

1 **DIVISION N—CYBERSECURITY**
2 **ACT OF 2015**

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

4 (a) **SHORT TITLE.**—This division may be cited as the
5 “Cybersecurity Act of 2015”.

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

Sec. 1. Short title; table of contents.

TITLE I—CYBERSECURITY INFORMATION SHARING

Sec. 101. Short title.

Sec. 102. Definitions.

Sec. 103. Sharing of information by the Federal Government.

Sec. 104. Authorizations for preventing, detecting, analyzing, and mitigating
cybersecurity threats.

Sec. 105. Sharing of cyber threat indicators and defensive measures with the
Federal Government.

Sec. 106. Protection from liability.

Sec. 107. Oversight of Government activities.

Sec. 108. Construction and preemption.

Sec. 109. Report on cybersecurity threats.

Sec. 110. Exception to limitation on authority of Secretary of Defense to dis-
seminate certain information.

Sec. 111. Effective period.

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

Subtitle A—National Cybersecurity and Communications Integration Center

Sec. 201. Short title.

Sec. 202. Definitions.

Sec. 203. Information sharing structure and processes.

Sec. 204. Information sharing and analysis organizations.

Sec. 205. National response framework.

Sec. 206. Report on reducing cybersecurity risks in DHS data centers.

Sec. 207. Assessment.

Sec. 208. Multiple simultaneous cyber incidents at critical infrastructure.

Sec. 209. Report on cybersecurity vulnerabilities of United States ports.

Sec. 210. Prohibition on new regulatory authority.

Sec. 211. Termination of reporting requirements.

Subtitle B—Federal Cybersecurity Enhancement

Sec. 221. Short title.

Sec. 222. Definitions.

Sec. 223. Improved Federal network security.

Sec. 224. Advanced internal defenses.

- Sec. 225. Federal cybersecurity requirements.
- Sec. 226. Assessment; reports.
- Sec. 227. Termination.
- Sec. 228. Identification of information systems relating to national security.
- Sec. 229. Direction to agencies.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

- Sec. 301. Short title.
- Sec. 302. Definitions.
- Sec. 303. National cybersecurity workforce measurement initiative.
- Sec. 304. Identification of cyber-related work roles of critical need.
- Sec. 305. Government Accountability Office status reports.

TITLE IV—OTHER CYBER MATTERS

- Sec. 401. Study on mobile device security.
- Sec. 402. Department of State international cyberspace policy strategy.
- Sec. 403. Apprehension and prosecution of international cyber criminals.
- Sec. 404. Enhancement of emergency services.
- Sec. 405. Improving cybersecurity in the health care industry.
- Sec. 406. Federal computer security.
- Sec. 407. Stopping the fraudulent sale of financial information of people of the United States.

1 **TITLE I—CYBERSECURITY**
2 **INFORMATION SHARING**

3 **SEC. 101. SHORT TITLE.**

4 This title may be cited as the “Cybersecurity Infor-
5 mation Sharing Act of 2015”.

6 **SEC. 102. DEFINITIONS.**

7 In this title:

8 (1) **AGENCY.**—The term “agency” has the
9 meaning given the term in section 3502 of title 44,
10 United States Code.

11 (2) **ANTITRUST LAWS.**—The term “antitrust
12 laws”—

13 (A) has the meaning given the term in the
14 first section of the Clayton Act (15 U.S.C. 12);

1 (B) includes section 5 of the Federal
2 Trade Commission Act (15 U.S.C. 45) to the
3 extent that section 5 of that Act applies to un-
4 fair methods of competition; and

5 (C) includes any State antitrust law, but
6 only to the extent that such law is consistent
7 with the law referred to in subparagraph (A) or
8 the law referred to in subparagraph (B).

9 (3) APPROPRIATE FEDERAL ENTITIES.—The
10 term “appropriate Federal entities” means the fol-
11 lowing:

12 (A) The Department of Commerce.

13 (B) The Department of Defense.

14 (C) The Department of Energy.

15 (D) The Department of Homeland Secu-
16 rity.

17 (E) The Department of Justice.

18 (F) The Department of the Treasury.

19 (G) The Office of the Director of National
20 Intelligence.

21 (4) CYBERSECURITY PURPOSE.—The term
22 “cybersecurity purpose” means the purpose of pro-
23 tecting an information system or information that is
24 stored on, processed by, or transiting an information

1 system from a cybersecurity threat or security vul-
2 nerability.

3 (5) CYBERSECURITY THREAT.—

4 (A) IN GENERAL.—Except as provided in
5 subparagraph (B), the term “cybersecurity
6 threat” means an action, not protected by the
7 First Amendment to the Constitution of the
8 United States, on or through an information
9 system that may result in an unauthorized ef-
10 fort to adversely impact the security, avail-
11 ability, confidentiality, or integrity of an infor-
12 mation system or information that is stored on,
13 processed by, or transiting an information sys-
14 tem.

15 (B) EXCLUSION.—The term “cybersecurity
16 threat” does not include any action that solely
17 involves a violation of a consumer term of serv-
18 ice or a consumer licensing agreement.

19 (6) CYBER THREAT INDICATOR.—The term
20 “cyber threat indicator” means information that is
21 necessary to describe or identify—

22 (A) malicious reconnaissance, including
23 anomalous patterns of communications that ap-
24 pear to be transmitted for the purpose of gath-

1 ering technical information related to a
2 cybersecurity threat or security vulnerability;

3 (B) a method of defeating a security con-
4 trol or exploitation of a security vulnerability;

5 (C) a security vulnerability, including
6 anomalous activity that appears to indicate the
7 existence of a security vulnerability;

8 (D) a method of causing a user with legiti-
9 mate access to an information system or infor-
10 mation that is stored on, processed by, or
11 transiting an information system to unwittingly
12 enable the defeat of a security control or exploi-
13 tation of a security vulnerability;

14 (E) malicious cyber command and control;

15 (F) the actual or potential harm caused by
16 an incident, including a description of the infor-
17 mation exfiltrated as a result of a particular
18 cybersecurity threat;

19 (G) any other attribute of a cybersecurity
20 threat, if disclosure of such attribute is not oth-
21 erwise prohibited by law; or

22 (H) any combination thereof.

23 (7) DEFENSIVE MEASURE.—

24 (A) IN GENERAL.—Except as provided in
25 subparagraph (B), the term “defensive meas-

1 ure” means an action, device, procedure, signa-
2 ture, technique, or other measure applied to an
3 information system or information that is
4 stored on, processed by, or transiting an infor-
5 mation system that detects, prevents, or miti-
6 gates a known or suspected cybersecurity threat
7 or security vulnerability.

8 (B) EXCLUSION.—The term “defensive
9 measure” does not include a measure that de-
10 stroys, renders unusable, provides unauthorized
11 access to, or substantially harms an information
12 system or information stored on, processed by,
13 or transiting such information system not
14 owned by—

15 (i) the private entity operating the
16 measure; or

17 (ii) another entity or Federal entity
18 that is authorized to provide consent and
19 has provided consent to that private entity
20 for operation of such measure.

21 (8) FEDERAL ENTITY.—The term “Federal en-
22 tity” means a department or agency of the United
23 States or any component of such department or
24 agency.

1 (9) INFORMATION SYSTEM.—The term “infor-
2 mation system”—

3 (A) has the meaning given the term in sec-
4 tion 3502 of title 44, United States Code; and

5 (B) includes industrial control systems,
6 such as supervisory control and data acquisition
7 systems, distributed control systems, and pro-
8 grammable logic controllers.

9 (10) LOCAL GOVERNMENT.—The term “local
10 government” means any borough, city, county, par-
11 ish, town, township, village, or other political sub-
12 division of a State.

13 (11) MALICIOUS CYBER COMMAND AND CON-
14 TROL.—The term “malicious cyber command and
15 control” means a method for unauthorized remote
16 identification of, access to, or use of, an information
17 system or information that is stored on, processed
18 by, or transiting an information system.

19 (12) MALICIOUS RECONNAISSANCE.—The term
20 “malicious reconnaissance” means a method for ac-
21 tively probing or passively monitoring an information
22 system for the purpose of discerning security
23 vulnerabilities of the information system, if such
24 method is associated with a known or suspected
25 cybersecurity threat.

1 (13) MONITOR.—The term “monitor” means to
2 acquire, identify, or scan, or to possess, information
3 that is stored on, processed by, or transiting an in-
4 formation system.

5 (14) NON-FEDERAL ENTITY.—

6 (A) IN GENERAL.—Except as otherwise
7 provided in this paragraph, the term “non-Fed-
8 eral entity” means any private entity, non-Fed-
9 eral government agency or department, or
10 State, tribal, or local government (including a
11 political subdivision, department, or component
12 thereof).

13 (B) INCLUSIONS.—The term “non-Federal
14 entity” includes a government agency or depart-
15 ment of the District of Columbia, the Common-
16 wealth of Puerto Rico, the United States Virgin
17 Islands, Guam, American Samoa, the Northern
18 Mariana Islands, and any other territory or
19 possession of the United States.

20 (C) EXCLUSION.—The term “non-Federal
21 entity” does not include a foreign power as de-
22 fined in section 101 of the Foreign Intelligence
23 Surveillance Act of 1978 (50 U.S.C. 1801).

24 (15) PRIVATE ENTITY.—

1 (A) IN GENERAL.—Except as otherwise
2 provided in this paragraph, the term “private
3 entity” means any person or private group, or-
4 ganization, proprietorship, partnership, trust,
5 cooperative, corporation, or other commercial or
6 nonprofit entity, including an officer, employee,
7 or agent thereof.

8 (B) INCLUSION.—The term “private enti-
9 ty” includes a State, tribal, or local government
10 performing utility services, such as electric, nat-
11 ural gas, or water services.

12 (C) EXCLUSION.—The term “private enti-
13 ty” does not include a foreign power as defined
14 in section 101 of the Foreign Intelligence Sur-
15 veillance Act of 1978 (50 U.S.C. 1801).

16 (16) SECURITY CONTROL.—The term “security
17 control” means the management, operational, and
18 technical controls used to protect against an unau-
19 thorized effort to adversely affect the confidentiality,
20 integrity, and availability of an information system
21 or its information.

22 (17) SECURITY VULNERABILITY.—The term
23 “security vulnerability” means any attribute of hard-
24 ware, software, process, or procedure that could en-
25 able or facilitate the defeat of a security control.

1 (18) TRIBAL.—The term “tribal” has the
2 meaning given the term “Indian tribe” in section 4
3 of the Indian Self-Determination and Education As-
4 sistance Act (25 U.S.C. 450b).

