

[DISCUSSION DRAFT]114TH CONGRESS
1ST SESSION**H. R.** _____

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

Mr. McCAUL introduced the following bill; which was referred to the
Committee on _____

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”.

1 **SEC. 2. NATIONAL CYBERSECURITY AND COMMUNICA-**
2 **TIONS INTEGRATION CENTER.**

3 (a) DEFINITIONS.—

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

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

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

13 (C) by adding at the end the following new
14 paragraphs:

15 “(5) the term ‘cyber threat indicator’ means
16 technical information—

17 “(A) that is necessary to describe or iden-
18 tify—

19 “(i) a method for probing or main-
20 taining network awareness of an informa-
21 tion system for the purpose of discerning
22 technical vulnerabilities of such informa-
23 tion system, if such method is known or
24 reasonably suspected of being associated
25 with a known or suspected cybersecurity
26 risk or incident, including communications

1 that reasonably appear to be transmitted
2 for the purpose of gathering technical in-
3 formation related to a cybersecurity risk or
4 incident;

5 “(ii) a method for defeating a tech-
6 nical or security control for an information
7 system that is primarily implemented and
8 executed by people;

9 “(iii) a technical vulnerability;

10 “(iv) a method of causing a user with
11 legitimate access to an information system
12 or information that is stored on, processed
13 by, or transiting an information system in-
14 advertently to enable the defeat of a tech-
15 nical or operational control;

16 “(v) a method for remote identifica-
17 tion of, access to, or use of an information
18 system or information that is stored on,
19 processed by, or transiting an information
20 system that is known or reasonably sus-
21 pected of being associated with a known or
22 suspected cyber risk or incident; or

23 “(vi) any combination of clauses (i)
24 through (v); and

1 “(B) from which reasonable efforts have
2 been made to remove information that can be
3 used to identify specific persons reasonably be-
4 lieved to be unrelated to the cybersecurity risk
5 or incident;

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

11 “(7) the term ‘defensive measure’ means auto-
12 mated or manual actions taken by or on behalf of
13 a Federal entity or non-Federal entity on an infor-
14 mation system owned or operated by such Federal
15 entity or non-Federal entity to modify or block data
16 packets associated with electronic or wire commu-
17 nications, internet traffic, program code, or other
18 system traffic transiting to or from or stored on
19 such information system for the purpose of pro-
20 tecting such information system from a cybersecu-
21 rity risk or incident, but such term does not include
22 any automated or manual action designed or de-
23 ployed in a manner that destroys, disables, or sub-
24 stantially harms an information system not owned or
25 operated by—

1 “(A) the Federal entity or non-Federal en-
2 tity owning or operating such an automated or
3 manual action; or

4 “(B) another non-Federal entity or Fed-
5 eral entity that has provided consent to the first
6 Federal entity or non-Federal entity for oper-
7 ation of such an automated or manual action in
8 accordance with this section;

9 “(8) the term ‘network awareness’ means to
10 scan, identify, or analyze information that is stored
11 on, processed by, or transiting an information sys-
12 tem;

13 “(9) the term ‘private entity’ means an indi-
14 vidual, a private or publicly traded company, a pri-
15 vate or public utility (including a utility that is a
16 unit of a State, local, or tribal government, or a po-
17 litical subdivision of a State government), an organi-
18 zation, or a corporation, including an officer, em-
19 ployee, or agent thereof;

20 “(10) the term ‘sharing’ means providing, re-
21 ceiving, and disseminating.”.

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

1 (1) in clause (i), by striking “and local” and in-
2 sserting “, local, and tribal”;

3 (2) in clause (ii)—

4 (A) by inserting “, including information
5 sharing and analysis centers” before the semi-
6 colon; and

7 (B) by striking “and” at the end;

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

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

12 “(iv) private entities.”.

13 **SEC. 3. INFORMATION SHARING STRUCTURE AND PROC-**
14 **ESSES.**

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

19 (1) in subsection (c)—

20 (A) in paragraph (1)—

21 (i) by striking “a Federal civilian
22 interface” and inserting “the primary Fed-
23 eral civilian interface”; and

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

4 (B) in paragraph (2), by inserting “share
5 cyber threat indicators and defensive measures
6 and” before “address”;

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

10 (D) in paragraph (4)—

11 (i) by inserting “share cyber threat
12 indicators and defensive measures and” be-
13 fore “address”; and

14 (ii) by striking “including cybersecu-
15 rity risks” and inserting “including cyber
16 threat indicators, defensive measures, cy-
17 bersecurity risks,”;

18 (E) in paragraph (5)(A), by striking “cy-
19 bersecurity risks” and inserting “cyber threat
20 indicators, defensive measures, cybersecurity
21 risks,”;

