

114TH CONGRESS
1ST SESSION

H. R. 1731

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

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 COMMUNICA-**
7 **TIONS INTEGRATION CENTER.**

8 (a) DEFINITIONS.—

1 (1) IN GENERAL.—Subsection (a) of the second
2 section 226 of the Homeland Security Act of 2002
3 (6 U.S.C. 148; relating to the National Cybersecu-
4 rity and Communications Integration Center) is
5 amended—

6 (A) in paragraph (3), by striking “and” at
7 the end;

8 (B) in paragraph (4), by striking the pe-
9 riod at the end and inserting “; and”; and

10 (C) by adding at the end the following new
11 paragraphs:

12 “(5) the term ‘cyber threat indicator’ means
13 technical information that is necessary to describe or
14 identify—

15 “(A) a method for probing, monitoring,
16 maintaining, or establishing network awareness
17 of an information system for the purpose of dis-
18 cerning technical vulnerabilities of such infor-
19 mation system, if such method is known or rea-
20 sonably suspected of being associated with a
21 known or suspected cybersecurity risk, includ-
22 ing communications that reasonably appear to
23 be transmitted for the purpose of gathering
24 technical information related to a cybersecurity
25 risk;

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

3 “(C) a technical vulnerability, including
4 anomalous technical behavior that may become
5 a vulnerability;

6 “(D) a method of causing a user with le-
7 gitimate access to an information system or in-
8 formation that is stored on, processed by, or
9 transiting an information system to inadvert-
10 ently enable the defeat of a technical or oper-
11 ational control;

12 “(E) a method for unauthorized remote
13 identification of, access to, or use of an infor-
14 mation system or information that is stored on,
15 processed by, or transiting an information sys-
16 tem that is known or reasonably suspected of
17 being associated with a known or suspected cy-
18 bersecurity risk;

19 “(F) the actual or potential harm caused
20 by a cybersecurity risk, including a description
21 of the information exfiltrated as a result of a
22 particular cybersecurity risk;

23 “(G) any other attribute of a cybersecurity
24 risk that cannot be used to identify specific per-
25 sons reasonably believed to be unrelated to such

1 cybersecurity risk, if disclosure of such at-
2 tribute is not otherwise prohibited by law; or

3 “(H) any combination of subparagraphs
4 (A) through (G);

5 “(6) the term ‘cybersecurity purpose’ means the
6 purpose of protecting an information system or in-
7 formation that is stored on, processed by, or
8 transiting an information system from a cybersecu-
9 rity risk or incident;

10 “(7)(A) except as provided in subparagraph
11 (B), the term ‘defensive measure’ means an action,
12 device, procedure, signature, technique, or other
13 measure applied to an information system or infor-
14 mation that is stored on, processed by, or transiting
15 an information system that detects, prevents, or
16 mitigates a known or suspected cybersecurity risk or
17 incident, or any attribute of hardware, software,
18 process, or procedure that could enable or facilitate
19 the defeat of a security control;

20 “(B) such term does not include a measure that
21 destroys, renders unusable, or substantially harms
22 an information system or data on an information
23 system not belonging to—

1 “(i) the non-Federal entity, not including a
2 State, local, or tribal government, operating
3 such measure; or

4 “(ii) another Federal entity or non-Federal
5 entity that is authorized to provide consent and
6 has provided such consent to the non-Federal
7 entity referred to in clause (i);

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

12 “(9)(A) the term ‘private entity’ means a non-
13 Federal entity that is an individual or private group,
14 organization, proprietorship, partnership, trust, co-
15 operative, corporation, or other commercial or non-
16 profit entity, including an officer, employee, or agent
17 thereof;

18 “(B) such term includes a component of a
19 State, local, or tribal government performing electric
20 utility services;

21 “(10) the term ‘security control’ means the
22 management, operational, and technical controls
23 used to protect against an unauthorized effort to ad-
24 versely affect the confidentiality, integrity, or avail-
25 ability of an information system or information that

1 is stored on, processed by, or transiting an informa-
2 tion system; and

3 “(11) the term ‘sharing’ means providing, re-
4 ceiving, and disseminating.”.