5 **SEC. 103. SHARING OF INFORMATION BY THE FEDERAL**
6 **GOVERNMENT.**

7 (a) IN GENERAL.—Consistent with the protection of
8 classified information, intelligence sources and methods,
9 and privacy and civil liberties, the Director of National
10 Intelligence, the Secretary of Homeland Security, the Sec-
11 retary of Defense, and the Attorney General, in consulta-
12 tion with the heads of the appropriate Federal entities,
13 shall jointly develop and issue procedures to facilitate and
14 promote—

15 (1) the timely sharing of classified cyber threat
16 indicators and defensive measures in the possession
17 of the Federal Government with representatives of
18 relevant Federal entities and non-Federal entities
19 that have appropriate security clearances;

20 (2) the timely sharing with relevant Federal en-
21 tities and non-Federal entities of cyber threat indica-
22 tors, defensive measures, and information relating to
23 cybersecurity threats or authorized uses under this
24 title, in the possession of the Federal Government

1 that may be declassified and shared at an unclassi-
2 fied level;

3 (3) the timely sharing with relevant Federal en-
4 tities and non-Federal entities, or the public if ap-
5 propriate, of unclassified, including controlled un-
6 classified, cyber threat indicators and defensive
7 measures in the possession of the Federal Govern-
8 ment;

9 (4) the timely sharing with Federal entities and
10 non-Federal entities, if appropriate, of information
11 relating to cybersecurity threats or authorized uses
12 under this title, in the possession of the Federal
13 Government about cybersecurity threats to such en-
14 tities to prevent or mitigate adverse effects from
15 such cybersecurity threats; and

16 (5) the periodic sharing, through publication
17 and targeted outreach, of cybersecurity best prac-
18 tices that are developed based on ongoing analyses
19 of cyber threat indicators, defensive measures, and
20 information relating to cybersecurity threats or au-
21 thorized uses under this title, in the possession of
22 the Federal Government, with attention to accessi-
23 bility and implementation challenges faced by small
24 business concerns (as defined in section 3 of the
25 Small Business Act (15 U.S.C. 632)).

1 (b) DEVELOPMENT OF PROCEDURES.—

2 (1) IN GENERAL.—The procedures developed
3 under subsection (a) shall—

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

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

15 (C) include procedures for notifying, in a
16 timely manner, Federal entities and non-Fed-
17 eral entities that have received a cyber threat
18 indicator or defensive measure from a Federal
19 entity under this title that is known or deter-
20 mined to be in error or in contravention of the
21 requirements of this title or another provision
22 of Federal law or policy of such error or con-
23 travention;

24 (D) include requirements for Federal enti-
25 ties sharing cyber threat indicators or defensive

1 measures to implement and utilize security con-
2 trols to protect against unauthorized access to
3 or acquisition of such cyber threat indicators or
4 defensive measures;

5 (E) include procedures that require a Fed-
6 eral entity, prior to the sharing of a cyber
7 threat indicator—

8 (i) to review such cyber threat indi-
9 cator to assess whether such cyber threat
10 indicator contains any information not di-
11 rectly related to a cybersecurity threat that
12 such Federal entity knows at the time of
13 sharing to be personal information of a
14 specific individual or information that
15 identifies a specific individual and remove
16 such information; or

17 (ii) to implement and utilize a tech-
18 nical capability configured to remove any
19 information not directly related to a
20 cybersecurity threat that the Federal entity
21 knows at the time of sharing to be per-
22 sonal information of a specific individual or
23 information that identifies a specific indi-
24 vidual; and

1 (F) include procedures for notifying, in a
2 timely manner, any United States person whose
3 personal information is known or determined to
4 have been shared by a Federal entity in viola-
5 tion of this title.

6 (2) CONSULTATION.—In developing the proce-
7 dures required under this section, the Director of
8 National Intelligence, the Secretary of Homeland Se-
9 curity, the Secretary of Defense, and the Attorney
10 General shall consult with appropriate Federal enti-
11 ties, including the Small Business Administration
12 and the National Laboratories (as defined in section
13 2 of the Energy Policy Act of 2005 (42 U.S.C.
14 15801)), to ensure that effective protocols are imple-
15 mented that will facilitate and promote the sharing
16 of cyber threat indicators by the Federal Govern-
17 ment in a timely manner.

18 (c) SUBMITTAL TO CONGRESS.—Not later than 60
19 days after the date of the enactment of this Act, the Direc-
20 tor of National Intelligence, in consultation with the heads
21 of the appropriate Federal entities, shall submit to Con-
22 gress the procedures required by subsection (a).

1 **SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
2 **ANALYZING, AND MITIGATING**
3 **CYBERSECURITY THREATS.**

4 (a) AUTHORIZATION FOR MONITORING.—

5 (1) IN GENERAL.—Notwithstanding any other
6 provision of law, a private entity may, for
7 cybersecurity purposes, monitor—

8 (A) an information system of such private
9 entity;

10 (B) an information system of another non-
11 Federal entity, upon the authorization and writ-
12 ten consent of such other entity;

13 (C) an information system of a Federal en-
14 tity, upon the authorization and written consent
15 of an authorized representative of the Federal
16 entity; and

17 (D) information that is stored on, proc-
18 essed by, or transiting an information system
19 monitored by the private entity under this para-
20 graph.

21 (2) CONSTRUCTION.—Nothing in this sub-
22 section shall be construed—

23 (A) to authorize the monitoring of an in-
24 formation system, or the use of any information
25 obtained through such monitoring, other than
26 as provided in this title; or

1 (B) to limit otherwise lawful activity.

2 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE
3 MEASURES.—

4 (1) IN GENERAL.—Notwithstanding any other
5 provision of law, a private entity may, for
6 cybersecurity purposes, operate a defensive measure
7 that is applied to—

8 (A) an information system of such private
9 entity in order to protect the rights or property
10 of the private entity;

11 (B) an information system of another non-
12 Federal entity upon written consent of such en-
13 tity for operation of such defensive measure to
14 protect the rights or property of such entity;
15 and

16 (C) an information system of a Federal en-
17 tity upon written consent of an authorized rep-
18 resentative of such Federal entity for operation
19 of such defensive measure to protect the rights
20 or property of the Federal Government.

21 (2) CONSTRUCTION.—Nothing in this sub-
22 section shall be construed—

23 (A) to authorize the use of a defensive
24 measure other than as provided in this sub-
25 section; or

1 (B) to limit otherwise lawful activity.

2 (c) AUTHORIZATION FOR SHARING OR RECEIVING
3 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-
4 URES.—

5 (1) IN GENERAL.—Except as provided in para-
6 graph (2) and notwithstanding any other provision
7 of law, a non-Federal entity may, for a cybersecurity
8 purpose and consistent with the protection of classi-
9 fied information, share with, or receive from, any
10 other non-Federal entity or the Federal Government
11 a cyber threat indicator or defensive measure.

12 (2) LAWFUL RESTRICTION.—A non-Federal en-
13 tity receiving a cyber threat indicator or defensive
14 measure from another non-Federal entity or a Fed-
15 eral entity shall comply with otherwise lawful restric-
16 tions placed on the sharing or use of such cyber
17 threat indicator or defensive measure by the sharing
18 non-Federal entity or Federal entity.

19 (3) CONSTRUCTION.—Nothing in this sub-
20 section shall be construed—

21 (A) to authorize the sharing or receiving of
22 a cyber threat indicator or defensive measure
23 other than as provided in this subsection; or

24 (B) to limit otherwise lawful activity.

25 (d) PROTECTION AND USE OF INFORMATION.—

1 (1) SECURITY OF INFORMATION.—A non-Fed-
2 eral entity monitoring an information system, oper-
3 ating a defensive measure, or providing or receiving
4 a cyber threat indicator or defensive measure under
5 this section shall implement and utilize a security
6 control to protect against unauthorized access to or
7 acquisition of such cyber threat indicator or defen-
8 sive measure.

9 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
10 TION.—A non-Federal entity sharing a cyber threat
11 indicator pursuant to this title shall, prior to such
12 sharing—

13 (A) review such cyber threat indicator to
14 assess whether such cyber threat indicator con-
15 tains any information not directly related to a
16 cybersecurity threat that the non-Federal entity
17 knows at the time of sharing to be personal in-
18 formation of a specific individual or information
19 that identifies a specific individual and remove
20 such information; or

21 (B) implement and utilize a technical capa-
22 bility configured to remove any information not
23 directly related to a cybersecurity threat that
24 the non-Federal entity knows at the time of
25 sharing to be personal information of a specific

1 individual or information that identifies a spe-
2 cific individual.

3 (3) USE OF CYBER THREAT INDICATORS AND
4 DEFENSIVE MEASURES BY NON-FEDERAL ENTI-
5 TIES.—

6 (A) IN GENERAL.—Consistent with this
7 title, a cyber threat indicator or defensive meas-
8 ure shared or received under this section may,
9 for cybersecurity purposes—

10 (i) be used by a non-Federal entity to
11 monitor or operate a defensive measure
12 that is applied to—

13 (I) an information system of the
14 non-Federal entity; or

15 (II) an information system of an-
16 other non-Federal entity or a Federal
17 entity upon the written consent of
18 that other non-Federal entity or that
19 Federal entity; and

20 (ii) be otherwise used, retained, and
21 further shared by a non-Federal entity
22 subject to—

23 (I) an otherwise lawful restriction
24 placed by the sharing non-Federal en-
25 tity or Federal entity on such cyber

1 threat indicator or defensive measure;
2 or

3 (II) an otherwise applicable pro-
4 vision of law.

5 (B) CONSTRUCTION.—Nothing in this
6 paragraph shall be construed to authorize the
7 use of a cyber threat indicator or defensive
8 measure other than as provided in this section.

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

11 (A) LAW ENFORCEMENT USE.—A State,
12 tribal, or local government that receives a cyber
13 threat indicator or defensive measure under this
14 title may use such cyber threat indicator or de-
15 fensive measure for the purposes described in
16 section 105(d)(5)(A).

17 (B) EXEMPTION FROM DISCLOSURE.—A
18 cyber threat indicator or defensive measure
19 shared by or with a State, tribal, or local gov-
20 ernment, including a component of a State,
21 tribal, or local government that is a private en-
22 tity, under this section shall be—

23 (i) deemed voluntarily shared informa-
24 tion; and

1 (ii) exempt from disclosure under any
2 provision of State, tribal, or local freedom
3 of information law, open government law,
4 open meetings law, open records law, sun-
5 shine law, or similar law requiring disclo-
6 sure of information or records.