22 (F) in paragraph (6), by striking “cyberse-
23 curity risks” and inserting “cyber threat indica-
24 tors, defensive measures, cybersecurity risks,”;

25 (G) in paragraph (7)—

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

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

6 (iii) by adding at the end the fol-
7 lowing new subparagraph:

8 “(C) sharing cyber threat indicators, de-
9 fensive measures, and information related to cy-
10 bersecurity risks and incidents;” and

11 (H) by adding at the end the following new
12 paragraphs

13 “(8) engage with international partners to—

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

17 “(B) enhance the security and resilience of
18 the global cybersecurity ecosystem; and

19 “(9) sharing cyber threat indicators, defensive
20 measures, and information related to cybersecurity
21 risks and incidents with Federal and non-Federal
22 entities.”;

23 (2) in subsection (d)—

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

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

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

5 “(E) a Multi-State Information Sharing
6 and Analysis Center to collaborate with State
7 and local governments;

8 “(F) a United States Computer Emer-
9 gency Readiness Team to coordinate informa-
10 tion related to cybersecurity risks and incidents,
11 proactively manage cybersecurity risks and inci-
12 dents to the United States, collaboratively re-
13 spond to cybersecurity risks and incidents, pro-
14 vide technical assistance to information system
15 owners and operators, and disseminate timely
16 information related to cybersecurity risks and
17 incidents;

18 “(G) the Industrial Control System Cyber
19 Emergency Response Team to coordinate with
20 industrial control systems owners and operators
21 and share industrial control systems-related se-
22 curity incidents and mitigation measures;

23 “(H) National Coordinating Center for
24 Communications to coordinate the protection,

1 response, and recovery of national security
2 emergency communications; and”;

3 (3) in subsection (e)—

4 (A) in paragraph (1)—

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

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

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

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

19 (B) in paragraph (2)—

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

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

1 (C) in paragraph (3), insert before the pe-
2 riod at the end the following: “, including by
3 working with the privacy officer appointed
4 under section 222”; 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
9 Cybersecurity and Infrastructure Protection shall
10 develop a capability that supports and rapidly ad-
11 vances the development, adoption, and implementa-
12 tion of an automated mechanism for the timely shar-
13 ing of cyber threat indicators and defensive meas-
14 ures to and from the Center.

15 “(2) BIENNIAL REPORT.—The Under Sec-
16 retary for Cybersecurity and Infrastructure Protec-
17 tion shall submit to the appropriate congressional
18 committees a biennial report on the status and
19 progress of the development of the capability de-
20 scribed in paragraph (1). Such reports shall be re-
21 quired until such capability is fully implemented.

22 “(h) VOLUNTARY INFORMATION SHARING PROCE-
23 DURES.—

24 “(1) IN GENERAL.—The Center may enter into
25 a voluntary information sharing relationship with

1 any consenting non-Federal entity for the sharing of
2 cyber threat indicators, defensive measures, and in-
3 formation related to cybersecurity risks and inci-
4 dents for cybersecurity purposes in accordance with
5 this section. Nothing in this section may be con-
6 strued to require any non-Federal entity to enter
7 into any such information sharing relationship with
8 the Center or any other entity. The Center may ter-
9minate a voluntary information sharing relationship
10 under this subsection if the Center determines that
11 the non-Federal entity with which the Center has
12 entered into such a relationship has, after repeated
13 notice, repeatedly and intentionally violated the
14 terms of this subsection.

15 “(2) AGREEMENTS.—

16 “(A) CENTER MEMORANDUM OF UNDER-
17 STANDING.—To enter into a voluntary informa-
18 tion sharing relationship with the Center under
19 this subsection, a consenting non-Federal entity
20 shall enter into a memorandum of under-
21 standing with the Center that sets forth the
22 general terms of the relationship, including all
23 information sharing procedures set forth in any
24 cooperative research and development agree-
25 ments or appendices in effect as of March 15,

1 2015, and all information protections and liabil-
2 ity exemptions specified in this subsection. A
3 memorandum of understanding described in
4 this subparagraph shall be finalized within 30
5 days of a request by a consenting non-Federal
6 entity to enter into a voluntary information
7 sharing relationship with the Center unless the
8 Secretary, for national security purposes, de-
9 clines to enter into such a relationship. Such
10 memorandum of understanding shall be the
11 only agreement required to enter into a formal
12 information sharing relationship with the Cen-
13 ter. Any information sharing agreement be-
14 tween the Center and a non-Federal entity in
15 effect prior to the date of the enactment of this
16 section is deemed in compliance with the re-
17 quirements of this subsection.

18 “(B) OTHER AGREEMENTS.—Nothing in
19 this subsection shall preclude the Department
20 or the Center from entering into information
21 sharing agreements other than a memorandum
22 of understanding as set forth in subparagraph
23 (A) with consenting non-Federal entities. All
24 such other agreements shall include all informa-

1 tion protections and liability exemptions as set
2 forth in this section.