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

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

10 (2) in clause (ii)—

11 (A) by inserting “, including information
12 sharing and analysis centers” before the semi-
13 colon; and

14 (B) by striking “and” at the end;

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

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

19 “(iv) private entities.”.

20 **SEC. 3. INFORMATION SHARING STRUCTURE AND PROC-**
21 **ESSES.**

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

1 (1) in subsection (c)—

2 (A) in paragraph (1)—

3 (i) by striking “a Federal civilian
4 interface” and inserting “the lead Federal
5 civilian interface”; and

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

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

12 (C) in paragraph (5)(A), by striking “cy-
13 bersecurity risks” and inserting “cyber threat
14 indicators, defensive measures, cybersecurity
15 risks,”;

16 (D) in paragraph (6)—

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

21 (ii) by striking “and” at the end;

22 (E) in paragraph (7)—

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

1 (ii) in subparagraph (B), by striking
2 the period at the end and inserting “;
3 and”; and

4 (iii) by adding at the end the fol-
5 lowing new subparagraph:

6 “(C) sharing cyber threat indicators and
7 defensive measures;” and

8 (F) by adding at the end the following new
9 paragraphs:

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

12 “(A) collaborate on cyber threat indicators,
13 defensive measures, and information related to
14 cybersecurity risks and incidents; and

15 “(B) enhance the security and resilience of
16 global cybersecurity;

17 “(9) sharing cyber threat indicators, defensive
18 measures, and other information related to cyberse-
19 curity risks and incidents with Federal and non-Fed-
20 eral entities, including across sectors of critical in-
21 frastructure;

22 “(10) promptly notifying the Secretary and the
23 Committee on Homeland Security of the House of
24 Representatives and the Committee on Homeland
25 Security and Governmental Affairs of the Senate of

1 any significant violations of the policies and proce-
2 dures specified in subsection (i)(6)(A); and

3 “(11) promptly notifying non-Federal entities
4 that have shared cyber threat indicators or defensive
5 measures that are known or determined to be in
6 error or in contravention of the requirements of this
7 section.”;

8 (2) in subsection (d)—

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

11 (B) by redesignating subparagraph (E) as
12 subparagraph (I); and

13 (C) by inserting after subparagraph (D)
14 the following new subparagraphs:

15 “(E) an entity that collaborates with State
16 and local governments on cybersecurity risks
17 and incidents, and has entered into a voluntary
18 information sharing relationship with the Cen-
19 ter;

20 “(F) a United States Computer Emer-
21 gency Readiness Team that coordinates infor-
22 mation related to cybersecurity risks and inci-
23 dents, proactively and collaboratively addresses
24 cybersecurity risks and incidents to the United
25 States, collaboratively responds to cybersecurity

1 risks and incidents, provides technical assist-
2 ance, upon request, to information system own-
3 ers and operators, and shares cyber threat indi-
4 cators, defensive measures, or information re-
5 lated to cybersecurity risks and incidents in a
6 timely manner;

7 “(G) the Industrial Control System Cyber
8 Emergency Response Team that—

9 “(i) coordinates with industrial con-
10 trol systems owners and operators;

11 “(ii) provides training, upon request,
12 to Federal entities and non-Federal enti-
13 ties on industrial control systems cyberse-
14 curity;

15 “(iii) collaboratively addresses cyber-
16 security risks and incidents to industrial
17 control systems;

18 “(iv) provides technical assistance,
19 upon request, to Federal entities and non-
20 Federal entities relating to industrial con-
21 trol systems cybersecurity; and

22 “(v) shares cyber threat indicators,
23 defensive measures, or information related
24 to cybersecurity risks and incidents of in-

1 industrial control systems in a timely fash-
2 ion;

3 “(H) a National Coordinating Center for
4 Communications that coordinates the protec-
5 tion, response, and recovery of emergency com-
6 munications; and”;