7 (C) STATE, TRIBAL, AND LOCAL REGU-
8 LATORY AUTHORITY.—

9 (i) IN GENERAL.—Except as provided
10 in clause (ii), a cyber threat indicator or
11 defensive measure shared with a State,
12 tribal, or local government under this title
13 shall not be used by any State, tribal, or
14 local government to regulate, including an
15 enforcement action, the lawful activity of
16 any non-Federal entity or any activity
17 taken by a non-Federal entity pursuant to
18 mandatory standards, including an activity
19 relating to monitoring, operating a defen-
20 sive measure, or sharing of a cyber threat
21 indicator.

22 (ii) REGULATORY AUTHORITY SPE-
23 CIFICALLY RELATING TO PREVENTION OR
24 MITIGATION OF CYBERSECURITY
25 THREATS.—A cyber threat indicator or de-

1 fensive measure shared as described in
2 clause (i) may, consistent with a State,
3 tribal, or local government regulatory au-
4 thority specifically relating to the preven-
5 tion or mitigation of cybersecurity threats
6 to information systems, inform the devel-
7 opment or implementation of a regulation
8 relating to such information systems.

9 (e) ANTITRUST EXEMPTION.—

10 (1) IN GENERAL.—Except as provided in sec-
11 tion 108(e), it shall not be considered a violation of
12 any provision of antitrust laws for 2 or more private
13 entities to exchange or provide a cyber threat indi-
14 cator or defensive measure, or assistance relating to
15 the prevention, investigation, or mitigation of a
16 cybersecurity threat, for cybersecurity purposes
17 under this title.

18 (2) APPLICABILITY.—Paragraph (1) shall apply
19 only to information that is exchanged or assistance
20 provided in order to assist with—

21 (A) facilitating the prevention, investiga-
22 tion, or mitigation of a cybersecurity threat to
23 an information system or information that is
24 stored on, processed by, or transiting an infor-
25 mation system; or

1 (B) communicating or disclosing a cyber
2 threat indicator to help prevent, investigate, or
3 mitigate the effect of a cybersecurity threat to
4 an information system or information that is
5 stored on, processed by, or transiting an infor-
6 mation system.

7 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber
8 threat indicator or defensive measure with a non-Federal
9 entity under this title shall not create a right or benefit
10 to similar information by such non-Federal entity or any
11 other non-Federal entity.

12 **SEC. 105. SHARING OF CYBER THREAT INDICATORS AND**
13 **DEFENSIVE MEASURES WITH THE FEDERAL**
14 **GOVERNMENT.**

15 (a) REQUIREMENT FOR POLICIES AND PROCE-
16 DURES.—

17 (1) INTERIM POLICIES AND PROCEDURES.—Not
18 later than 60 days after the date of the enactment
19 of this Act, the Attorney General and the Secretary
20 of Homeland Security shall, in consultation with the
21 heads of the appropriate Federal entities, jointly de-
22 velop and submit to Congress interim policies and
23 procedures relating to the receipt of cyber threat in-
24 dicators and defensive measures by the Federal Gov-
25 ernment.

1 (2) FINAL POLICIES AND PROCEDURES.—Not
2 later than 180 days after the date of the enactment
3 of this Act, the Attorney General and the Secretary
4 of Homeland Security shall, in consultation with the
5 heads of the appropriate Federal entities, jointly
6 issue and make publicly available final policies and
7 procedures relating to the receipt of cyber threat in-
8 dicators and defensive measures by the Federal Gov-
9 ernment.

10 (3) REQUIREMENTS CONCERNING POLICIES AND
11 PROCEDURES.—Consistent with the guidelines re-
12 quired by subsection (b), the policies and procedures
13 developed or issued under this subsection shall—

14 (A) ensure that cyber threat indicators
15 shared with the Federal Government by any
16 non-Federal entity pursuant to section 104(c)
17 through the real-time process described in sub-
18 section (c) of this section—

19 (i) are shared in an automated man-
20 ner with all of the appropriate Federal en-
21 tities;

22 (ii) are only subject to a delay, modi-
23 fication, or other action due to controls es-
24 tablished for such real-time process that
25 could impede real-time receipt by all of the

1 appropriate Federal entities when the
2 delay, modification, or other action is due
3 to controls—

4 (I) agreed upon unanimously by
5 all of the heads of the appropriate
6 Federal entities;

7 (II) carried out before any of the
8 appropriate Federal entities retains or
9 uses the cyber threat indicators or de-
10 fensive measures; and

11 (III) uniformly applied such that
12 each of the appropriate Federal enti-
13 ties is subject to the same delay,
14 modification, or other action; and

15 (iii) may be provided to other Federal
16 entities;

17 (B) ensure that cyber threat indicators
18 shared with the Federal Government by any
19 non-Federal entity pursuant to section 104 in a
20 manner other than the real-time process de-
21 scribed in subsection (c) of this section—

22 (i) are shared as quickly as operation-
23 ally practicable with all of the appropriate
24 Federal entities;

1 (ii) are not subject to any unnecessary
2 delay, interference, or any other action
3 that could impede receipt by all of the ap-
4 propriate Federal entities; and

5 (iii) may be provided to other Federal
6 entities; and

7 (C) ensure there are—

8 (i) audit capabilities; and

9 (ii) appropriate sanctions in place for
10 officers, employees, or agents of a Federal
11 entity who knowingly and willfully conduct
12 activities under this title in an unauthor-
13 ized manner.

14 (4) GUIDELINES FOR ENTITIES SHARING CYBER
15 THREAT INDICATORS WITH FEDERAL GOVERN-
16 MENT.—

17 (A) IN GENERAL.—Not later than 60 days
18 after the date of the enactment of this Act, the
19 Attorney General and the Secretary of Home-
20 land Security shall jointly develop and make
21 publicly available guidance to assist entities and
22 promote sharing of cyber threat indicators with
23 Federal entities under this title.

24 (B) CONTENTS.—The guidelines developed
25 and made publicly available under subpara-

1 graph (A) shall include guidance on the fol-
2 lowing:

3 (i) Identification of types of informa-
4 tion that would qualify as a cyber threat
5 indicator under this title that would be un-
6 likely to include information that—

7 (I) is not directly related to a
8 cybersecurity threat; and

9 (II) is personal information of a
10 specific individual or information that
11 identifies a specific individual.

12 (ii) Identification of types of informa-
13 tion protected under otherwise applicable
14 privacy laws that are unlikely to be directly
15 related to a cybersecurity threat.

16 (iii) Such other matters as the Attor-
17 ney General and the Secretary of Home-
18 land Security consider appropriate for enti-
19 ties sharing cyber threat indicators with
20 Federal entities under this title.

21 (b) PRIVACY AND CIVIL LIBERTIES.—

22 (1) INTERIM GUIDELINES.—Not later than 60
23 days after the date of the enactment of this Act, the
24 Attorney General and the Secretary of Homeland
25 Security shall, in consultation with heads of the ap-

1 appropriate Federal entities and in consultation with
2 officers designated under section 1062 of the Na-
3 tional Security Intelligence Reform Act of 2004 (42
4 U.S.C. 2000ee-1), jointly develop, submit to Con-
5 gress, and make available to the public interim
6 guidelines relating to privacy and civil liberties which
7 shall govern the receipt, retention, use, and dissemi-
8 nation of cyber threat indicators by a Federal entity
9 obtained in connection with activities authorized in
10 this title.

11 (2) FINAL GUIDELINES.—

12 (A) IN GENERAL.—Not later than 180
13 days after the date of the enactment of this
14 Act, the Attorney General and the Secretary of
15 Homeland Security shall, in coordination with
16 heads of the appropriate Federal entities and in
17 consultation with officers designated under sec-
18 tion 1062 of the National Security Intelligence
19 Reform Act of 2004 (42 U.S.C. 2000ee-1) and
20 such private entities with industry expertise as
21 the Attorney General and the Secretary con-
22 sider relevant, jointly issue and make publicly
23 available final guidelines relating to privacy and
24 civil liberties which shall govern the receipt, re-
25 tention, use, and dissemination of cyber threat

1 indicators by a Federal entity obtained in con-
2 nection with activities authorized in this title.

3 (B) PERIODIC REVIEW.—The Attorney
4 General and the Secretary of Homeland Secu-
5 rity shall, in coordination with heads of the ap-
6 propriate Federal entities and in consultation
7 with officers and private entities described in
8 subparagraph (A), periodically, but not less fre-
9 quently than once every 2 years, jointly review
10 the guidelines issued under subparagraph (A).

11 (3) CONTENT.—The guidelines required by
12 paragraphs (1) and (2) shall, consistent with the
13 need to protect information systems from
14 cybersecurity threats and mitigate cybersecurity
15 threats—

16 (A) limit the effect on privacy and civil lib-
17 erties of activities by the Federal Government
18 under this title;

19 (B) limit the receipt, retention, use, and
20 dissemination of cyber threat indicators con-
21 taining personal information of specific individ-
22 uals or information that identifies specific indi-
23 viduals, including by establishing—

24 (i) a process for the timely destruction
25 of such information that is known not to

1 be directly related to uses authorized under
2 this title; and

3 (ii) specific limitations on the length
4 of any period in which a cyber threat indi-
5 cator may be retained;

6 (C) include requirements to safeguard
7 cyber threat indicators containing personal in-
8 formation of specific individuals or information
9 that identifies specific individuals from unau-
10 thorized access or acquisition, including appro-
11 priate sanctions for activities by officers, em-
12 ployees, or agents of the Federal Government in
13 contravention of such guidelines;

14 (D) consistent with this title, any other ap-
15 plicable provisions of law, and the fair informa-
16 tion practice principles set forth in appendix A
17 of the document entitled “National Strategy for
18 Trusted Identities in Cyberspace” and pub-
19 lished by the President in April 2011, govern
20 the retention, use, and dissemination by the
21 Federal Government of cyber threat indicators
22 shared with the Federal Government under this
23 title, including the extent, if any, to which such
24 cyber threat indicators may be used by the Fed-
25 eral Government;

1 (E) include procedures for notifying enti-
2 ties and Federal entities if information received
3 pursuant to this section is known or determined
4 by a Federal entity receiving such information
5 not to constitute a cyber threat indicator;

6 (F) protect the confidentiality of cyber
7 threat indicators containing personal informa-
8 tion of specific individuals or information that
9 identifies specific individuals to the greatest ex-
10 tent practicable and require recipients to be in-
11 formed that such indicators may only be used
12 for purposes authorized under this title; and

13 (G) include steps that may be needed so
14 that dissemination of cyber threat indicators is
15 consistent with the protection of classified and
16 other sensitive national security information.