3 “(3) INFORMATION SHARING AUTHORIZA-
4 TION.—

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, share cyber
10 threat indicators, defensive measures, or infor-
11 mation related to cybersecurity risks and inci-
12 dents obtained on its own information system in
13 accordance with this section with—

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

15 “(ii) the Center, as provided in this
16 section.

17 “(B) LAWFUL RESTRICTION.—A non-Fed-
18 eral entity receiving a cybersecurity risk indi-
19 cator, defensive measure, or information related
20 to cybersecurity risks and incidents from an-
21 other Federal or non-Federal entity shall com-
22 ply with otherwise lawful restrictions placed on
23 the sharing or use of such cybersecurity risk in-
24 dicator, defensive measure or information re-

1 lated to cybersecurity risks and incidents by the
2 sharing Federal or non-Federal entity.

3 “(C) REMOVAL OF INFORMATION UNRE-
4 LATED TO CYBERSECURITY RISKS OR INCI-
5 DENTS.—A non-Federal entity shall take rea-
6 sonable efforts to minimize information that
7 can be used to identify specific persons and is
8 reasonably believed to be unrelated to a cyber-
9 security risk or incident, and to safeguard in-
10 formation that can be used to identify specific
11 persons from unintended disclosure and unau-
12 thorized access or acquisition.

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

15 “(i) limit or modify an existing infor-
16 mation sharing relationship;

17 “(ii) prohibit a new information shar-
18 ing relationship;

19 “(iii) require a new information shar-
20 ing relationship between any non-Federal
21 entity and a Federal entity;

22 “(iv) limit otherwise lawful activity; or

23 “(v) in any manner impact or modify
24 procedures in existence as of the date of
25 the enactment of this section for reporting

1 known or suspected criminal activity to ap-
2 propriate law enforcement authorities.

3 “(4) NETWORK AWARENESS AUTHORIZATION.—

4 “(A) IN GENERAL.—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, conduct net-
8 work awareness of—

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
14 of such other non-Federal entity for con-
15 ducting such network awareness to protect
16 the rights or property of such other non-
17 Federal 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 conducting such network awareness
22 to protect the rights or property of such
23 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 conducting the network
7 awareness of an information system, or the
8 use of any information obtained through
9 such conducting of network awareness,
10 other than as provided in this section; or

11 “(ii) limit otherwise lawful activity.

12 “(5) DEFENSIVE MEASURE AUTHORIZATION.—

13 “(A) IN GENERAL.—Except as provided in
14 subparagraph (B) and notwithstanding any
15 other provision of law, a non-Federal entity, not
16 including a State, local, or tribal government,
17 may, for cybersecurity purposes, operate a de-
18 fensive measure that is applied to—

19 “(i) an information system of such
20 non-Federal entity to protect the rights or
21 property of such non-Federal entity;

22 “(ii) an information system of another
23 non-Federal entity upon written consent of
24 such other non-Federal entity for operation
25 of such defensive measure to protect the

1 rights or property of such other non-Fed-
2 eral entity;

3 “(iii) an information system of a Fed-
4 eral entity upon written consent of an au-
5 thorized representative of such Federal en-
6 tity for operation of such defensive meas-
7 ure to protect the rights or property of
8 such Federal entity; or

9 “(iv) information that is stored on,
10 processed by, or transiting an information
11 system described in this subparagraph.

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

14 “(i) authorize the use of a defensive
15 measure other than as provided in this sec-
16 tion; or

17 “(ii) limit otherwise lawful activity.

18 “(6) PRIVACY AND CIVIL LIBERTIES PROTEC-
19 TIONS.—

20 “(A) POLICIES AND PROCEDURES.—

21 “(i) IN GENERAL.—The Under Sec-
22 retary for Cybersecurity and Infrastructure
23 Protection shall, in coordination with the
24 Chief Privacy Officer and the Chief Civil
25 Rights and Civil Liberties Officer of the

1 Department, establish and annually review
2 policies and procedures governing the re-
3 ceipt, retention, use, and disclosure of
4 cyber threat indicators, defensive meas-
5 ures, and information related to cybersecu-
6 rity risks and incidents shared with the
7 Center in accordance with this section.
8 Such policies and procedures shall, con-
9 sistent with the need to protect informa-
10 tion systems from cybersecurity risks and
11 incidents and mitigate cybersecurity risks
12 and incidents in a timely manner—

13 “(I) be consistent with the De-
14 partment’s Fair Information Practice
15 Principles developed pursuant to sec-
16 tion 552a of title 5, United States
17 Code (commonly referred to as the
18 ‘Privacy Act of 1974’ or the ‘Privacy
19 Act’), and subject to the Secretary’s
20 authority under subsection (a)(2) of
21 section 222 of this Act;