7 (3) in subsection (e)—

8 (A) in paragraph (1)—

9 (i) in subparagraph (A), by inserting
10 “cyber threat indicators, defensive meas-
11 ures, and” before “information”;

12 (ii) in subparagraph (B), by inserting
13 “cyber threat indicators, defensive meas-
14 ures, and” before “information”;

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

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

23 (B) in paragraph (2)—

24 (i) by striking “cybersecurity risks”
25 and inserting “cyber threat indicators, de-

1 fensive measures, cybersecurity risks,”;
2 and

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

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

11 (4) by adding at the end the following new sub-
12 sections:

13 “(g) RAPID AUTOMATED SHARING.—

14 “(1) IN GENERAL.—The Under Secretary for
15 Cybersecurity and Infrastructure Protection, in co-
16 ordination with industry and other stakeholders,
17 shall develop capabilities based on standards and
18 widely used approaches in the information tech-
19 nology industry that support and rapidly advance
20 the development, adoption, and implementation of
21 automated mechanisms for the timely sharing of
22 cyber threat indicators and defensive measures to
23 and from the Center and with each Federal agency
24 designated as the ‘Sector Specific Agency’ for each

1 critical infrastructure sector in accordance with sub-
2 section (h).

3 “(2) BIENNIAL REPORT.—The Under Sec-
4 retary for Cybersecurity and Infrastructure Protec-
5 tion shall submit to the Committee on Homeland Se-
6 curity of the House of Representatives and the Com-
7 mittee on Homeland Security and Governmental Af-
8 fairs of the Senate a biennial report on the status
9 and progress of the development of the capability de-
10 scribed in paragraph (1). Such reports shall be re-
11 quired until such capability is fully implemented.

12 “(h) SECTOR SPECIFIC AGENCIES.—The Secretary,
13 in collaboration with the relevant critical infrastructure
14 sector and the heads of other appropriate Federal agen-
15 cies, shall recognize the Federal agency designated as of
16 March 25, 2015, as the ‘Sector Specific Agency’ for each
17 critical infrastructure sector designated in the Depart-
18 ment’s National Infrastructure Protection Plan. If the
19 designated Sector Specific Agency for a particular critical
20 infrastructure sector is the Department, for purposes of
21 this section, the Secretary is deemed to be the head of
22 such Sector Specific Agency and shall carry out this sec-
23 tion. The Secretary, in coordination with the heads of each
24 such Sector Specific Agency, shall—

1 “(1) support the security and resilience activities
2 of the relevant critical infrastructure sector in ac-
3 cordance with this section;

4 “(2) provide institutional knowledge, specialized
5 expertise, and technical assistance upon request to
6 the relevant critical infrastructure sector; and

7 “(3) support the timely sharing of cyber threat
8 indicators and defensive measures with the relevant
9 critical infrastructure sector with the Center in ac-
10 cordance with this section.

11 “(i) VOLUNTARY INFORMATION SHARING PROCE-
12 DURES.—

13 “(1) PROCEDURES.—

14 “(A) IN GENERAL.—The Center may enter
15 into a voluntary information sharing relation-
16 ship with any consenting non-Federal entity for
17 the sharing of cyber threat indicators and de-
18 fensive measures for cybersecurity purposes in
19 accordance with this section. Nothing in this
20 section may be construed to require any non-
21 Federal entity to enter into any such informa-
22 tion sharing relationship with the Center or any
23 other entity. The Center may terminate a vol-
24 untary information sharing relationship under
25 this subsection if the Center determines that

1 the non-Federal entity with which the Center
2 has entered into such a relationship has, after
3 repeated notice, repeatedly and intentionally
4 violated the terms of this subsection.

5 “(B) NATIONAL SECURITY.—The Sec-
6 retary may decline to enter into a voluntary in-
7 formation sharing relationship under this sub-
8 section if the Secretary determines that such is
9 appropriate for national security.

10 “(2) VOLUNTARY INFORMATION SHARING RELA-
11 TIONSHIPS.—A voluntary information sharing rela-
12 tionship under this subsection may be characterized
13 as an agreement described in this paragraph.