17 (c) CAPABILITY AND PROCESS WITHIN THE DEPART-
18 MENT OF HOMELAND SECURITY.—

19 (1) IN GENERAL.—Not later than 90 days after
20 the date of the enactment of this Act, the Secretary
21 of Homeland Security, in coordination with the
22 heads of the appropriate Federal entities, shall de-
23 velop and implement a capability and process within
24 the Department of Homeland Security that—

1 (A) shall accept from any non-Federal en-
2 tity in real time cyber threat indicators and de-
3 fensive measures, pursuant to this section;

4 (B) shall, upon submittal of the certifi-
5 cation under paragraph (2) that such capability
6 and process fully and effectively operates as de-
7 scribed in such paragraph, be the process by
8 which the Federal Government receives cyber
9 threat indicators and defensive measures under
10 this title that are shared by a non-Federal enti-
11 ty with the Federal Government through elec-
12 tronic mail or media, an interactive form on an
13 Internet website, or a real time, automated
14 process between information systems except—

15 (i) consistent with section 104, com-
16 munications between a Federal entity and
17 a non-Federal entity regarding a previously
18 shared cyber threat indicator to describe
19 the relevant cybersecurity threat or develop
20 a defensive measure based on such cyber
21 threat indicator; and

22 (ii) communications by a regulated
23 non-Federal entity with such entity's Fed-
24 eral regulatory authority regarding a
25 cybersecurity threat;

1 (C) ensures that all of the appropriate
2 Federal entities receive in an automated man-
3 ner such cyber threat indicators and defensive
4 measures shared through the real-time process
5 within the Department of Homeland Security;

6 (D) is in compliance with the policies, pro-
7 cedures, and guidelines required by this section;
8 and

9 (E) does not limit or prohibit otherwise
10 lawful disclosures of communications, records,
11 or other information, including—

12 (i) reporting of known or suspected
13 criminal activity, by a non-Federal entity
14 to any other non-Federal entity or a Fed-
15 eral entity, including cyber threat indica-
16 tors or defensive measures shared with a
17 Federal entity in furtherance of opening a
18 Federal law enforcement investigation;

19 (ii) voluntary or legally compelled par-
20 ticipation in a Federal investigation; and

21 (iii) providing cyber threat indicators
22 or defensive measures as part of a statu-
23 tory or authorized contractual requirement.

24 (2) CERTIFICATION AND DESIGNATION.—

1 (A) CERTIFICATION OF CAPABILITY AND
2 PROCESS.—Not later than 90 days after the
3 date of the enactment of this Act, the Secretary
4 of Homeland Security shall, in consultation
5 with the heads of the appropriate Federal enti-
6 ties, submit to Congress a certification as to
7 whether the capability and process required by
8 paragraph (1) fully and effectively operates—

9 (i) as the process by which the Fed-
10 eral Government receives from any non-
11 Federal entity a cyber threat indicator or
12 defensive measure under this title; and

13 (ii) in accordance with the interim
14 policies, procedures, and guidelines devel-
15 oped under this title.

16 (B) DESIGNATION.—

17 (i) IN GENERAL.—At any time after
18 certification is submitted under subpara-
19 graph (A), the President may designate an
20 appropriate Federal entity, other than the
21 Department of Defense (including the Na-
22 tional Security Agency), to develop and im-
23 plement a capability and process as de-
24 scribed in paragraph (1) in addition to the
25 capability and process developed under

1 such paragraph by the Secretary of Home-
2 land Security, if, not fewer than 30 days
3 before making such designation, the Presi-
4 dent submits to Congress a certification
5 and explanation that—

6 (I) such designation is necessary
7 to ensure that full, effective, and se-
8 cure operation of a capability and
9 process for the Federal Government
10 to receive from any non-Federal entity
11 cyber threat indicators or defensive
12 measures under this title;

13 (II) the designated appropriate
14 Federal entity will receive and share
15 cyber threat indicators and defensive
16 measures in accordance with the poli-
17 cies, procedures, and guidelines devel-
18 oped under this title, including sub-
19 section (a)(3)(A); and

20 (III) such designation is con-
21 sistent with the mission of such ap-
22 propriate Federal entity and improves
23 the ability of the Federal Government
24 to receive, share, and use cyber threat

1 indicators and defensive measures as
2 authorized under this title.

3 (ii) APPLICATION TO ADDITIONAL CA-
4 PABILITY AND PROCESS.—If the President
5 designates an appropriate Federal entity to
6 develop and implement a capability and
7 process under clause (i), the provisions of
8 this title that apply to the capability and
9 process required by paragraph (1) shall
10 also be construed to apply to the capability
11 and process developed and implemented
12 under clause (i).

13 (3) PUBLIC NOTICE AND ACCESS.—The Sec-
14 retary of Homeland Security shall ensure there is
15 public notice of, and access to, the capability and
16 process developed and implemented under paragraph
17 (1) so that—

18 (A) any non-Federal entity may share
19 cyber threat indicators and defensive measures
20 through such process with the Federal Govern-
21 ment; and

22 (B) all of the appropriate Federal entities
23 receive such cyber threat indicators and defen-
24 sive measures in real time with receipt through
25 the process within the Department of Home-

1 land Security consistent with the policies and
2 procedures issued under subsection (a).

3 (4) OTHER FEDERAL ENTITIES.—The process
4 developed and implemented under paragraph (1)
5 shall ensure that other Federal entities receive in a
6 timely manner any cyber threat indicators and de-
7 fensive measures shared with the Federal Govern-
8 ment through such process.

9 (d) INFORMATION SHARED WITH OR PROVIDED TO
10 THE FEDERAL GOVERNMENT.—

11 (1) NO WAIVER OF PRIVILEGE OR PROTEC-
12 TION.—The provision of cyber threat indicators and
13 defensive measures to the Federal Government
14 under this title shall not constitute a waiver of any
15 applicable privilege or protection provided by law, in-
16 cluding trade secret protection.

17 (2) PROPRIETARY INFORMATION.—Consistent
18 with section 104(c)(2) and any other applicable pro-
19 vision of law, a cyber threat indicator or defensive
20 measure provided by a non-Federal entity to the
21 Federal Government under this title shall be consid-
22 ered the commercial, financial, and proprietary in-
23 formation of such non-Federal entity when so des-
24 ignated by the originating non-Federal entity or a

1 third party acting in accordance with the written au-
2 thorization of the originating non-Federal entity.

3 (3) EXEMPTION FROM DISCLOSURE.—A cyber
4 threat indicator or defensive measure shared with
5 the Federal Government under this title shall be—

6 (A) deemed voluntarily shared information
7 and exempt from disclosure under section 552
8 of title 5, United States Code, and any State,
9 tribal, or local provision of law requiring disclo-
10 sure of information or records; and

11 (B) withheld, without discretion, from the
12 public under section 552(b)(3)(B) of title 5,
13 United States Code, and any State, tribal, or
14 local provision of law requiring disclosure of in-
15 formation or records.

16 (4) EX PARTE COMMUNICATIONS.—The provi-
17 sion of a cyber threat indicator or defensive measure
18 to the Federal Government under this title shall not
19 be subject to a rule of any Federal agency or depart-
20 ment or any judicial doctrine regarding ex parte
21 communications with a decision-making official.

22 (5) DISCLOSURE, RETENTION, AND USE.—

23 (A) AUTHORIZED ACTIVITIES.—Cyber
24 threat indicators and defensive measures pro-
25 vided to the Federal Government under this

1 title may be disclosed to, retained by, and used
2 by, consistent with otherwise applicable provi-
3 sions of Federal law, any Federal agency or de-
4 partment, component, officer, employee, or
5 agent of the Federal Government solely for—

- 6 (i) a cybersecurity purpose;
- 7 (ii) the purpose of identifying—
- 8 (I) a cybersecurity threat, includ-
9 ing the source of such cybersecurity
10 threat; or
- 11 (II) a security vulnerability;
- 12 (iii) the purpose of responding to, or
13 otherwise preventing or mitigating, a spe-
14 cific threat of death, a specific threat of se-
15 rious bodily harm, or a specific threat of
16 serious economic harm, including a ter-
17 rorist act or a use of a weapon of mass de-
18 struction;
- 19 (iv) the purpose of responding to, in-
20 vestigating, prosecuting, or otherwise pre-
21 venting or mitigating, a serious threat to a
22 minor, including sexual exploitation and
23 threats to physical safety; or
- 24 (v) the purpose of preventing, inves-
25 tigating, disrupting, or prosecuting an of-

1 fense arising out of a threat described in
2 clause (iii) or any of the offenses listed
3 in—

4 (I) sections 1028 through 1030
5 of title 18, United States Code (relat-
6 ing to fraud and identity theft);

7 (II) chapter 37 of such title (re-
8 lating to espionage and censorship);
9 and

10 (III) chapter 90 of such title (re-
11 lating to protection of trade secrets).

12 (B) PROHIBITED ACTIVITIES.—Cyber
13 threat indicators and defensive measures pro-
14 vided to the Federal Government under this
15 title shall not be disclosed to, retained by, or
16 used by any Federal agency or department for
17 any use not permitted under subparagraph (A).

18 (C) PRIVACY AND CIVIL LIBERTIES.—
19 Cyber threat indicators and defensive measures
20 provided to the Federal Government under this
21 title shall be retained, used, and disseminated
22 by the Federal Government—

23 (i) in accordance with the policies,
24 procedures, and guidelines required by sub-
25 sections (a) and (b);

1 (ii) in a manner that protects from
2 unauthorized use or disclosure any cyber
3 threat indicators that may contain—

4 (I) personal information of a spe-
5 cific individual; or

6 (II) information that identifies a
7 specific individual; and

8 (iii) in a manner that protects the
9 confidentiality of cyber threat indicators
10 containing—

11 (I) personal information of a spe-
12 cific individual; or

13 (II) information that identifies a
14 specific individual.

15 (D) FEDERAL REGULATORY AUTHORITY.—

16 (i) IN GENERAL.—Except as provided
17 in clause (ii), cyber threat indicators and
18 defensive measures provided to the Federal
19 Government under this title shall not be
20 used by any Federal, State, tribal, or local
21 government to regulate, including an en-
22 forcement action, the lawful activities of
23 any non-Federal entity or any activities
24 taken by a non-Federal entity pursuant to
25 mandatory standards, including activities

1 relating to monitoring, operating defensive
2 measures, or sharing cyber threat indica-
3 tors.

4 (ii) EXCEPTIONS.—

5 (I) REGULATORY AUTHORITY
6 SPECIFICALLY RELATING TO PREVEN-
7 TION OR MITIGATION OF
8 CYBERSECURITY THREATS.—Cyber
9 threat indicators and defensive meas-
10 ures provided to the Federal Govern-
11 ment under this title may, consistent
12 with Federal or State regulatory au-
13 thority specifically relating to the pre-
14 vention or mitigation of cybersecurity
15 threats to information systems, inform
16 the development or implementation of
17 regulations relating to such informa-
18 tion systems.