22 “(II) reasonably limit the receipt,
23 retention, use, and disclosure of cyber
24 threat indicators, defensive measures,
25 and information related to cybersecu-

1 rity risks and incidents associated
2 with specific persons that is not nec-
3 essary, for cybersecurity purposes, to
4 protect an information system from
5 cybersecurity risks and incidents or
6 mitigate cybersecurity risks and inci-
7 dents in a timely manner;

8 “(III) minimize any impact on
9 privacy and civil liberties;

10 “(IV) provide data integrity
11 through the timely removal and de-
12 struction of obsolete or erroneous
13 names and personal information that
14 is unrelated to the cybersecurity risk
15 or incident information shared in ac-
16 cordance with this section;

17 “(V) include requirements to
18 safeguard cyber threat indicators, de-
19 fensive measures, and information re-
20 lated to cybersecurity risks and inci-
21 dents, including information that is
22 proprietary or business-sensitive, that
23 may be used to identify specific per-
24 sons from unauthorized access or ac-
25 quisition;

1 “(VI) protect the confidentiality
2 of cyber threat indicators, defensive
3 measures, and information related to
4 cybersecurity risks and incidents asso-
5 ciated with specific persons to the
6 greatest extent practicable;

7 “(VII) not delay or impede the
8 flow of cyber threat indicators, defen-
9 sive measures, and information re-
10 lated to cybersecurity risks and inci-
11 dents necessary to defend against or
12 mitigate cybersecurity risks and inci-
13 dents; and

14 “(VIII) ensure all relevant con-
15 stitutional, legal, and privacy protec-
16 tions are observed.

17 “(ii) SUBMISSION TO CONGRESS.—
18 Not later than 180 days after the date of
19 the enactment of this section and annually
20 thereafter, the Chief Privacy Officer of the
21 Department, in consultation with the Pri-
22 vacy and Civil Liberties Oversight Board
23 (established pursuant to section 1061 of
24 the Intelligence Reform and Terrorism
25 Prevention Act of 2004 (42 U.S.C.

1 2000ee)), shall submit to the appropriate
2 congressional committees the policies and
3 procedures governing the sharing of cyber
4 threat indicators, defensive measures, and
5 information related to cybersecurity risks
6 and incidents described in clause (i) of
7 subparagraph (A).

8 “(iii) PUBLIC NOTICE AND ACCESS.—
9 The Under Secretary for Cybersecurity
10 and Infrastructure Protection, in consulta-
11 tion with the Chief Privacy Officer and the
12 Chief Civil Rights and Civil Liberties Offi-
13 cer of the Department, and the Privacy
14 and Civil Liberties Oversight Board (estab-
15 lished pursuant to section 1061 of the In-
16 telligence Reform and Terrorism Preven-
17 tion Act of 2004 (42 U.S.C. 2000ee)),
18 shall ensure there is public notice of, and
19 access to, the polices and procedures gov-
20 erning the sharing of cyber threat indica-
21 tors, defensive measures, and information
22 related to cybersecurity risks and inci-
23 dents.

1 “(B) IMPLEMENTATION.—The Chief Pri-
2 vacy Officer of the Department, on an ongoing
3 basis, shall—

4 “(i) implement the policies and proce-
5 dures governing the sharing of cyber threat
6 indicators, defensive measures, and infor-
7 mation related to cybersecurity risks and
8 incidents established pursuant to clause (i)
9 of subparagraph (A);

10 “(ii) annually prepare privacy impact
11 assessments to ensure all relevant constitu-
12 tional, legal, and privacy protections are
13 being followed;

14 “(iii) promptly notify the Secretary
15 and the appropriate congressional commit-
16 tees of any significant violations of such
17 policies and procedures;

18 “(iv) annually submit to the appro-
19 priate congressional committees a report
20 that contains an audit of the effectiveness
21 of such policies and procedures;

22 “(v) promptly notify non-Federal enti-
23 ties that have shared cyber threat indica-
24 tors, defensive measures, or information
25 related to cybersecurity risks or incidents

1 that is known or determined to be in error
2 or in contravention of the requirements of
3 this section; and

4 “(vii) ensure there are appropriate
5 sanctions in place for officers, employees,
6 or agents of the Department who know-
7 ingly and willfully conduct activities under
8 this section in an unauthorized manner.