14 “(A) STANDARD AGREEMENT.—For the
15 use of a non-Federal entity, the Center shall
16 make available a standard agreement, con-
17 sistent with this section, on the Department’s
18 website.

19 “(B) NEGOTIATED AGREEMENT.—At the
20 request of a non-Federal entity, and if deter-
21 mined appropriate by the Center, the Depart-
22 ment shall negotiate a non-standard agreement,
23 consistent with this section.

24 “(C) EXISTING AGREEMENTS.—An agree-
25 ment between the Center and a non-Federal en-

1 tity that is entered into before the date of the
2 enactment of this section, or such an agreement
3 that is in effect before such date, shall be
4 deemed in compliance with the requirements of
5 this subsection, notwithstanding any other pro-
6 vision or requirement of this subsection. An
7 agreement under this subsection shall include
8 the relevant privacy protections as in effect
9 under the Cooperative Research and Develop-
10 ment Agreement for Cybersecurity Information
11 Sharing and Collaboration, as of December 31,
12 2014. Nothing in this subsection may be con-
13 strued to require a non-Federal entity to enter
14 into either a standard or negotiated agreement
15 to be in compliance with this subsection.

16 “(3) INFORMATION SHARING AUTHORIZA-
17 TION.—

18 “(A) IN GENERAL.—Except as provided in
19 subparagraph (B), and notwithstanding any
20 other provision of law, a non-Federal entity
21 may, for cybersecurity purposes, share cyber
22 threat indicators or defensive measures ob-
23 tained on its own information system, or on an
24 information system of another Federal entity or
25 non-Federal entity, upon written consent of

1 such other Federal entity or non-Federal entity
2 or an authorized representative of such other
3 Federal entity or non-Federal entity in accord-
4 ance with this section with—

5 “(i) another non-Federal entity; or

6 “(ii) the Center, as provided in this
7 section.

8 “(B) **LAWFUL RESTRICTION.**—A non-Fed-
9 eral entity receiving a cyber threat indicator or
10 defensive measure from another Federal entity
11 or non-Federal entity shall comply with other-
12 wise lawful restrictions placed on the sharing or
13 use of such cyber threat indicator or defensive
14 measure by the sharing Federal entity or non-
15 Federal entity.

16 “(C) **REMOVAL OF INFORMATION UNRE-**
17 **LATED TO CYBERSECURITY RISKS OR INCI-**
18 **DENTS.**—Federal entities and non-Federal enti-
19 ties shall, prior to such sharing, take reasonable
20 efforts to remove information that can be used
21 to identify specific persons and is reasonably
22 believed at the time of sharing to be unrelated
23 to a cybersecurity risks or incident and to safe-
24 guard information that can be used to identify

1 specific persons from unintended disclosure or
2 unauthorized access or acquisition.

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

5 “(i) limit or modify an existing infor-
6 mation sharing relationship;

7 “(ii) prohibit a new information shar-
8 ing relationship;

9 “(iii) require a new information shar-
10 ing relationship between any non-Federal
11 entity and a Federal entity;

12 “(iv) limit otherwise lawful activity; or

13 “(v) in any manner impact or modify
14 procedures in existence as of the date of
15 the enactment of this section for reporting
16 known or suspected criminal activity to ap-
17 propriate law enforcement authorities or
18 for participating voluntarily or under legal
19 requirement in an investigation.

20 “(4) NETWORK AWARENESS AUTHORIZATION.—

21 “(A) IN GENERAL.—Notwithstanding any
22 other provision of law, a non-Federal entity, not
23 including a State, local, or tribal government,
24 may, for cybersecurity purposes, conduct net-
25 work awareness of—

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

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

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

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

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

21 “(i) authorize conducting network
22 awareness of an information system, or the
23 use of any information obtained through
24 such conducting of network awareness,
25 other than as provided in this section; or

1 “(ii) limit otherwise lawful activity.