19 (II) PROCEDURES DEVELOPED
20 AND IMPLEMENTED UNDER THIS
21 TITLE.—Clause (i) shall not apply to
22 procedures developed and imple-
23 mented under this title.

1 **SEC. 106. PROTECTION FROM LIABILITY.**

2 (a) MONITORING OF INFORMATION SYSTEMS.—No
3 cause of action shall lie or be maintained in any court
4 against any private entity, and such action shall be
5 promptly dismissed, for the monitoring of an information
6 system and information under section 104(a) that is con-
7 ducted in accordance with this title.

8 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
9 CATORS.—No cause of action shall lie or be maintained
10 in any court against any private entity, and such action
11 shall be promptly dismissed, for the sharing or receipt of
12 a cyber threat indicator or defensive measure under sec-
13 tion 104(c) if—

14 (1) such sharing or receipt is conducted in ac-
15 cordance with this title; and

16 (2) in a case in which a cyber threat indicator
17 or defensive measure is shared with the Federal
18 Government, the cyber threat indicator or defensive
19 measure is shared in a manner that is consistent
20 with section 105(c)(1)(B) and the sharing or receipt,
21 as the case may be, occurs after the earlier of—

22 (A) the date on which the interim policies
23 and procedures are submitted to Congress
24 under section 105(a)(1) and guidelines are sub-
25 mitted to Congress under section 105(b)(1); or

1 (B) the date that is 60 days after the date
2 of the enactment of this Act.

3 (c) CONSTRUCTION.—Nothing in this title shall be
4 construed—

5 (1) to create—

6 (A) a duty to share a cyber threat indi-
7 cator or defensive measure; or

8 (B) a duty to warn or act based on the re-
9 ceipt of a cyber threat indicator or defensive
10 measure; or

11 (2) to undermine or limit the availability of oth-
12 erwise applicable common law or statutory defenses.

13 **SEC. 107. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

14 (a) REPORT ON IMPLEMENTATION.—

15 (1) IN GENERAL.—Not later than 1 year after
16 the date of the enactment of this title, the heads of
17 the appropriate Federal entities shall jointly submit
18 to Congress a detailed report concerning the imple-
19 mentation of this title.

20 (2) CONTENTS.—The report required by para-
21 graph (1) may include such recommendations as the
22 heads of the appropriate Federal entities may have
23 for improvements or modifications to the authorities,
24 policies, procedures, and guidelines under this title
25 and shall include the following:

1 (A) An evaluation of the effectiveness of
2 real-time information sharing through the capa-
3 bility and process developed under section
4 105(c), including any impediments to such real-
5 time sharing.

6 (B) An assessment of whether cyber threat
7 indicators or defensive measures have been
8 properly classified and an accounting of the
9 number of security clearances authorized by the
10 Federal Government for the purpose of sharing
11 cyber threat indicators or defensive measures
12 with the private sector.

13 (C) The number of cyber threat indicators
14 or defensive measures received through the ca-
15 pability and process developed under section
16 105(c).

17 (D) A list of Federal entities that have re-
18 ceived cyber threat indicators or defensive
19 measures under this title.

20 (b) BIENNIAL REPORT ON COMPLIANCE.—

21 (1) IN GENERAL.—Not later than 2 years after
22 the date of the enactment of this Act and not less
23 frequently than once every 2 years thereafter, the in-
24 spectors general of the appropriate Federal entities,
25 in consultation with the Inspector General of the In-

1 intelligence Community and the Council of Inspectors
2 General on Financial Oversight, shall jointly submit
3 to Congress an interagency report on the actions of
4 the executive branch of the Federal Government to
5 carry out this title during the most recent 2-year pe-
6 riod.

7 (2) CONTENTS.—Each report submitted under
8 paragraph (1) shall include, for the period covered
9 by the report, the following:

10 (A) An assessment of the sufficiency of the
11 policies, procedures, and guidelines relating to
12 the sharing of cyber threat indicators within the
13 Federal Government, including those policies,
14 procedures, and guidelines relating to the re-
15 moval of information not directly related to a
16 cybersecurity threat that is personal informa-
17 tion of a specific individual or information that
18 identifies a specific individual.

19 (B) An assessment of whether cyber threat
20 indicators or defensive measures have been
21 properly classified and an accounting of the
22 number of security clearances authorized by the
23 Federal Government for the purpose of sharing
24 cyber threat indicators or defensive measures
25 with the private sector.

1 (C) A review of the actions taken by the
2 Federal Government based on cyber threat indi-
3 cators or defensive measures shared with the
4 Federal Government under this title, including
5 a review of the following:

6 (i) The appropriateness of subsequent
7 uses and disseminations of cyber threat in-
8 dicators or defensive measures.

9 (ii) Whether cyber threat indicators or
10 defensive measures were shared in a timely
11 and adequate manner with appropriate en-
12 tities, or, if appropriate, were made pub-
13 licly available.

14 (D) An assessment of the cyber threat in-
15 dicators or defensive measures shared with the
16 appropriate Federal entities under this title, in-
17 cluding the following:

18 (i) The number of cyber threat indica-
19 tors or defensive measures shared through
20 the capability and process developed under
21 section 105(c).

22 (ii) An assessment of any information
23 not directly related to a cybersecurity
24 threat that is personal information of a
25 specific individual or information identi-

1 fying a specific individual and was shared
2 by a non-Federal government entity with
3 the Federal government in contravention of
4 this title, or was shared within the Federal
5 Government in contravention of the guide-
6 lines required by this title, including a de-
7 scription of any significant violation of this
8 title.

9 (iii) The number of times, according
10 to the Attorney General, that information
11 shared under this title was used by a Fed-
12 eral entity to prosecute an offense listed in
13 section 105(d)(5)(A).

14 (iv) A quantitative and qualitative as-
15 sessment of the effect of the sharing of
16 cyber threat indicators or defensive meas-
17 ures with the Federal Government on pri-
18 vacy and civil liberties of specific individ-
19 uals, including the number of notices that
20 were issued with respect to a failure to re-
21 move information not directly related to a
22 cybersecurity threat that was personal in-
23 formation of a specific individual or infor-
24 mation that identified a specific individual

1 in accordance with the procedures required
2 by section 105(b)(3)(E).

3 (v) The adequacy of any steps taken
4 by the Federal Government to reduce any
5 adverse effect from activities carried out
6 under this title on the privacy and civil lib-
7 erties of United States persons.

8 (E) An assessment of the sharing of cyber
9 threat indicators or defensive measures among
10 Federal entities to identify inappropriate bar-
11 riers to sharing information.

12 (3) RECOMMENDATIONS.—Each report sub-
13 mitted under this subsection may include such rec-
14 ommendations as the inspectors general may have
15 for improvements or modifications to the authorities
16 and processes under this title.

17 (c) INDEPENDENT REPORT ON REMOVAL OF PER-
18 SONAL INFORMATION.—Not later than 3 years after the
19 date of the enactment of this Act, the Comptroller General
20 of the United States shall submit to Congress a report
21 on the actions taken by the Federal Government to remove
22 personal information from cyber threat indicators or de-
23 fensive measures pursuant to this title. Such report shall
24 include an assessment of the sufficiency of the policies,

1 procedures, and guidelines established under this title in
2 addressing concerns relating to privacy and civil liberties.

3 (d) FORM OF REPORTS.—Each report required under
4 this section shall be submitted in an unclassified form, but
5 may include a classified annex.

6 (e) PUBLIC AVAILABILITY OF REPORTS.—The un-
7 classified portions of the reports required under this sec-
8 tion shall be made available to the public.

9 **SEC. 108. CONSTRUCTION AND PREEMPTION.**

10 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in
11 this title shall be construed—

12 (1) to limit or prohibit otherwise lawful dislo-
13 sures of communications, records, or other informa-
14 tion, including reporting of known or suspected
15 criminal activity, by a non-Federal entity to any
16 other non-Federal entity or the Federal Government
17 under this title; or

18 (2) to limit or prohibit otherwise lawful use of
19 such disclosures by any Federal entity, even when
20 such otherwise lawful disclosures duplicate or rep-
21 licate disclosures made under this title.

22 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in
23 this title shall be construed to prohibit or limit the dislo-
24 sure of information protected under section 2302(b)(8) of
25 title 5, United States Code (governing disclosures of ille-

1 gality, waste, fraud, abuse, or public health or safety
2 threats), section 7211 of title 5, United States Code (gov-
3 erning disclosures to Congress), section 1034 of title 10,
4 United States Code (governing disclosure to Congress by
5 members of the military), section 1104 of the National
6 Security Act of 1947 (50 U.S.C. 3234) (governing disclo-
7 sure by employees of elements of the intelligence commu-
8 nity), or any similar provision of Federal or State law.

9 (c) PROTECTION OF SOURCES AND METHODS.—

10 Nothing in this title shall be construed—

11 (1) as creating any immunity against, or other-
12 wise affecting, any action brought by the Federal
13 Government, or any agency or department thereof,
14 to enforce any law, executive order, or procedure
15 governing the appropriate handling, disclosure, or
16 use of classified information;

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

19 (3) to modify the authority of a department or
20 agency of the Federal Government to protect classi-
21 fied information and sources and methods and the
22 national security of the United States.

23 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in
24 this title shall be construed to affect any requirement

1 under any other provision of law for a non-Federal entity
2 to provide information to the Federal Government.

3 (e) PROHIBITED CONDUCT.—Nothing in this title
4 shall be construed to permit price-fixing, allocating a mar-
5 ket between competitors, monopolizing or attempting to
6 monopolize a market, boycotting, or exchanges of price or
7 cost information, customer lists, or information regarding
8 future competitive planning.

9 (f) INFORMATION SHARING RELATIONSHIPS.—Noth-
10 ing in this title shall be construed—

11 (1) to limit or modify an existing information
12 sharing relationship;

13 (2) to prohibit a new information sharing rela-
14 tionship;

15 (3) to require a new information sharing rela-
16 tionship between any non-Federal entity and a Fed-
17 eral entity or another non-Federal entity; or

18 (4) to require the use of the capability and
19 process within the Department of Homeland Secu-
20 rity developed under section 105(c).

21 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS
22 AND RIGHTS.—Nothing in this title shall be construed—

23 (1) to amend, repeal, or supersede any current
24 or future contractual agreement, terms of service
25 agreement, or other contractual relationship between

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

3 (2) to abrogate trade secret or intellectual prop-
4 erty rights of any non-Federal entity or Federal en-
5 tity.