9 “(C) INSPECTOR GENERAL REPORT.—The
10 Inspector General of the Department, in con-
11 sultation with the Privacy and Civil Liberties
12 Oversight Board and the Inspector General of
13 each Federal agency that receives cyber threat
14 indicators, defensive measures, or information
15 related to cybersecurity risks and incidents
16 shared with the Center under this section, shall
17 annually submit to the appropriate congres-
18 sional committees a report containing a review
19 of the use of cybersecurity risk information
20 shared with the Center, including the following:

21 “(i) A report on the receipt, use, and
22 dissemination of cyber threat indicators,
23 defensive measures, and information re-
24 lated to cybersecurity risks and incidents

1 that has been shared with Federal entities
2 under this section.

3 “(ii) A review of the use by the Center
4 of such information for a purpose other
5 than a cybersecurity purpose.

6 “(iii) A review of the type of informa-
7 tion shared with the Center under this sec-
8 tion.

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

11 “(v) Appropriate metrics to determine
12 the impact, if any, on privacy and civil lib-
13 erties as a result of the sharing of such in-
14 formation with the Center.

15 “(vi) A list of other Federal agencies
16 receiving such information.

17 “(vii) A review of the sharing of such
18 information within the Federal Govern-
19 ment to identify inappropriate stove piping
20 of such information.

21 “(viii) Any recommendations of the
22 Inspector General of the Department for
23 improvements or modifications to informa-
24 tion sharing under this section.

1 “(D) PRIVACY AND CIVIL LIBERTIES OFFI-
2 CERS REPORT.—The Chief Privacy Officer and
3 the Chief Civil Rights and Civil Liberties Offi-
4 cer of the Department, in consultation with the
5 Privacy and Civil Liberties Oversight Board,
6 the Inspector General of the Department, and
7 the senior privacy and civil liberties officer of
8 each Federal agency that receives cyber threat
9 indicators, defensive measures, and information
10 related to cybersecurity risks and incidents
11 shared with the Center under this section, shall
12 annually submit to the appropriate congres-
13 sional committees a report assessing the privacy
14 and civil liberties impact of the activities under
15 this paragraph. Each such report shall include
16 any recommendations the Chief Privacy Officer
17 and the Chief Civil Rights and Civil Liberties
18 Officer of the Department consider appropriate
19 to minimize or mitigate the privacy and civil
20 liberties impact of the sharing of cyber threat
21 indicators, defensive measures, and information
22 related to cybersecurity risks and incidents
23 under this section.

24 “(E) FORM.—Each report required under
25 paragraphs (C) and (D) shall be submitted in

1 unclassified form, but may include a classified
2 annex.

3 “(7) USES AND PROTECTION OF INFORMA-
4 TION.—

5 “(A) NON-FEDERAL ENTITIES.—A non-
6 Federal entity, not including a State, local, or
7 tribal government, that shares cyber threat in-
8 dicators, defensive measures, or information re-
9 lated to cybersecurity risks or incidents through
10 the Center or otherwise under this section—

11 “(i) may use, retain, or further dis-
12 close such cyber threat indicators, defen-
13 sive measures, and information related to
14 cybersecurity risks or incidents solely for
15 cybersecurity purposes;

16 “(ii) shall take reasonable efforts to
17 minimize information that can be used to
18 identify specific persons and is reasonably
19 believed to be unrelated to a cybersecurity
20 risk or incident, and to safeguard informa-
21 tion that can be used to identify specific
22 persons from unintended disclosure and
23 unauthorized access or acquisition;

24 “(iii) shall comply with appropriate
25 restrictions that a Federal entity or non-

1 Federal entity places on the subsequent
2 disclosure or retention of cyber threat indi-
3 cators, defensive measures, and informa-
4 tion related to cybersecurity risks and inci-
5 dents that it discloses to other Federal en-
6 tities or non-Federal entities;

7 “(iv) shall be deemed voluntarily
8 shared;

9 “(v) shall implement and utilize a se-
10 curity control to protect against unauthor-
11 ized access to or acquisition of such cyber
12 threat indicators, defensive measures, or
13 information related to cybersecurity risks
14 or incidents; and

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

18 “(B) FEDERAL ENTITIES.—A Federal en-
19 tity that receives cyber threat indicators, defen-
20 sive measures, or information related to cyber-
21 security risks or incidents shared through the
22 Center or otherwise under this section—

23 “(i) may use, retain, or further dis-
24 close such cyber threat indicators, defen-
25 sive measures, and information related to

1 cybersecurity risks or incidents solely for
2 cybersecurity purposes;

3 “(ii) shall take reasonable efforts to
4 minimize information that can be used to
5 identify specific persons and is reasonably
6 believed to be unrelated to a cybersecurity
7 risk or incident, and to safeguard informa-
8 tion that can be used to identify specific
9 persons from unintended disclosure and
10 unauthorized access or acquisition;

11 “(iii) shall comply with appropriate
12 restrictions that a non-Federal entity
13 places on the subsequent disclosure or re-
14 tention of cyber threat indicators, defensive
15 measures, and information related to cy-
16 bersecurity risks and incidents that it dis-
17 closes to other non-Federal entities;

18 “(iv) shall be deemed voluntarily
19 shared;

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, defensive measures, or
24 information related to cybersecurity risks
25 or incidents;

1 “(vi) is exempt from disclosure under
2 section 552 of title 5, United States Code,
3 and withheld, without discretion, from the
4 public under subsection (b)(3)(B) of such
5 section;

6 “(vii) shall be considered proprietary
7 information and may not be disclosed to an
8 entity outside the Federal Government un-
9 less otherwise expressly authorized by the
10 non-Federal entity sharing such informa-
11 tion or anonymized to protect source infor-
12 mation.

