protection;*  
 15 *and*

16 “(4) *State, local, and tribal governments, as ap-*  
 17 *propriate.”.*

18 (b) *CLERICAL AMENDMENT.*—*The table of contents of*  
 19 *the Homeland Security Act of 2002 is amended by inserting*  
 20 *after the item relating to section 317 the following new item:*

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

21 **SEC. 9. REPORT ON REDUCING CYBERSECURITY RISKS IN**  
 22 **DHS DATA CENTERS.**

23 *Not later than one year after the date of the enactment*  
 24 *of this Act, the Secretary of Homeland Security shall sub-*



1 *mit to the Committee on Homeland Security of the House*  
2 *of Representatives and the Committee on Homeland Secu-*  
3 *rity and Governmental Affairs of the Senate a report on*  
4 *the feasibility of the Department of Homeland Security cre-*  
5 *ating an environment for the reduction in cybersecurity*  
6 *risks in Department data centers, including by increasing*  
7 *compartmentalization between systems, and providing a*  
8 *mix of security controls between such compartments.*

9 **SEC. 10. ASSESSMENT.**

10 *Not later than two years after the date of the enact-*  
11 *ment of this Act, the Comptroller General of the United*  
12 *States shall submit to the Committee on Homeland Security*  
13 *of the House of Representatives and the Committee on*  
14 *Homeland Security and Governmental Affairs of the Senate*  
15 *a report that contains an assessment of the implementation*  
16 *by the Secretary of Homeland Security of this Act and the*  
17 *amendments made by this Act and, to the extent prac-*  
18 *ticable, findings regarding increases in the sharing of cyber*  
19 *threat indicators, defensive measures, and information re-*  
20 *lating to cybersecurity risks and incidents at the National*  
21 *Cybersecurity and Communications Integration Center and*  
22 *throughout the United States.*

23 **SEC. 11. CONSULTATION.**

24 *The Under Secretary for Cybersecurity and Infrastruc-*  
25 *ture Protection shall produce a report on the feasibility of*

1 *creating a risk-informed prioritization plan should mul-*  
2 *tiple critical infrastructures experience cyber incidents si-*  
3 *multaneously.*

4 **SEC. 12. TECHNICAL ASSISTANCE.**

5 *The Inspector General of the Department of Homeland*  
6 *Security shall review the operations of the United States*  
7 *Computer Emergency Readiness Team (US-CERT) and the*  
8 *Industrial Control Systems Cyber Emergency Response*  
9 *Team (ICS-CERT) to assess the capacity to provide tech-*  
10 *nical assistance to non-Federal entities and to adequately*  
11 *respond to potential increases in requests for technical as-*  
12 *sistance.*

13 **SEC. 13. PROHIBITION ON NEW REGULATORY AUTHORITY.**

14 *Nothing in this Act or the amendments made by this*  
15 *Act may be construed to grant the Secretary of Homeland*  
16 *Security any authority to promulgate regulations or set*  
17 *standards relating to the cybersecurity of non-Federal enti-*  
18 *ties, not including State, local, and tribal governments, that*  
19 *was not in effect on the day before the date of the enactment*  
20 *of this Act.*

21 **SEC. 14. SUNSET.**

22 *Any requirements for reports required by this Act or*  
23 *the amendments made by this Act shall terminate on the*  
24 *date that is seven years after the date of the enactment of*  
25 *this Act.*

1 **SEC. 15. PROHIBITION ON NEW FUNDING.**

2       *No funds are authorized to be appropriated to carry*  
3 *out this Act and the amendments made by this Act. This*  
4 *Act and such amendments shall be carried out using*  
5 *amounts appropriated or otherwise made available for such*  
6 *purposes.*

Union Calendar No. 61

114<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session

**H. R. 1731**

[Report No. 114-83]

---

---

**A BILL**

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.

---

---

APRIL 17, 2015

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