6 (h) ANTI-TASKING RESTRICTION.—Nothing in this
7 title shall be construed to permit a Federal entity—

8 (1) to require a non-Federal entity to provide
9 information to a Federal entity or another non-Fed-
10 eral entity;

11 (2) to condition the sharing of cyber threat in-
12 dicators with a non-Federal entity on such entity's
13 provision of cyber threat indicators to a Federal en-
14 tity or another non-Federal entity; or

15 (3) to condition the award of any Federal
16 grant, contract, or purchase on the provision of a
17 cyber threat indicator to a Federal entity or another
18 non-Federal entity.

19 (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-
20 ing in this title shall be construed to subject any entity
21 to liability for choosing not to engage in the voluntary ac-
22 tivities authorized in this title.

23 (j) USE AND RETENTION OF INFORMATION.—Noth-
24 ing in this title shall be construed to authorize, or to mod-
25 ify any existing authority of, a department or agency of

1 the Federal Government to retain or use any information
2 shared under this title for any use other than permitted
3 in this title.

4 (k) FEDERAL PREEMPTION.—

5 (1) IN GENERAL.—This title supersedes any
6 statute or other provision of law of a State or polit-
7 ical subdivision of a State that restricts or otherwise
8 expressly regulates an activity authorized under this
9 title.

10 (2) STATE LAW ENFORCEMENT.—Nothing in
11 this title shall be construed to supersede any statute
12 or other provision of law of a State or political sub-
13 division of a State concerning the use of authorized
14 law enforcement practices and procedures.

15 (l) REGULATORY AUTHORITY.—Nothing in this title
16 shall be construed—

17 (1) to authorize the promulgation of any regu-
18 lations not specifically authorized to be issued under
19 this title;

20 (2) to establish or limit any regulatory author-
21 ity not specifically established or limited under this
22 title; or

23 (3) to authorize regulatory actions that would
24 duplicate or conflict with regulatory requirements,

1 mandatory standards, or related processes under an-
2 other provision of Federal law.

3 (m) **AUTHORITY OF SECRETARY OF DEFENSE TO**
4 **RESPOND TO MALICIOUS CYBER ACTIVITY CARRIED OUT**
5 **BY FOREIGN POWERS.**—Nothing in this title shall be con-
6 strued to limit the authority of the Secretary of Defense
7 under section 130g of title 10, United States Code.

8 (n) **CRIMINAL PROSECUTION.**—Nothing in this title
9 shall be construed to prevent the disclosure of a cyber
10 threat indicator or defensive measure shared under this
11 title in a case of criminal prosecution, when an applicable
12 provision of Federal, State, tribal, or local law requires
13 disclosure in such case.

14 **SEC. 109. REPORT ON CYBERSECURITY THREATS.**

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

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

1 (1) An assessment of the current intelligence
2 sharing and cooperation relationships of the United
3 States with other countries regarding cybersecurity
4 threats, including cyber attacks, theft, and data
5 breaches, directed against the United States and
6 which threaten the United States national security
7 interests and economy and intellectual property, spe-
8 cifically identifying the relative utility of such rela-
9 tionships, which elements of the intelligence commu-
10 nity participate in such relationships, and whether
11 and how such relationships could be improved.

12 (2) A list and an assessment of the countries
13 and nonstate actors that are the primary threats of
14 carrying out a cybersecurity threat, including a
15 cyber attack, theft, or data breach, against the
16 United States and which threaten the United States
17 national security, economy, and intellectual property.

18 (3) A description of the extent to which the ca-
19 pabilities of the United States Government to re-
20 spond to or prevent cybersecurity threats, including
21 cyber attacks, theft, or data breaches, directed
22 against the United States private sector are de-
23 graded by a delay in the prompt notification by pri-
24 vate entities of such threats or cyber attacks, theft,
25 and data breaches.

1 (4) An assessment of additional technologies or
2 capabilities that would enhance the ability of the
3 United States to prevent and to respond to
4 cybersecurity threats, including cyber attacks, theft,
5 and data breaches.

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

10 (c) FORM OF REPORT.—The report required by sub-
11 section (a) shall be made available in classified and unclas-
12 sified forms.

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

17 **SEC. 110. EXCEPTION TO LIMITATION ON AUTHORITY OF**
18 **SECRETARY OF DEFENSE TO DISSEMINATE**
19 **CERTAIN INFORMATION.**

20 Notwithstanding subsection (c)(3) of section 393 of
21 title 10, United States Code, the Secretary of Defense may
22 authorize the sharing of cyber threat indicators and defen-
23 sive measures pursuant to the policies, procedures, and
24 guidelines developed or issued under this title.

1 **SEC. 111. EFFECTIVE PERIOD.**

2 (a) IN GENERAL.—Except as provided in subsection
3 (b), this title and the amendments made by this title shall
4 be effective during the period beginning on the date of
5 the enactment of this Act and ending on September 30,
6 2025.

7 (b) EXCEPTION.—With respect to any action author-
8 ized by this title or information obtained pursuant to an
9 action authorized by this title, which occurred before the
10 date on which the provisions referred to in subsection (a)
11 cease to have effect, the provisions of this title shall con-
12 tinue in effect.

13 **TITLE II—NATIONAL**
14 **CYBERSECURITY ADVANCE-**
15 **MENT**

16 **Subtitle A—National Cybersecurity**
17 **and Communications Integra-**
18 **tion Center**

19 **SEC. 201. SHORT TITLE.**

20 This subtitle may be cited as the “National
21 Cybersecurity Protection Advancement Act of 2015”.

22 **SEC. 202. DEFINITIONS.**

23 In this subtitle:

24 (1) APPROPRIATE CONGRESSIONAL COMMIT-
25 TEES.—The term “appropriate congressional com-
26 mittees” means—

1 (A) the Committee on Homeland Security
2 and Governmental Affairs of the Senate; and

3 (B) the Committee on Homeland Security
4 of the House of Representatives.

5 (2) CYBERSECURITY RISK; INCIDENT.—The
6 terms “cybersecurity risk” and “incident” have the
7 meanings given those terms in section 227 of the
8 Homeland Security Act of 2002, as so redesignated
9 by section 223(a)(3) of this division.

10 (3) CYBER THREAT INDICATOR; DEFENSIVE
11 MEASURE.—The terms “cyber threat indicator” and
12 “defensive measure” have the meanings given those
13 terms in section 102.

14 (4) DEPARTMENT.—The term “Department”
15 means the Department of Homeland Security.

16 (5) SECRETARY.—The term “Secretary” means
17 the Secretary of Homeland Security.

18 **SEC. 203. INFORMATION SHARING STRUCTURE AND PROC-**
19 **ESSES.**

20 Section 227 of the Homeland Security Act of 2002,
21 as so redesignated by section 223(a)(3) of this division,
22 is amended—

23 (1) in subsection (a)—

24 (A) by redesignating paragraphs (3) and

25 (4) as paragraphs (4) and (5), respectively;

1 (B) by striking paragraphs (1) and (2) and
2 inserting the following:

3 “(1) the term ‘cybersecurity risk’—

4 “(A) means threats to and vulnerabilities
5 of information or information systems and any
6 related consequences caused by or resulting
7 from unauthorized access, use, disclosure, deg-
8 radation, disruption, modification, or destruc-
9 tion of such information or information sys-
10 tems, including such related consequences
11 caused by an act of terrorism; and

12 “(B) does not include any action that sole-
13 ly involves a violation of a consumer term of
14 service or a consumer licensing agreement;

15 “(2) the terms ‘cyber threat indicator’ and ‘de-
16 fensive measure’ have the meanings given those
17 terms in section 102 of the Cybersecurity Act of
18 2015;

19 “(3) the term ‘incident’ means an occurrence
20 that actually or imminently jeopardizes, without law-
21 ful authority, the integrity, confidentiality, or avail-
22 ability of information on an information system, or
23 actually or imminently jeopardizes, without lawful
24 authority, an information system;”;

1 (C) in paragraph (4), as so redesignated,
2 by striking “and” at the end;

3 (D) in paragraph (5), as so redesignated,
4 by striking the period at the end and inserting
5 “; and”; and

6 (E) by adding at the end the following:

7 “(6) the term ‘sharing’ (including all conjuga-
8 tions thereof) means providing, receiving, and dis-
9 seminating (including all conjugations of each of
10 such terms).”;

11 (2) in subsection (c)—

12 (A) in paragraph (1)—

13 (i) by inserting “, including the imple-
14 mentation of title I of the Cybersecurity
15 Act of 2015” before the semicolon at the
16 end; and

17 (ii) by inserting “cyber threat indica-
18 tors, defensive measures,” before
19 “cybersecurity risks”;

20 (B) in paragraph (3), by striking
21 “cybersecurity risks” and inserting “cyber
22 threat indicators, defensive measures,
23 cybersecurity risks,”;

24 (C) in paragraph (5)(A), by striking
25 “cybersecurity risks” and inserting “cyber

1 threat indicators, defensive measures,
2 cybersecurity 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:

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

19 (F) by adding at the end the following:

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

22 “(A) collaborate on cyber threat indicators,
23 defensive measures, and information related to
24 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
5 cybersecurity risks and incidents with Federal and
6 non-Federal entities, including across sectors of crit-
7 ical infrastructure and with State and major urban
8 area fusion centers, as appropriate;

9 “(10) participating, as appropriate, in national
10 exercises run by the Department; and

11 “(11) in coordination with the Office of Emer-
12 gency Communications of the Department, assessing
13 and evaluating consequence, vulnerability, and threat
14 information regarding cyber incidents to public safe-
15 ty communications to help facilitate continuous im-
16 provements to the security and resiliency of such
17 communications.”;

18 (3) in subsection (d)(1)—

19 (A) in subparagraph (B)—

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

22 (ii) in clause (ii), by striking “; and”
23 and inserting “, including information
24 sharing and analysis centers.”;

1 (iii) in clause (iii), by adding “and” at
2 the end; and

3 (iv) by adding at the end the fol-
4 lowing:

5 “(iv) private entities;”.

