

APRIL 15, 2015

RULES COMMITTEE PRINT 114-12
TEXT OF H.R. 1731, NATIONAL CYBERSECURITY
PROTECTION ADVANCEMENT ACT OF 2015

[Showing the text of the bill as ordered reported by the
Committee on Homeland Security.]

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “National Cybersecurity
3 Protection Advancement Act of 2015”.

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

6 (a) **DEFINITIONS.—**

7 (1) **IN GENERAL.—**Subsection (a) of the second
8 section 226 of the Homeland Security Act of 2002
9 (6 U.S.C. 148; relating to the National Cybersecu-
10 rity and Communications Integration Center) is
11 amended—

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

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

16 (C) by adding at the end the following new
17 paragraphs:

1 “(5) the term ‘cyber threat indicator’ means
2 technical information that is necessary to describe or
3 identify—

4 “(A) a method for probing, monitoring,
5 maintaining, or establishing network awareness
6 of an information system for the purpose of dis-
7 cerning technical vulnerabilities of such infor-
8 mation system, if such method is known or rea-
9 sonably suspected of being associated with a
10 known or suspected cybersecurity risk, includ-
11 ing communications that reasonably appear to
12 be transmitted for the purpose of gathering
13 technical information related to a cybersecurity
14 risk;

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

17 “(C) a technical vulnerability, including
18 anomalous technical behavior that may become
19 a vulnerability;

20 “(D) a method of causing a user with le-
21 gitimate access to an information system or in-
22 formation that is stored on, processed by, or
23 transiting an information system to inadvert-
24 ently enable the defeat of a technical or oper-
25 ational control;

1 “(E) a method for unauthorized remote
2 identification of, access to, or use of an infor-
3 mation system or information that is stored on,
4 processed by, or transiting an information sys-
5 tem that is known or reasonably suspected of
6 being associated with a known or suspected cy-
7 bersecurity risk;

8 “(F) the actual or potential harm caused
9 by a cybersecurity risk, including a description
10 of the information exfiltrated as a result of a
11 particular cybersecurity risk;

12 “(G) any other attribute of a cybersecurity
13 risk that cannot be used to identify specific per-
14 sons reasonably believed to be unrelated to such
15 cybersecurity risk, if disclosure of such at-
16 tribute is not otherwise prohibited by law; or

17 “(H) any combination of subparagraphs
18 (A) through (G);

19 “(6) the term ‘cybersecurity purpose’ means the
20 purpose of protecting an information system or in-
21 formation that is stored on, processed by, or
22 transiting an information system from a cybersecu-
23 rity risk or incident;

24 “(7)(A) except as provided in subparagraph
25 (B), the term ‘defensive measure’ means an action,

1 device, procedure, signature, technique, or other
2 measure applied to an information system or infor-
3 mation that is stored on, processed by, or transiting
4 an information system that detects, prevents, or
5 mitigates a known or suspected cybersecurity risk or
6 incident, or any attribute of hardware, software,
7 process, or procedure that could enable or facilitate
8 the defeat of a security control;

9 “(B) such term does not include a measure that
10 destroys, renders unusable, or substantially harms
11 an information system or data on an information
12 system not belonging to—

13 “(i) the non-Federal entity, not including a
14 State, local, or tribal government, operating
15 such measure; or

16 “(ii) another Federal entity or non-Federal
17 entity that is authorized to provide consent and
18 has provided such consent to the non-Federal
19 entity referred to in clause (i);

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

24 “(9)(A) the term ‘private entity’ means a non-
25 Federal entity that is an individual or private group,

1 organization, proprietorship, partnership, trust, co-
2 operative, corporation, or other commercial or non-
3 profit entity, including an officer, employee, or agent
4 thereof;

5 “(B) such term includes a component of a
6 State, local, or tribal government performing electric
7 utility services;

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

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

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

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

22 (2) in clause (ii)—

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

1 (B) by striking “and” at the end;

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

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

6 “(iv) private entities.”.