13 “(viii) may not be used by the Federal
14 Government for regulatory purposes;

15 “(ix) may not constitute a waiver of
16 any applicable privilege or protection pro-
17 vided by law, including trade secret protec-
18 tion;

19 “(x) shall be considered the commer-
20 cial, financial, and proprietary information
21 of such non-Federal entity when so des-
22 ignated by such non-Federal entity; and

23 “(xi) may not be subject to a rule of
24 any Federal entity or any judicial doctrine

1 regarding ex parte communications with a
2 decisionmaking official.

3 “(C) STATE, TRIBAL, OR LOCAL GOVERN-
4 MENT.—Cyber threat indicators, defensive
5 measures, or information related to cybersecu-
6 rity risks or incidents shared with a State, trib-
7 al, or local government by the Center or other-
8 wise under this section—

9 “(i) may use, retain, or further dis-
10 close such cyber threat indicators, defen-
11 sive measures, and information related to
12 cybersecurity risks or incidents solely for
13 cybersecurity purposes;

14 “(ii) shall take reasonable efforts to
15 minimize information that can be used to
16 identify specific persons and is reasonably
17 believed to be unrelated to a cybersecurity
18 risk or incident, and to safeguard informa-
19 tion that can be used to identify specific
20 persons from unintended disclosure and
21 unauthorized access or acquisition;

22 “(iii) shall comply with appropriate
23 restrictions that a Federal entity or non-
24 Federal entity places on the subsequent
25 disclosure or retention of cyber threat indi-

1 cators, defensive measures, and informa-
2 tion related to cybersecurity risks and inci-
3 dents that it discloses to other Federal en-
4 tities or non-Federal entities;

5 “(iv) shall be deemed voluntarily
6 shared;

7 “(v) shall implement and utilize a se-
8 curity control to protect against unauthor-
9 ized access to or acquisition of such cyber
10 threat indicators, defensive measures, or
11 information related to cybersecurity risks
12 or incidents;

13 “(vi) shall be exempt from disclosure
14 under any State, tribal, or local law or reg-
15 ulation that requires public disclosure of
16 information or records by a public or
17 quasi-public entity; and

18 “(vii) may not be used by any State,
19 tribal, or local government to regulate a
20 lawful activity of a non-Federal entity.

21 “(8) LIABILITY EXEMPTIONS.—

22 “(A) IN GENERAL.—A non-Federal entity,
23 not including a State, local, or tribal govern-
24 ment, that, for cybersecurity purposes, in ac-
25 cordance with paragraphs (3) and (4), shares

1 cyber threat indicators, defensive measures, or
2 information related to cybersecurity risks or in-
3 cidents or conducts network awareness on an
4 information system shall not be liable in any
5 civil or criminal action brought under this sub-
6 section unless such non-Federal entity engaged
7 in willful misconduct or gross negligence with
8 respect to such sharing or conduct and such
9 gross negligence or willful misconduct proxi-
10 mately caused injury.

11 “(B) GROSS NEGLIGENCE.—The term
12 ‘gross negligence’ shall, for purposes of this
13 subsection, mean an act or omission—

14 “(i) which when viewed objectively
15 from the standpoint of the non-Federal en-
16 tity at issue at the time of the occurrence
17 of such act or omission involves an extreme
18 degree of risk, considering the substantial
19 probability and magnitude of the potential
20 harm to others; and

21 “(ii) of which such non-Federal entity
22 has actual, subjective awareness of the risk
23 involved, but nevertheless proceeds with
24 conscious, flagrant indifference to the
25 rights or safety of others.

1 “(C) WILLFUL MISCONDUCT.—The term
2 ‘willful misconduct’ shall, for purposes of this
3 subsection, mean an act or omission that is
4 taken—

5 “(i) intentionally to achieve a wrong-
6 ful purpose;

7 “(ii) knowingly without legal or fac-
8 tual justification; and

9 “(iii) in disregard of a known or obvi-
10 ous risk that is so great as to make it
11 highly probable that the harm resulting
12 from taking such act or omission will out-
13 weigh the benefit.