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

8 (C) by redesignating subparagraph (E) as
9 subparagraph (F); and

10 (D) by inserting after subparagraph (D)
11 the following:

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

17 (4) in subsection (e)—

18 (A) in paragraph (1)—

19 (i) in subparagraph (A), by inserting
20 “cyber threat indicators, defensive meas-
21 ures, and” before “information”;

22 (ii) in subparagraph (B), by inserting
23 “cyber threat indicators, defensive meas-
24 ures, and” before “information related”;

25 (iii) in subparagraph (F)—

1 (I) by striking “cybersecurity
2 risks” and inserting “cyber threat in-
3 dicators, defensive measures,
4 cybersecurity risks,”; and

5 (II) by striking “and” at the end;

6 (iv) in subparagraph (G), by striking
7 “cybersecurity risks and incidents” and in-
8 serting “cyber threat indicators, defensive
9 measures, cybersecurity risks, and inci-
10 dents; and”;

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

12 “(H) the Center designates an agency con-
13 tact for non-Federal entities;”;

14 (B) in paragraph (2)—

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

19 (ii) by inserting “or disclosure” after
20 “access”; and

21 (C) in paragraph (3), by inserting before
22 the period at the end the following: “, including
23 by working with the Privacy Officer appointed
24 under section 222 to ensure that the Center fol-
25 lows the policies and procedures specified in

1 subsections (b) and (d)(5)(C) of section 105 of
2 the Cybersecurity Act of 2015”; and

3 (5) by adding at the end the following:

4 “(g) AUTOMATED INFORMATION SHARING.—

5 “(1) IN GENERAL.—The Under Secretary ap-
6 pointed under section 103(a)(1)(H), in coordination
7 with industry and other stakeholders, shall develop
8 capabilities making use of existing information tech-
9 nology industry standards and best practices, as ap-
10 propriate, that support and rapidly advance the de-
11 velopment, adoption, and implementation of auto-
12 mated mechanisms for the sharing of cyber threat
13 indicators and defensive measures in accordance
14 with title I of the Cybersecurity Act of 2015.

15 “(2) ANNUAL REPORT.—The Under Secretary
16 appointed under section 103(a)(1)(H) shall submit
17 to the Committee on Homeland Security and Gov-
18 ernmental Affairs of the Senate and the Committee
19 on Homeland Security of the House of Representa-
20 tives an annual report on the status and progress of
21 the development of the capabilities described in
22 paragraph (1). Such reports shall be required until
23 such capabilities are fully implemented.

24 “(h) VOLUNTARY INFORMATION SHARING PROCE-
25 DURES.—

1 “(1) PROCEDURES.—

2 “(A) IN GENERAL.—The Center may enter
3 into a voluntary information sharing relation-
4 ship with any consenting non-Federal entity for
5 the sharing of cyber threat indicators and de-
6 fensive measures for cybersecurity purposes in
7 accordance with this section. Nothing in this
8 subsection may be construed to require any
9 non-Federal entity to enter into any such infor-
10 mation sharing relationship with the Center or
11 any other entity. The Center may terminate a
12 voluntary information sharing relationship
13 under this subsection, at the sole and
14 unreviewable discretion of the Secretary, acting
15 through the Under Secretary appointed under
16 section 103(a)(1)(H), for any reason, including
17 if the Center determines that the non-Federal
18 entity with which the Center has entered into
19 such a relationship has violated the terms of
20 this subsection.

21 “(B) NATIONAL SECURITY.—The Sec-
22 retary may decline to enter into a voluntary in-
23 formation sharing relationship under this sub-
24 section, at the sole and unreviewable discretion
25 of the Secretary, acting through the Under Sec-

1 retary appointed under section 103(a)(1)(H),
2 for any reason, including if the Secretary deter-
3 mines that such is appropriate for national se-
4 curity.

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

9 “(A) STANDARD AGREEMENT.—For the
10 use of a non-Federal entity, the Center shall
11 make available a standard agreement, con-
12 sistent with this section, on the Department’s
13 website.

14 “(B) NEGOTIATED AGREEMENT.—At the
15 request of a non-Federal entity, and if deter-
16 mined appropriate by the Center, at the sole
17 and unreviewable discretion of the Secretary,
18 acting through the Under Secretary appointed
19 under section 103(a)(1)(H), the Department
20 shall negotiate a non-standard agreement, con-
21 sistent with this section.

22 “(C) EXISTING AGREEMENTS.—An agree-
23 ment between the Center and a non-Federal en-
24 tity that is entered into before the date of en-
25 actment of this subsection, or such an agree-

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

14 “(i) DIRECT REPORTING.—The Secretary shall de-
15 velop policies and procedures for direct reporting to the
16 Secretary by the Director of the Center regarding signifi-
17 cant cybersecurity risks and incidents.

18 “(j) REPORTS ON INTERNATIONAL COOPERATION.—
19 Not later than 180 days after the date of enactment of
20 this subsection, and periodically thereafter, the Secretary
21 of Homeland Security shall submit to the Committee on
22 Homeland Security and Governmental Affairs of the Sen-
23 ate and the Committee on Homeland Security of the
24 House of Representatives a report on the range of efforts
25 underway to bolster cybersecurity collaboration with rel-

1 evant international partners in accordance with subsection
2 (c)(8).

3 “(k) OUTREACH.—Not later than 60 days after the
4 date of enactment of this subsection, the Secretary, acting
5 through the Under Secretary appointed under section
6 103(a)(1)(H), shall—

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

10 “(2) enhance outreach to critical infrastructure
11 owners and operators for purposes of such sharing.

12 “(l) COORDINATED VULNERABILITY DISCLOSURE.—
13 The Secretary, in coordination with industry and other
14 stakeholders, may develop and adhere to Department poli-
15 cies and procedures for coordinating vulnerability disclo-
16 sures.”.

17 **SEC. 204. INFORMATION SHARING AND ANALYSIS ORGANI-**
18 **ZATIONS.**

19 Section 212 of the Homeland Security Act of 2002
20 (6 U.S.C. 131) is amended—

21 (1) in paragraph (5)—

22 (A) in subparagraph (A)—

23 (i) by inserting “, including informa-
24 tion related to cybersecurity risks and inci-

1 dents,” after “critical infrastructure infor-
2 mation”; and

3 (ii) by inserting “, including
4 cybersecurity risks and incidents,” after
5 “related to critical infrastructure”;

6 (B) in subparagraph (B)—

7 (i) by inserting “, including
8 cybersecurity risks and incidents,” after
9 “critical infrastructure information”; and

10 (ii) by inserting “, including
11 cybersecurity risks and incidents,” after
12 “related to critical infrastructure”; and

13 (C) in subparagraph (C), by inserting “,
14 including cybersecurity risks and incidents,”
15 after “critical infrastructure information”; and

16 (2) by adding at the end the following:

17 “(8) CYBERSECURITY RISK; INCIDENT.—The
18 terms ‘cybersecurity risk’ and ‘incident’ have the
19 meanings given those terms in section 227.”.

20 **SEC. 205. NATIONAL RESPONSE FRAMEWORK.**

21 Section 228 of the Homeland Security Act of 2002,
22 as added by section 223(a)(4) of this division, is amended
23 by adding at the end the following:

24 “(d) NATIONAL RESPONSE FRAMEWORK.—The Sec-
25 retary, in coordination with the heads of other appropriate

1 Federal departments and agencies, and in accordance with
2 the National Cybersecurity Incident Response Plan re-
3 quired under subsection (c), shall regularly update, main-
4 tain, and exercise the Cyber Incident Annex to the Na-
5 tional Response Framework of the Department.”.

6 **SEC. 206. REPORT ON REDUCING CYBERSECURITY RISKS IN**
7 **DHS DATA CENTERS.**

8 Not later than 1 year after the date of the enactment
9 of this Act, the Secretary shall submit to the appropriate
10 congressional committees a report on the feasibility of the
11 Department creating an environment for the reduction in
12 cybersecurity risks in Department data centers, including
13 by increasing compartmentalization between systems, and
14 providing a mix of security controls between such compart-
15 ments.

16 **SEC. 207. ASSESSMENT.**

17 Not later than 2 years after the date of enactment
18 of this Act, the Comptroller General of the United States
19 shall submit to the appropriate congressional committees
20 a report that includes—

21 (1) an assessment of the implementation by the
22 Secretary of this title and the amendments made by
23 this title; and

24 (2) to the extent practicable, findings regarding
25 increases in the sharing of cyber threat indicators,

1 defensive measures, and information relating to
2 cybersecurity risks and incidents at the center estab-
3 lished under section 227 of the Homeland Security
4 Act of 2002, as redesignated by section 223(a) of
5 this division, and throughout the United States.

6 **SEC. 208. MULTIPLE SIMULTANEOUS CYBER INCIDENTS AT**
7 **CRITICAL INFRASTRUCTURE.**

8 Not later than 1 year after the date of enactment
9 of this Act, the Under Secretary appointed under section
10 103(a)(1)(H) of the Homeland Security Act of 2002 (6
11 U.S.C. 113(a)(1)(H)) shall provide information to the ap-
12 propriate congressional committees on the feasibility of
13 producing a risk-informed plan to address the risk of mul-
14 tiple simultaneous cyber incidents affecting critical infra-
15 structure, including cyber incidents that may have a cas-
16 cading effect on other critical infrastructure.

17 **SEC. 209. REPORT ON CYBERSECURITY VULNERABILITIES**
18 **OF UNITED STATES PORTS.**

19 Not later than 180 days after the date of enactment
20 of this Act, the Secretary shall submit to the appropriate
21 congressional committees, the Committee on Commerce,
22 Science and Transportation of the Senate, and the Com-
23 mittee on Transportation and Infrastructure of the House
24 of Representatives a report on cybersecurity vulnerabilities
25 for the 10 United States ports that the Secretary deter-

1 mines are at greatest risk of a cybersecurity incident and
2 provide recommendations to mitigate such vulnerabilities.

3 **SEC. 210. PROHIBITION ON NEW REGULATORY AUTHORITY.**

4 Nothing in this subtitle or the amendments made by
5 this subtitle may be construed to grant the Secretary any
6 authority to promulgate regulations or set standards relat-
7 ing to the cybersecurity of non-Federal entities, not in-
8 cluding State, local, and tribal governments, that was not
9 in effect on the day before the date of enactment of this
10 Act.

11 **SEC. 211. TERMINATION OF REPORTING REQUIREMENTS.**

12 Any reporting requirements in this subtitle shall ter-
13minate on the date that is 7 years after the date of enact-
14ment of this Act.

15 **Subtitle B—Federal Cybersecurity**
16 **Enhancement**

17 **SEC. 221. SHORT TITLE.**

18 This subtitle may be cited as the “Federal
19 Cybersecurity Enhancement Act of 2015”.

20 **SEC. 222. DEFINITIONS.**

21 In this subtitle:

22 (1) AGENCY.—The term “agency” has the
23 meaning given the term in section 3502 of title 44,
24 United States Code.

1 (2) AGENCY INFORMATION SYSTEM.—The term
2 “agency information system” has the meaning given
3 the term in section 228 of the Homeland Security
4 Act of 2002, as added by section 223(a)(4) of this
5 division.

6 (3) APPROPRIATE CONGRESSIONAL COMMIT-
7 TEES.—The term “appropriate congressional com-
8 mittees” means—

9 (A) the Committee on Homeland Security
10 and Governmental Affairs of the Senate; and

11 (B) the Committee on Homeland Security
12 of the House of Representatives.