7 **SEC. 3. INFORMATION SHARING STRUCTURE AND PROC-**
8 **ESSES.**

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

13 (1) in subsection (c)—

14 (A) in paragraph (1)—

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

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

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

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

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

3 (D) in paragraph (6)—

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

8 (ii) by striking “and” at the end;

9 (E) in paragraph (7)—

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

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

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

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

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

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

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

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

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

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

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

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

23 (2) in subsection (d)—

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

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

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

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

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

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

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

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

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

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

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

17 “(H) a National Coordinating Center for
18 Communications that coordinates the protec-
19 tion, response, and recovery of emergency com-
20 munications;

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

23 (3) in subsection (e)—

24 (A) in paragraph (1)—

1 (i) in subparagraph (A), by inserting
2 “cyber threat indicators, defensive meas-
3 ures, and” before “information”;

4 (ii) in subparagraph (B), by inserting
5 “cyber threat indicators, defensive meas-
6 ures, and” before “information”;

7 (iii) in subparagraph (F), by striking
8 “cybersecurity risks” and inserting “cyber
9 threat indicators, defensive measures, cy-
10 bersecurity risks,”;

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

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

17 (vi) by adding at the end the fol-
18 lowing:

19 “(H) the Center ensures that it shares in-
20 formation relating to cybersecurity risks and in-
21 cidents with small and medium-sized busi-
22 nesses, as appropriate; and

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

25 (B) in paragraph (2)—

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

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

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

13 (4) by adding at the end the following new sub-
14 sections:

15 “(g) RAPID AUTOMATED SHARING.—

16 “(1) IN GENERAL.—The Under Secretary for
17 Cybersecurity and Infrastructure Protection, in co-
18 ordination with industry and other stakeholders,
19 shall develop capabilities making use of existing in-
20 formation technology industry standards and best
21 practices, as appropriate, that support and rapidly
22 advance the development, adoption, and implementa-
23 tion of automated mechanisms for the timely sharing
24 of cyber threat indicators and defensive measures to
25 and from the Center and with each Federal agency

1 designated as the ‘Sector Specific Agency’ for each
2 critical infrastructure sector in accordance with sub-
3 section (h).

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

13 “(h) SECTOR SPECIFIC AGENCIES.—The Secretary,
14 in collaboration with the relevant critical infrastructure
15 sector and the heads of other appropriate Federal agen-
16 cies, shall recognize the Federal agency designated as of
17 March 25, 2015, as the ‘Sector Specific Agency’ for each
18 critical infrastructure sector designated in the Depart-
19 ment’s National Infrastructure Protection Plan. If the
20 designated Sector Specific Agency for a particular critical
21 infrastructure sector is the Department, for purposes of
22 this section, the Secretary is deemed to be the head of
23 such Sector Specific Agency and shall carry out this sec-
24 tion. The Secretary, in coordination with the heads of each
25 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 violated the terms of
4 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 “(E) COORDINATED VULNERABILITY DIS-
21 CLOSURE.—The Under Secretary for Cyberse-
22 curity and Infrastructure Protection, in coordi-
23 nation with industry and other stakeholders,
24 shall develop, publish, and adhere to policies
25 and procedures for coordinating vulnerability

1 disclosures, to the extent practicable, consistent
2 with international standards in the information
3 technology industry.

4 “(4) NETWORK AWARENESS AUTHORIZATION.—

5 “(A) IN GENERAL.—Notwithstanding any
6 other provision of law, a non-Federal entity, not
7 including a State, local, or tribal government,
8 may, for cybersecurity purposes, conduct net-
9 work awareness of—

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

13 “(ii) an information system of another
14 non-Federal entity, upon written consent
15 of such other non-Federal entity for con-
16 ducting such network awareness to protect
17 the rights or property of such other non-
18 Federal entity;

19 “(iii) an information system of a Fed-
20 eral entity, upon written consent of an au-
21 thorized representative of such Federal en-
22 tity for conducting such network awareness
23 to protect the rights or property of such
24 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 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 apply
9 only to the Department, consistent with
10 the need to protect information systems
11 from cybersecurity risks and incidents and
12 mitigate cybersecurity risks and incidents
13 in a timely manner, and shall—

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

23 “(II) reasonably limit, to the
24 greatest extent practicable, the re-
25 ceipt, retention, use, and disclosure of