14 “(D) RULE OF CONSTRUCTION.—Notwith-
15 standing any other provision of law, a non-Fed-
16 eral entity shall not have engaged in gross neg-
17 ligence or willful misconduct as a matter of law
18 if such non-Federal entity acted in accordance
19 with this section or applicable directions, guide-
20 lines, or recommendations by the Secretary re-
21 garding the administration or use of an infor-
22 mation system.

23 “(E) PROOF OF GROSS NEGLIGENCE OR
24 WILLFUL MISCONDUCT.—In an action under
25 subparagraph (A), the plaintiff shall have the

1 burden of proving by clear and convincing evi-
2 dence gross negligence or willful misconduct by
3 each non-Federal entity sued, and that such
4 gross negligence or willful misconduct proxi-
5 mately caused such plaintiff's injury. Punitive
6 damages intended to punish or deter, exemplary
7 damages, or other damages not intended to
8 compensate a plaintiff for actual losses may be
9 awarded in such an action only if a plaintiff
10 proves that a non-Federal entity engaged in
11 willful misconduct.

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 (7)(B) on the use and protection of
20 voluntarily shared cyber threat indicators, de-
21 fensive measures, or information related to cy-
22 bersecurity risks or incidents, the Federal Gov-
23 ernment shall be liable to a person injured by
24 such violation in an amount equal to the sum
25 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) the costs of the action, together
5 with reasonable attorney fees as deter-
6 mined by the court.

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

10 “(i) the district in which the com-
11 plainant resides;

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

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

18 “(iv) the District of Columbia.

19 “(C) STATUTE OF LIMITATIONS.—No ac-
20 tion shall lie under this subsection unless such
21 action is commenced not later than two years
22 after the date of the violation of any restriction
23 specified in paragraph 7(B) that is the basis for
24 such action.

1 “(D) EXCLUSIVE CAUSE OF ACTION.—A
2 cause of action under this subsection shall be
3 the exclusive means available to a complainant
4 seeking a remedy for a violation of any restric-
5 tion specified in paragraph 7(B).

6 “(10) ANTI-TRUST EXEMPTION.—

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

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

21 “(i) facilitating the prevention, inves-
22 tigation, or mitigation of a cybersecurity
23 risk or incident to an information system
24 or information that is stored on, processed
25 by, or transiting an information system; or

1 “(ii) communicating or disclosing a
2 cybersecurity risk indicator, defensive
3 measure, or information related to a cyber-
4 security risk or incident to help prevent,
5 investigate, or mitigate the effect of a cy-
6 bersecurity risk or incident to an informa-
7 tion system or information that is stored
8 on, processed by, or transiting an informa-
9 tion 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, boycotting, or exchanges of price or
15 cost information, customer lists, or information
16 regarding 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, by a non-Federal to
24 any other non-Federal entity or Federal entity
25 under this section.

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

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

21 “(D) PRESERVATION OF CONTRACTUAL
22 OBLIGATIONS AND RIGHTS.—Nothing in this
23 section may be construed to—

24 “(i) amend, repeal, or supersede any
25 current or future contractual agreement,

1 terms of service agreement, or other con-
2 tractual relationship between any non-Fed-
3 eral entities, or between any non-Federal
4 entity and a Federal entity; or

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

8 “(E) ANTI-TASKING RESTRICTION.—Noth-
9 ing in this section may be construed to permit
10 a Federal entity to—

11 “(i) require a non-Federal entity to
12 provide information to a Federal entity;

13 “(ii) condition the sharing of cyber
14 threat indicators, defensive measures, and
15 information related to cybersecurity risks
16 and incidents with a non-Federal entity on
17 such non-Federal entity’s provision of
18 cyber threat indicators to a Federal entity;
19 or

20 “(iii) condition the award of any Fed-
21 eral grant, contract, or purchase on the
22 sharing of cyber threat indicators, defen-
23 sive measures, and information related to
24 cybersecurity risks and incidents with a
25 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 participate 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 cy-
18 bersecurity 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. PROTECTION OF FEDERAL CIVILIAN INFORMATION**
5 **SYSTEMS.**

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

9 **“SEC. 230. PROTECTION OF FEDERAL INFORMATION SYS-**
10 **TEMS.**

11 “(a) IN GENERAL.—The Secretary shall—

12 “(1) administer Federal Government-wide ef-
13 forts to develop and provide adequate, risk-based,
14 cost-effective, and technology neutral information se-
15 curity capabilities;

16 “(2) establish and sustain continuous
17 diagnostics systems for Federal civilian information
18 systems to aggregate data and identify and prioritize
19 the mitigation of cybersecurity risks and incidents in
20 such systems for cybersecurity purposes;

21 “(3) develop, acquire, and operate an integrated
22 and consolidated system of intrusion detection, ana-
23 lytics, intrusion prevention, and other information
24 sharing and protective capabilities to defend Federal