2 “(5) DEFENSIVE MEASURE AUTHORIZATION.—

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

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

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

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

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

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

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

9 “(ii) limit otherwise lawful activity.

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

12 “(A) POLICIES AND PROCEDURES.—

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

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

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

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

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

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

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

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

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

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

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

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

15 “(B) IMPLEMENTATION.—The Chief Pri-
16 vacy Officer of the Department, on an ongoing
17 basis, shall—

18 “(i) monitor the implementation of
19 the policies and procedures governing the
20 sharing of cyber threat indicators and de-
21 fensive measures established pursuant to
22 clause (i) of subparagraph (A);

23 “(ii) regularly review and update pri-
24 vacy impact assessments, as appropriate,

1 to ensure all relevant constitutional, legal,
2 and privacy protections are being followed;

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

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

15 “(v) ensure there are appropriate
16 sanctions in place for officers, employees,
17 or agents of the Department who inten-
18 tionally or willfully conduct activities under
19 this section in an unauthorized manner.

20 “(C) INSPECTOR GENERAL REPORT.—The
21 Inspector General of the Department, in con-
22 sultation with the Privacy and Civil Liberties
23 Oversight Board and the Inspector General of
24 each Federal agency that receives cyber threat
25 indicators or defensive measures shared with

1 the Center under this section, shall, not later
2 than two years after the date of the enactment
3 of this subsection and periodically thereafter
4 submit to the Committee on Homeland Security
5 of the House of Representatives and the Com-
6 mittee on Homeland Security and Govern-
7 mental Affairs of the Senate a report con-
8 taining a review of the use of cybersecurity risk
9 information shared with the Center, including
10 the following:

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

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

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

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

24 “(v) The appropriate metrics that
25 exist to determine the impact, if any, on

1 privacy and civil liberties as a result of the
2 sharing of such information with the Cen-
3 ter.

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

6 “(vii) A review of the sharing of such
7 information within the Federal Govern-
8 ment to identify inappropriate stove piping
9 of such information.

10 “(viii) Any recommendations of the
11 Inspector General of the Department for
12 improvements or modifications to informa-
13 tion sharing under this section.

14 “(D) PRIVACY AND CIVIL LIBERTIES OFFI-
15 CERS REPORT.—The Chief Privacy Officer and
16 the Chief Civil Rights and Civil Liberties Offi-
17 cer of the Department, in consultation with the
18 Privacy and Civil Liberties Oversight Board,
19 the Inspector General of the Department, and
20 the senior privacy and civil liberties officer of
21 each Federal agency that receives cyber threat
22 indicators and defensive measures shared with
23 the Center under this section, shall biennially
24 submit to the appropriate congressional com-
25 mittees a report assessing the privacy and civil

1 liberties impact of the activities under this
2 paragraph. Each such report shall include any
3 recommendations the Chief Privacy Officer and
4 the Chief Civil Rights and Civil Liberties Offi-
5 cer of the Department consider appropriate to
6 minimize or mitigate the privacy and civil lib-
7 erties impact of the sharing of cyber threat in-
8 dicators and defensive measures under this sec-
9 tion.

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 INFORMA-
15 TION.—

16 “(A) NON-FEDERAL ENTITIES.—A non-
17 Federal entity, not including a State, local, or
18 tribal government, that shares cyber threat in-
19 dicators or defensive measures through the Cen-
20 ter or otherwise under this section—

21 “(i) may use, retain, or further dis-
22 close such cyber threat indicators or defen-
23 sive measures solely for cybersecurity pur-
24 poses;

1 “(ii) shall, prior to such sharing, take
2 reasonable efforts to remove information
3 that can be used to identify specific per-
4 sons and is reasonably believed at the time
5 of sharing to be unrelated to a cybersecu-
6 rity risk or incident, and to safeguard in-
7 formation that can be used to identify spe-
8 cific persons from unintended disclosure or
9 unauthorized access or acquisition;