1 cyber threat indicators and defensive
2 measures associated with specific per-
3 sons that is not necessary, for cyber-
4 security purposes, to protect a net-
5 work or information system from cy-
6 bersecurity risks or mitigate cyberse-
7 curity risks and incidents in a timely
8 manner;

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

11 “(IV) provide data integrity
12 through the prompt removal and de-
13 struction of obsolete or erroneous
14 names and personal information that
15 is unrelated to the cybersecurity risk
16 or incident information shared and re-
17 tained by the Center in accordance
18 with this section;

19 “(V) include requirements to
20 safeguard cyber threat indicators and
21 defensive measures retained by the
22 Center, including information that is
23 proprietary or business-sensitive that
24 may be used to identify specific per-

1 sons from unauthorized access or ac-
2 quisition;

3 “(VI) protect the confidentiality
4 of cyber threat indicators and defen-
5 sive measures associated with specific
6 persons to the greatest extent prac-
7 ticable; and

8 “(VII) ensure all relevant con-
9 stitutional, legal, and privacy protec-
10 tions are observed.

11 “(ii) SUBMISSION TO CONGRESS.—
12 Not later than 180 days after the date of
13 the enactment of this section and annually
14 thereafter, the Chief Privacy Officer and
15 the Officer for Civil Rights and Civil Lib-
16 erties of the Department, in consultation
17 with the Privacy and Civil Liberties Over-
18 sight Board (established pursuant to sec-
19 tion 1061 of the Intelligence Reform and
20 Terrorism Prevention Act of 2004 (42
21 U.S.C. 2000ee)), shall submit to the Com-
22 mittee on Homeland Security of the House
23 of Representatives and the Committee on
24 Homeland Security and Governmental Af-
25 fairs of the Senate the policies and proce-

1 dures governing the sharing of cyber threat
2 indicators, defensive measures, and infor-
3 mation related to cybsersecurity risks and
4 incidents described in clause (i) of sub-
5 paragraph (A).

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

22 “(iv) CONSULTATION.—The Under
23 Secretary for Cybersecurity and Infrastruc-
24 ture Protection when establishing policies
25 and procedures to support privacy and civil

1 liberties may consult with the National In-
2 stitute of Standards and Technology.

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

6 “ (i) monitor the implementation of
7 the policies and procedures governing the
8 sharing of cyber threat indicators and de-
9 fensive measures established pursuant to
10 clause (i) of subparagraph (A);

11 “ (ii) regularly review and update pri-
12 vacy impact assessments, as appropriate,
13 to ensure all relevant constitutional, legal,
14 and privacy protections are being followed;

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

19 “ (iv) annually submit to the Com-
20 mittee on Homeland Security of the House
21 of Representatives and the Committee on
22 Homeland Security and Governmental Af-
23 fairs of the Senate a report that contains
24 a review of the effectiveness of such poli-

1 cies and procedures to protect privacy and
2 civil liberties; and

3 “(v) ensure there are appropriate
4 sanctions in place for officers, employees,
5 or agents of the Department who inten-
6 tionally or willfully conduct activities under
7 this section in an unauthorized manner.

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

24 “(i) A report on the receipt, use, and
25 dissemination of cyber threat indicators

1 and defensive measures that have been
2 shared with Federal entities under this
3 section.

4 “(ii) Information on the use by the
5 Center of such information for a purpose
6 other than a cybersecurity purpose.

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

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

12 “(v) The appropriate metrics that
13 exist to determine the impact, if any, on
14 privacy and civil liberties as a result of the
15 sharing of such information with the Cen-
16 ter.

17 “(vi) A list of other Federal agencies
18 receiving such information.

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

23 “(viii) Any recommendations of the
24 Inspector General of the Department for

1 improvements or modifications to informa-
2 tion sharing under this section.