1 civilian information systems from cybersecurity risks
2 and incidents;

3 “(4) develop and conduct targeted risk assess-
4 ments and operational evaluations of Federal civilian
5 information systems, in consultation with Federal
6 entities and non-Federal entities that own and oper-
7 ate Federal civilian information systems, including
8 threat, vulnerability, and impact assessments and
9 penetration testing;

10 “(5) develop and provide technical assistance
11 and cyber incident response capabilities to secure
12 and ensure the resilience of Federal civilian informa-
13 tion systems;

14 “(6) develop reporting requirements, consistent
15 with relevant law, to ensure the National Cybersecu-
16 rity and Communications Integration Center estab-
17 lished pursuant to the second section 226 receives all
18 actionable information related to cybersecurity risks
19 and incidents; and

20 “(7) develop training requirements regarding
21 privacy, civil rights, civil liberties, and information
22 oversight for information security employees who op-
23 erate Federal civilian information systems.

24 “(b) USE OF CERTAIN COMMUNICATIONS.—

1 “(1) IN GENERAL.—The Secretary may enter
2 into contracts or other agreements, or otherwise re-
3 quest and obtain, in accordance with applicable law,
4 the assistance of private entities that provide elec-
5 tronic communication services, remote computing
6 services, or cybersecurity services to acquire, inter-
7 cept, retain, use, and disclose communications and
8 other system traffic, deploy defensive measures (as
9 such term is defined in the second section 226 (re-
10 lating to the National Cybersecurity and Commu-
11 nications Integration Center)), or otherwise operate
12 protective capabilities in accordance with paragraphs
13 (2), (3), (4), and (5) of subsection (a). No cause of
14 action shall exist against private entities for assist-
15 ance provided to the Secretary in accordance with
16 this subsection.

17 “(2) RULE OF CONSTRUCTION.—Nothing in
18 paragraph (1) may be construed to—

19 “(A) require or compel any private entity
20 to enter in a contract or agreement described in
21 such paragraph; or

22 “(B) authorize the Secretary to take any
23 action with respect to any communications or
24 system traffic transiting or residing on any in-

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

6 (2) by adding at the end the following new
7 paragraph:

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

13 **SEC. 6. 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 en-
18 tities, not including State, local, and tribal governments,
19 that was not in effect on the day before the date of the
20 enactment of this Act.

21 **SEC. 7. STREAMLINING OF DEPARTMENT OF HOMELAND**
22 **SECURITY CYBERSECURITY AND INFRA-**
23 **STRUCTURE PROTECTION ORGANIZATION.**

24 (a) CYBERSECURITY AND INFRASTRUCTURE PRO-
25 TECTION DIRECTORATE.—The National Protection and

1 Programs Directorate of the Department of Homeland Se-
2 curity shall, after the date of the enactment of this Act,
3 be known and designated as the “Cybersecurity and Infra-
4 structure Protection Directorate”. Any reference to the
5 National Protection and Programs Directorate of the De-
6 partment in any law, regulation, map, document, record,
7 or other paper of the United States shall be deemed to
8 be a reference to the Cybersecurity and Infrastructure
9 Protection Directorate of the Department.

10 (b) SENIOR LEADERSHIP OF THE CYBERSECURITY
11 AND INFRASTRUCTURE PROTECTION DIRECTORATE.—

12 (1) IN GENERAL.—Paragraph (1) of section
13 103(a) of the Homeland Security Act of 2002 (6
14 U.S.C. 113(a)) is amended—

15 (A) by amending subparagraph (H) to
16 read as follows:

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

19 (B) by adding at the end the following new
20 subparagraphs:

21 “(K) A Deputy Under Secretary for Cyber-
22 security.

23 “(L) A Deputy Under Secretary for Infra-
24 structure Protection.”.

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

8 (c) REPORT.—To improve the operational capability
9 and effectiveness in carrying out the cybersecurity mission
10 of the Department of Homeland Security, the Secretary
11 of Homeland Security shall submit to the Committee on
12 Homeland Security of the House of Representatives and
13 the Committee on Homeland Security and Government Af-
14 fairs of the Senate a report on the feasibility of making
15 the Cybersecurity and Communications Office of the De-
16 partment an operational component of the Department.

17 **SEC. 8. CONFORMING AMENDMENTS.**

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

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

22 (2) in paragraph (9), by striking the period at
23 the end and inserting “; or”; and

24 (3) by adding at the end the following new
25 paragraph:

1 “(10) information shared with or provided to
2 the Department of Homeland Security pursuant to
3 the second section 226 of the Homeland Security
4 Act of 2002 (6 U.S.C. 148; relating to the National
5 Cybersecurity and Communications Integration Cen-
6 ter).”.