10 “(iii) shall comply with appropriate
11 restrictions that a Federal entity or non-
12 Federal entity places on the subsequent
13 disclosure or retention of cyber threat indi-
14 cators and defensive measures that it dis-
15 closes to other Federal entities or non-Fed-
16 eral entities;

17 “(iv) shall be deemed to have volun-
18 tarily shared such cyber threat indicators
19 or defensive measures;

20 “(v) shall implement and utilize a se-
21 curity control to protect against unauthor-
22 ized access to or acquisition of such cyber
23 threat indicators or defensive measures;
24 and

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

4 “(B) FEDERAL ENTITIES.—

5 “(i) USES OF INFORMATION.—A Fed-
6 eral entity that receives cyber threat indi-
7 cators or defensive measures shared
8 through the Center or otherwise under this
9 section from another Federal entity or a
10 non-Federal entity—

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

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

1 “(III) shall be deemed to have
2 voluntarily shared such cyber threat
3 indicators or defensive measures; and

4 “(IV) shall implement and utilize
5 a security control to protect against
6 unauthorized access to or acquisition
7 of such cyber threat indicators or de-
8 fensive measures.

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

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

17 “(II) may not be used by the
18 Federal Government for regulatory
19 purposes;

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

24 “(IV) shall be considered the
25 commercial, financial, and proprietary

1 information of the non-Federal entity
2 referred to in clause (i) when so des-
3 ignated by such non-Federal entity;
4 and

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

10 “(C) STATE, LOCAL, OR TRIBAL GOVERN-
11 MENT.—

12 “(i) USES OF INFORMATION.—A
13 State, local, or tribal government that re-
14 ceives cyber threat indicators or defensive
15 measures from the Center from a Federal
16 entity or a non-Federal entity—

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

21 “(II) shall, prior to such sharing,
22 take reasonable efforts to remove in-
23 formation that can be used to identify
24 specific persons and is reasonably be-
25 lieved at the time of sharing to be un-

1 related to a cybersecurity risk or inci-
2 dent, and to safeguard information
3 that can be used to identify specific
4 persons from unintended disclosure or
5 unauthorized access or acquisition;

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

12 “(IV) shall be deemed to have
13 voluntarily shared such cyber threat
14 indicators or defensive measures; and

15 “(V) shall implement and utilize
16 a security control to protect against
17 unauthorized access to or acquisition
18 of such cyber threat indicators or de-
19 fensive measures.

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

23 “(I) shall be exempt from disclo-
24 sure under any State, local, or tribal
25 law or regulation that requires public

1 disclosure of information or records
2 by a public or quasi-public entity; and

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

7 “(8) LIABILITY EXEMPTIONS.—

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

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

1 “(C) WILLFUL MISCONDUCT.—

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

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

9 “(II) undermine or limit the
10 availability of otherwise applicable
11 common law or statutory defenses.

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

22 “(iii) WILLFUL MISCONDUCT DE-
23 FINED.—In this subsection, the term ‘will-
24 ful misconduct’ means an act or omission
25 that is taken—

1 “(I) intentionally to achieve a
2 wrongful purpose;

3 “(II) knowingly without legal or
4 factual justification; and

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

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

12 “(9) FEDERAL GOVERNMENT LIABILITY FOR
13 VIOLATIONS OF RESTRICTIONS ON THE USE AND
14 PROTECTION OF VOLUNTARILY SHARED INFORMA-
15 TION.—

16 “(A) IN GENERAL.—If a department or
17 agency of the Federal Government intentionally
18 or willfully violates the restrictions specified in
19 paragraph (3), (6), or (7)(B) on the use and
20 protection of voluntarily shared cyber threat in-
21 dicators or defensive measures, or any other
22 provision of this section, the Federal Govern-
23 ment shall be liable to a person injured by such
24 violation in 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
7 under this subsection in which the com-
8 plainant has substantially prevailed.