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

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 or defensive measures through the Cen-
9 ter or otherwise under this section—

10 “(i) may use, retain, or further dis-
11 close such cyber threat indicators or defen-
12 sive measures solely for cybersecurity pur-
13 poses;

14 “(ii) shall, prior to such sharing, take
15 reasonable efforts to remove information
16 that can be used to identify specific per-
17 sons and is reasonably believed at the time
18 of sharing to be unrelated to a cybersecu-
19 rity risk or incident, and to safeguard in-
20 formation that can be used to identify spe-
21 cific persons from unintended disclosure or
22 unauthorized access or acquisition;

23 “(iii) shall comply with appropriate
24 restrictions that a Federal entity or non-
25 Federal entity places on the subsequent

1 disclosure or retention of cyber threat indi-
2 cators and defensive measures that it dis-
3 closes to other Federal entities or non-Fed-
4 eral entities;

5 “(iv) shall be deemed to have volun-
6 tarily shared such cyber threat indicators
7 or defensive measures;

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

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

16 “(B) FEDERAL ENTITIES.—

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

23 “(I) may use, retain, or further
24 disclose such cyber threat indicators

1 or defensive measures solely for cyber-
2 security purposes;

3 “(II) shall, prior to such sharing,
4 take reasonable efforts to remove in-
5 formation that can be used to identify
6 specific persons and is reasonably be-
7 lieved at the time of sharing to be un-
8 related to a cybersecurity risk or inci-
9 dent, and to safeguard information
10 that can be used to identify specific
11 persons from unintended disclosure or
12 unauthorized access or acquisition;

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

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

21 “(V) may not use such cyber
22 threat indicators or defensive meas-
23 ures to engage in surveillance or other
24 collection activities for the purpose of

1 tracking an individual’s personally
2 identifiable information.

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

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

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

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

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

24 “(V) may not be subject to a rule
25 of any Federal entity or any judicial

1 doctrine regarding ex parte commu-
2 nications with a decisionmaking offi-
3 cial.

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

6 “(i) USES OF INFORMATION.—A
7 State, local, or tribal government that re-
8 ceives cyber threat indicators or defensive
9 measures from the Center from a Federal
10 entity or a 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 consider such infor-
2 mation the commercial, financial, and
3 proprietary information of such Fed-
4 eral entity or non-Federal entity if so
5 designated by such Federal entity or
6 non-Federal entity;

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

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

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

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

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

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

3 “(8) LIABILITY EXEMPTIONS.—

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

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

21 “(C) WILLFUL MISCONDUCT.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 “(iv) the District of Columbia.

16 “(C) STATUTE OF LIMITATIONS.—No ac-
17 tion shall lie under this subsection unless such
18 action is commenced not later than two years
19 after the date of the violation of any restriction
20 specified in paragraph (3), (6), or 7(B), or any
21 other provision of this section, that is the basis
22 for such action.

23 “(D) EXCLUSIVE CAUSE OF ACTION.—A
24 cause of action under this subsection shall be
25 the exclusive means available to a complainant

1 seeking a remedy for a violation of any restric-
2 tion specified in paragraph (3), (6), or 7(B) or
3 any other provision of this section.

4 “(10) ANTI-TRUST EXEMPTION.—

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

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

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

23 “(ii) communicating or disclosing a
24 cyber threat indicator or defensive measure
25 to help prevent, investigate, or mitigate the

1 effect of a cybersecurity risk or incident to
2 an information system or information that
3 is stored on, processed by, or transiting an
4 information system.

5 “(C) PROHIBITED CONDUCT.—Nothing in
6 this section may be construed to permit price-
7 fixing, allocating a market between competitors,
8 monopolizing or attempting to monopolize a
9 market, or exchanges of price or cost informa-
10 tion, customer lists, or information regarding
11 future competitive planning.

12 “(11) CONSTRUCTION AND PREEMPTION.—

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

23 “(B) WHISTLE BLOWER PROTECTIONS.—
24 Nothing in this section may be construed to
25 prohibit or limit the disclosure of information

1 protected under section 2302(b)(8) of title 5,
2 United States Code (governing disclosures of il-
3 legality, waste, fraud, abuse, or public health or
4 safety threats), section 7211 of title 5, United
5 States Code (governing disclosures to Con-
6 gress), section 1034 of title 10, United States
7 Code (governing disclosure to Congress by
8 members of the military), section 1104 of the
9 National Security Act of 1947 (50 U.S.C.
10 3234) (governing disclosure by employees of
11 elements of the intelligence community), or any
12 similar provision of Federal or State law.

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

18 “(D) PRESERVATION OF CONTRACTUAL
19 OBLIGATIONS AND RIGHTS.—Nothing in this
20 section may be construed to—

21 “(i) amend, repeal, or supersede any
22 current or future contractual agreement,
23 terms of service agreement, or other con-
24 tractual relationship between any non-Fed-

1 eral entities, or between any non-Federal
2 entity and a Federal entity; or

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

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

9 “(i) require a non-Federal entity to
10 provide information to a Federal entity;

11 “(ii) condition the sharing of cyber
12 threat indicators or defensive measures
13 with a non-Federal entity on such non-
14 Federal entity’s provision of cyber threat
15 indicators or defensive measures to a Fed-
16 eral entity; or

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

21 “(F) NO LIABILITY FOR NON-PARTICIPA-
22 TION.—Nothing in this section may be con-
23 strued to subject any non-Federal entity to li-
24 ability for choosing to not engage in the vol-
25 untary activities authorized under this section.

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

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

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

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

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

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

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

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

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

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

1 **SEC. 4. INFORMATION SHARING AND ANALYSIS ORGANIZA-**
2 **TIONS.**

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

5 (1) in paragraph (5)—

6 (A) in subparagraph (A)—

7 (i) by inserting “information related
8 to cybersecurity risks and incidents and”
9 after “critical infrastructure information”;
10 and

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

15 (B) in subparagraph (B)—

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

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

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

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

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

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

11 **SEC. 5. STREAMLINING OF DEPARTMENT OF HOMELAND**
12 **SECURITY CYBERSECURITY AND INFRA-**
13 **STRUCTURE PROTECTION ORGANIZATION.**

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

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

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

6 (A) in paragraph (1)—

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

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

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

13 “(K) A Deputy Under Secretary for Cyber-
14 security.

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

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

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

24 (2) CONTINUATION IN OFFICE.—The individ-
25 uals who hold the positions referred in subpara-

1 graphs (H), (K), and (L) of paragraph (1) of section
2 103(a) the Homeland Security Act of 2002 (as
3 amended and added by paragraph (1) of this sub-
4 section) as of the date of the enactment of this Act
5 may continue to hold such positions.

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

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

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

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

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

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

8 (3) by adding at the end the following new sub-
9 section:

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

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

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

1 **SEC. 7. SECURITY AND RESILIENCY OF PUBLIC SAFETY**
2 **COMMUNICATIONS; CYBERSECURITY AWARE-**
3 **NESS CAMPAIGN.**

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

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

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

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

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

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

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

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

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

12 (b) CLERICAL AMENDMENT.—The table of contents
13 of the Homeland Security Act of 2002 is amended by in-
14 serting after the item relating to section 226 (relating to
15 cybersecurity recruitment and retention) the following new
16 items:

“Sec. 230. Security and resiliency of public safety communications.
“Sec. 231. Cybersecurity awareness campaign.”.

17 **SEC. 8. CRITICAL INFRASTRUCTURE PROTECTION RE-**
18 **SEARCH AND DEVELOPMENT.**

19 (a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSOR-
20 TIUMS.—Title III of the Homeland Security Act of 2002
21 (6 U.S.C. 181 et seq.) is amended by adding at the end
22 the following new section:

1 **“SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR**
2 **CRITICAL INFRASTRUCTURE PROTECTION.**

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

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

15 “(1) An identification of critical infrastructure
16 security risks and any associated security technology
17 gaps, that are developed following—

18 “(A) consultation with stakeholders, in-
19 cluding critical infrastructure Sector Coordi-
20 nating Councils; and

21 “(B) performance by the Department of a
22 risk and gap analysis that considers informa-
23 tion received in such consultations.

24 “(2) A set of critical infrastructure security
25 technology needs that—

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

3 “(B) emphasizes research and development
4 of technologies that need to be accelerated due
5 to rapidly evolving threats or rapidly advancing
6 infrastructure technology; and

7 “(C) includes research, development, and
8 acquisition roadmaps with clearly defined objec-
9 tives, goals, and measures.