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

12 “(i) the district in which the com-
13 plainant resides;

14 “(ii) the district in which the principal
15 place of business of the complainant is lo-
16 cated;

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 ac-
22 tion shall lie under this subsection unless such
23 action is commenced not later than two years
24 after the date of the violation of any restriction
25 specified in paragraph (3), (6), or 7(B), or any

1 other provision of this section, that is the basis
2 for such action.

3 “(D) EXCLUSIVE CAUSE OF ACTION.—A
4 cause of action under this subsection shall be
5 the exclusive means available to a complainant
6 seeking a remedy for a violation of any restric-
7 tion specified in paragraph (3), (6), or 7(B) or
8 any 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
14 cyber threat indicator or defensive measure, or
15 assistance relating to the prevention, investiga-
16 tion, or mitigation of a cybersecurity risk or in-
17 cident, for cybersecurity purposes under this
18 Act.

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

23 “(i) facilitating the prevention, inves-
24 tigation, or mitigation of a cybersecurity
25 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-
12 fixing, 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
16 future competitive planning.

17 “(11) CONSTRUCTION AND PREEMPTION.—

18 “(A) OTHERWISE LAWFUL DISCLO-
19 SURES.—Nothing in this section may be con-
20 strued to limit or prohibit otherwise lawful dis-
21 closures of communications, records, or other
22 information, including reporting of known or
23 suspected criminal activity or participating vol-
24 untarily or under legal requirement in an inves-
25 tigation, by a non-Federal to any other non-

1 Federal entity or Federal entity under this sec-
2 tion.

3 “(B) WHISTLEBLOWER PROTECTIONS.—
4 Nothing in this section may be construed to
5 prohibit or limit the disclosure of information
6 protected under section 2302(b)(8) of title 5,
7 United States Code (governing disclosures of il-
8 legality, waste, fraud, abuse, or public health or
9 safety threats), section 7211 of title 5, United
10 States Code (governing disclosures to Con-
11 gress), section 1034 of title 10, United States
12 Code (governing disclosure to Congress by
13 members of the military), section 1104 of the
14 National Security Act of 1947 (50 U.S.C.
15 3234) (governing disclosure by employees of
16 elements of the intelligence community), or any
17 similar provision of Federal or 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
24 OBLIGATIONS AND RIGHTS.—Nothing in this
25 section may be construed to—

1 “(i) amend, repeal, or supersede any
2 current or future contractual agreement,
3 terms of service agreement, or other con-
4 tractual relationship between any non-Fed-
5 eral entities, or between any non-Federal
6 entity 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.—Noth-
11 ing in this section may be construed to permit
12 a 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
17 with a non-Federal entity on such non-
18 Federal entity’s provision of cyber threat
19 indicators or defensive measures to a Fed-
20 eral entity; or

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

1 “(F) NO LIABILITY FOR NON-PARTICIPA-
2 TION.—Nothing in this section may be con-
3 strued to subject any non-Federal entity to li-
4 ability for choosing to not engage in the vol-
5 untary activities authorized under this section.

6 “(G) USE AND RETENTION OF INFORMA-
7 TION.—Nothing in this section may be con-
8 strued to authorize, or to modify any existing
9 authority of, a department or agency of the
10 Federal Government to retain or use any infor-
11 mation shared under this section for any use
12 other than permitted in this section.

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

24 “(I) FEDERAL PREEMPTION.—This section
25 supersedes any statute or other provision of law

1 of a State or political subdivision of a State
2 that restricts or otherwise expressly regulates
3 an activity authorized under this section.”.

4 **SEC. 4. INFORMATION SHARING AND ANALYSIS ORGANIZA-**
5 **TIONS.**

6 Section 212 of the Homeland Security Act of 2002
7 (6 U.S.C. 131) is amended—

8 (1) in paragraph (5)—

9 (A) in subparagraph (A)—

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

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

18 (B) in subparagraph (B)—

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

24 (ii) by striking “related to critical in-
25 frastructure or” and inserting “related to

1 cybersecurity risks, incidents, critical infra-
2 structure, or” and

3 (C) in subparagraph (C), by striking “dis-
4 seminating critical infrastructure information”
5 and inserting “disseminating cybersecurity
6 risks, incidents, and critical infrastructure in-
7 formation”; and