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

15 “(4) An identification of current and planned
16 programmatic initiatives for fostering the rapid ad-
17 vancement and deployment of security technologies
18 for critical infrastructure protection, including a
19 consideration of opportunities for public-private
20 partnerships, intragovernment collaboration, univer-
21 sity centers of excellence, and national laboratory
22 technology transfer.

23 “(5) A description of progress made with re-
24 spect to each critical infrastructure security risk, as-
25 sociated security technology gap, and critical infra-

1 structure technology need identified in the preceding
2 strategic plan required under subsection (a).

3 “(c) COORDINATION.—In carrying out this section,
4 the Under Secretary for Science and Technology shall co-
5 ordinate with the Under Secretary for the National Pro-
6 tection and Programs Directorate.

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

10 “(1) critical infrastructure Sector Coordinating
11 Councils;

12 “(2) to the extent practicable, subject matter
13 experts on critical infrastructure protection from
14 universities, colleges, national laboratories, and pri-
15 vate industry;

16 “(3) the heads of other relevant Federal depart-
17 ments and agencies that conduct research and devel-
18 opment relating to critical infrastructure protection;
19 and

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

22 (b) CLERICAL AMENDMENT.—The table of contents
23 of the Homeland Security Act of 2002 is amended by in-
24 serting after the item relating to section 317 the following
25 new item:

“Sec. 318. Research and development strategy for critical infrastructure protection.”.

1 **SEC. 9. REPORT ON REDUCING CYBERSECURITY RISKS IN**
2 **DHS DATA CENTERS.**

3 Not later than one year after the date of the enact-
4 ment of this Act, the Secretary of Homeland Security shall
5 submit to the Committee on Homeland Security of the
6 House of Representatives and the Committee on Home-
7 land Security and Governmental Affairs of the Senate a
8 report on the feasibility of the Department of Homeland
9 Security creating an environment for the reduction in cy-
10 bersecurity risks in Department data centers, including by
11 increasing compartmentalization between systems, and
12 providing a mix of security controls between such compart-
13 ments.

14 **SEC. 10. ASSESSMENT.**

15 Not later than two years after the date of the enact-
16 ment of this Act, the Comptroller General of the United
17 States shall submit to the Committee on Homeland Secu-
18 rity of the House of Representatives and the Committee
19 on Homeland Security and Governmental Affairs of the
20 Senate a report that contains an assessment of the imple-
21 mentation by the Secretary of Homeland Security of this
22 Act and the amendments made by this Act and, to the
23 extent practicable, findings regarding increases in the
24 sharing of cyber threat indicators, defensive measures,

1 and information relating to cybersecurity risks and inci-
2 dents at the National Cybersecurity and Communications
3 Integration Center and throughout the United States.

4 **SEC. 11. CONSULTATION.**

5 The Under Secretary for Cybersecurity and Infra-
6 structure Protection shall produce a report on the feasi-
7 bility of creating a risk-informed prioritization plan should
8 multiple critical infrastructures experience cyber incidents
9 simultaneously.

10 **SEC. 12. TECHNICAL ASSISTANCE.**

11 The Inspector General of the Department of Home-
12 land Security shall review the operations of the United
13 States Computer Emergency Readiness Team (US-
14 CERT) and the Industrial Control Systems Cyber Emer-
15 gency Response Team (ICS-CERT) to assess the capacity
16 to provide technical assistance to non-Federal entities and
17 to adequately respond to potential increases in requests
18 for technical assistance.

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

20 Nothing in this Act or the amendments made by this
21 Act may be construed to grant the Secretary of Homeland
22 Security any authority to promulgate regulations or set
23 standards relating to the cybersecurity of non-Federal en-
24 tities, not including State, local, and tribal governments,

1 that was not in effect on the day before the date of the
2 enactment of this Act.

3 **SEC. 14. SUNSET.**

4 Any requirements for reports required by this Act or
5 the amendments made by this Act shall terminate on the
6 date that is seven years after the date of the enactment
7 of this Act.

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

9 No funds are authorized to be appropriated to carry
10 out this Act and the amendments made by this Act. This
11 Act and such amendments shall be carried out using
12 amounts appropriated or otherwise made available for
13 such purposes.