8 (2) by adding at the end the following new
9 paragraph:

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

15 **SEC. 5. PROHIBITION ON NEW REGULATORY AUTHORITY.**

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

1 **SEC. 6. STREAMLINING OF DEPARTMENT OF HOMELAND**
2 **SECURITY CYBERSECURITY AND INFRA-**
3 **STRUCTURE PROTECTION ORGANIZATION.**

4 (a) **CYBERSECURITY AND INFRASTRUCTURE PRO-**
5 **TECTION.**—The National Protection and Programs Direc-
6 torate of the Department of Homeland Security shall,
7 after the date of the enactment of this Act, be known and
8 designated as the “Cybersecurity and Infrastructure Pro-
9 tection”. Any reference to the National Protection and
10 Programs Directorate of the Department in any law, regu-
11 lation, map, document, record, or other paper of the
12 United States shall be deemed to be a reference to the
13 Cybersecurity and Infrastructure Protection of the De-
14 partment.

15 (b) **SENIOR LEADERSHIP OF CYBERSECURITY AND**
16 **INFRASTRUCTURE PROTECTION.**—

17 (1) **IN GENERAL.**—Subsection (a) of section
18 103 of the Homeland Security Act of 2002 (6
19 U.S.C. 113) is amended—

20 (A) in paragraph (1)—

21 (i) by amending subparagraph (H) to
22 read as follows:

23 “(H) An Under Secretary for Cybersecu-
24 rity and Infrastructure Protection.”; and

25 (ii) by adding at the end the following
26 new subparagraphs:

1 “(K) A Deputy Under Secretary for Cyber-
2 security.

3 “(L) A Deputy Under Secretary for Infra-
4 structure Protection.”; and

5 (B) by adding at the end the following new
6 paragraph:

7 “(3) DEPUTY UNDER SECRETARIES.—The Dep-
8 uty Under Secretaries referred to in subparagraphs
9 (K) and (L) of paragraph (1) shall be appointed by
10 the President without the advice and consent of the
11 Senate.”.

12 (2) CONTINUATION IN OFFICE.—The individ-
13 uals who hold the positions referred in subpara-
14 graphs (H), (K), and (L) of paragraph (1) of section
15 103(a) the Homeland Security Act of 2002 (as
16 amended and added by paragraph (1) of this sub-
17 section) as of the date of the enactment of this Act
18 may continue to hold such positions.

19 (c) REPORT.—Not later than 90 days after the date
20 of the enactment of this Act, the Under Secretary for Cy-
21 bersecurity and Infrastructure Protection of the Depart-
22 ment of Homeland Security shall submit to the Committee
23 on Homeland Security of the House of Representatives
24 and the Committee on Homeland Security and Govern-
25 mental Affairs of the Senate a report on the feasibility

1 of becoming an operational component, including an anal-
2 ysis of alternatives, and if a determination is rendered that
3 becoming an operational component is the best option for
4 achieving the mission of Cybersecurity and Infrastructure
5 Protection, a legislative proposal and implementation plan
6 for becoming such an operational component. Such report
7 shall also include plans to more effectively carry out the
8 cybersecurity mission of Cybersecurity and Infrastructure
9 Protection, including expediting information sharing
10 agreements.

11 **SEC. 7. REPORT ON REDUCING CYBERSECURITY RISKS IN**
12 **DHS DATA CENTERS.**

13 Not later than one year after the date of the enact-
14 ment of this Act, the Secretary of Homeland Security shall
15 submit to the Committee on Homeland Security of the
16 House of Representatives and the Committee on Home-
17 land Security and Governmental Affairs of the Senate a
18 report on the feasibility of the Department of Homeland
19 Security creating an environment for the reduction in cy-
20 bersecurity risks in Department data centers, including by
21 increasing compartmentalization between systems, and
22 providing a mix of security controls between such compart-
23 ments.

1 **SEC. 8. 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
6 such purposes.

○