13 (4) CYBERSECURITY RISK; INFORMATION SYS-
14 TEM.—The terms “cybersecurity risk” and “infor-
15 mation system” have the meanings given those
16 terms in section 227 of the Homeland Security Act
17 of 2002, as so redesignated by section 223(a)(3) of
18 this division.

19 (5) DIRECTOR.—The term “Director” means
20 the Director of the Office of Management and Budg-
21 et.

22 (6) INTELLIGENCE COMMUNITY.—The term
23 “intelligence community” has the meaning given the
24 term in section 3(4) of the National Security Act of
25 1947 (50 U.S.C. 3003(4)).

1 (7) NATIONAL SECURITY SYSTEM.—The term
2 “national security system” has the meaning given
3 the term in section 11103 of title 40, United States
4 Code.

5 (8) SECRETARY.—The term “Secretary” means
6 the Secretary of Homeland Security.

7 **SEC. 223. IMPROVED FEDERAL NETWORK SECURITY.**

8 (a) IN GENERAL.—Subtitle C of title II of the Home-
9 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
10 ed—

11 (1) by redesignating section 228 as section 229;

12 (2) by redesignating section 227 as subsection
13 (c) of section 228, as added by paragraph (4), and
14 adjusting the margins accordingly;

15 (3) by redesignating the second section des-
16 ignated as section 226 (relating to the national
17 cybersecurity and communications integration cen-
18 ter) as section 227;

19 (4) by inserting after section 227, as so redesign-
20 ated, the following:

21 **“SEC. 228. CYBERSECURITY PLANS.**

22 “(a) DEFINITIONS.—In this section—

23 “(1) the term ‘agency information system’
24 means an information system used or operated by an
25 agency or by another entity on behalf of an agency;

1 “(2) the terms ‘cybersecurity risk’ and ‘infor-
2 mation system’ have the meanings given those terms
3 in section 227;

4 “(3) the term ‘intelligence community’ has the
5 meaning given the term in section 3(4) of the Na-
6 tional Security Act of 1947 (50 U.S.C. 3003(4));
7 and

8 “(4) the term ‘national security system’ has the
9 meaning given the term in section 11103 of title 40,
10 United States Code.

11 “(b) INTRUSION ASSESSMENT PLAN.—

12 “(1) REQUIREMENT.—The Secretary, in coordi-
13 nation with the Director of the Office of Manage-
14 ment and Budget, shall—

15 “(A) develop and implement an intrusion
16 assessment plan to proactively detect, identify,
17 and remove intruders in agency information
18 systems on a routine basis; and

19 “(B) update such plan as necessary.

20 “(2) EXCEPTION.—The intrusion assessment
21 plan required under paragraph (1) shall not apply to
22 the Department of Defense, a national security sys-
23 tem, or an element of the intelligence community.”;

1 (5) in section 228(c), as so redesignated, by
2 striking “section 226” and inserting “section 227”;
3 and

4 (6) by inserting after section 229, as so redesignated, the following:

6 **“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVEN-**
7 **TION SYSTEM.**

8 “(a) DEFINITIONS.—In this section—

9 “(1) the term ‘agency’ has the meaning given
10 the term in section 3502 of title 44, United States
11 Code;

12 “(2) the term ‘agency information’ means infor-
13 mation collected or maintained by or on behalf of an
14 agency;

15 “(3) the term ‘agency information system’ has
16 the meaning given the term in section 228; and

17 “(4) the terms ‘cybersecurity risk’ and ‘infor-
18 mation system’ have the meanings given those terms
19 in section 227.

20 “(b) REQUIREMENT.—

21 “(1) IN GENERAL.—Not later than 1 year after
22 the date of enactment of this section, the Secretary
23 shall deploy, operate, and maintain, to make avail-
24 able for use by any agency, with or without reim-
25 bursement—

1 “(A) a capability to detect cybersecurity
2 risks in network traffic transiting or traveling
3 to or from an agency information system; and

4 “(B) a capability to prevent network traffic
5 associated with such cybersecurity risks from
6 transiting or traveling to or from an agency in-
7 formation system or modify such network traf-
8 fic to remove the cybersecurity risk.

9 “(2) REGULAR IMPROVEMENT.—The Secretary
10 shall regularly deploy new technologies and modify
11 existing technologies to the intrusion detection and
12 prevention capabilities described in paragraph (1) as
13 appropriate to improve the intrusion detection and
14 prevention capabilities.

15 “(c) ACTIVITIES.—In carrying out subsection (b), the
16 Secretary—

17 “(1) may access, and the head of an agency
18 may disclose to the Secretary or a private entity pro-
19 viding assistance to the Secretary under paragraph
20 (2), information transiting or traveling to or from an
21 agency information system, regardless of the location
22 from which the Secretary or a private entity pro-
23 viding assistance to the Secretary under paragraph
24 (2) accesses such information, notwithstanding any
25 other provision of law that would otherwise restrict

1 or prevent the head of an agency from disclosing
2 such information to the Secretary or a private entity
3 providing assistance to the Secretary under para-
4 graph (2);

5 “(2) may enter into contracts or other agree-
6 ments with, or otherwise request and obtain the as-
7 sistance of, private entities to deploy, operate, and
8 maintain technologies in accordance with subsection
9 (b);

10 “(3) may retain, use, and disclose information
11 obtained through the conduct of activities authorized
12 under this section only to protect information and
13 information systems from cybersecurity risks;

14 “(4) shall regularly assess through operational
15 test and evaluation in real world or simulated envi-
16 ronments available advanced protective technologies
17 to improve detection and prevention capabilities, in-
18 cluding commercial and noncommercial technologies
19 and detection technologies beyond signature-based
20 detection, and acquire, test, and deploy such tech-
21 nologies when appropriate;

22 “(5) shall establish a pilot through which the
23 Secretary may acquire, test, and deploy, as rapidly
24 as possible, technologies described in paragraph (4);
25 and

1 “(6) shall periodically update the privacy im-
2 pact assessment required under section 208(b) of
3 the E-Government Act of 2002 (44 U.S.C. 3501
4 note).

5 “(d) PRINCIPLES.—In carrying out subsection (b),
6 the Secretary shall ensure that—

7 “(1) activities carried out under this section are
8 reasonably necessary for the purpose of protecting
9 agency information and agency information systems
10 from a cybersecurity risk;

11 “(2) information accessed by the Secretary will
12 be retained no longer than reasonably necessary for
13 the purpose of protecting agency information and
14 agency information systems from a cybersecurity
15 risk;

16 “(3) notice has been provided to users of an
17 agency information system concerning access to
18 communications of users of the agency information
19 system for the purpose of protecting agency informa-
20 tion and the agency information system; and

21 “(4) the activities are implemented pursuant to
22 policies and procedures governing the operation of
23 the intrusion detection and prevention capabilities.

24 “(e) PRIVATE ENTITIES.—

1 “(1) CONDITIONS.—A private entity described
2 in subsection (c)(2) may not—

3 “(A) disclose any network traffic transiting
4 or traveling to or from an agency information
5 system to any entity other than the Department
6 or the agency that disclosed the information
7 under subsection (c)(1), including personal in-
8 formation of a specific individual or information
9 that identifies a specific individual not directly
10 related to a cybersecurity risk; or

11 “(B) use any network traffic transiting or
12 traveling to or from an agency information sys-
13 tem to which the private entity gains access in
14 accordance with this section for any purpose
15 other than to protect agency information and
16 agency information systems against
17 cybersecurity risks or to administer a contract
18 or other agreement entered into pursuant to
19 subsection (c)(2) or as part of another contract
20 with the Secretary.

21 “(2) LIMITATION ON LIABILITY.—No cause of
22 action shall lie in any court against a private entity
23 for assistance provided to the Secretary in accord-
24 ance with this section and any contract or agree-
25 ment entered into pursuant to subsection (c)(2).

1 “(3) RULE OF CONSTRUCTION.—Nothing in
2 paragraph (2) shall be construed to authorize an
3 Internet service provider to break a user agreement
4 with a customer without the consent of the cus-
5 tomer.

6 “(f) PRIVACY OFFICER REVIEW.—Not later than 1
7 year after the date of enactment of this section, the Pri-
8 vacy Officer appointed under section 222, in consultation
9 with the Attorney General, shall review the policies and
10 guidelines for the program carried out under this section
11 to ensure that the policies and guidelines are consistent
12 with applicable privacy laws, including those governing the
13 acquisition, interception, retention, use, and disclosure of
14 communications.”.

15 (b) AGENCY RESPONSIBILITIES.—

16 (1) IN GENERAL.—Except as provided in para-
17 graph (2)—

18 (A) not later than 1 year after the date of
19 enactment of this Act or 2 months after the
20 date on which the Secretary makes available the
21 intrusion detection and prevention capabilities
22 under section 230(b)(1) of the Homeland Secu-
23 rity Act of 2002, as added by subsection (a),
24 whichever is later, the head of each agency shall
25 apply and continue to utilize the capabilities to

1 all information traveling between an agency in-
2 formation system and any information system
3 other than an agency information system; and

4 (B) not later than 6 months after the date
5 on which the Secretary makes available im-
6 provements to the intrusion detection and pre-
7 vention capabilities pursuant to section
8 230(b)(2) of the Homeland Security Act of
9 2002, as added by subsection (a), the head of
10 each agency shall apply and continue to utilize
11 the improved intrusion detection and prevention
12 capabilities.

13 (2) EXCEPTION.—The requirements under
14 paragraph (1) shall not apply to the Department of
15 Defense, a national security system, or an element
16 of the intelligence community.

17 (3) DEFINITION.—Notwithstanding section
18 222, in this subsection, the term “agency informa-
19 tion system” means an information system owned or
20 operated by an agency.

21 (4) RULE OF CONSTRUCTION.—Nothing in this
22 subsection shall be construed to limit an agency
23 from applying the intrusion detection and prevention
24 capabilities to an information system other than an
25 agency information system under section 230(b)(1)

1 of the Homeland Security Act of 2002, as added by
2 subsection (a), at the discretion of the head of the
3 agency or as provided in relevant policies, directives,
4 and guidelines.

5 (c) TABLE OF CONTENTS AMENDMENT.—The table
6 of contents in section 1(b) of the Homeland Security Act
7 of 2002 (6 U.S.C. 101 note) is amended by striking the
8 items relating to the first section designated as section
9 226, the second section designated as section 226 (relating
10 to the national cybersecurity and communications integra-
11 tion center), section 227, and section 228 and inserting
12 the following:

“Sec. 226. Cybersecurity recruitment and retention.

“Sec. 227. National cybersecurity and communications integration center.

“Sec. 228. Cybersecurity plans.

“Sec. 229. Clearances.

“Sec. 230. Federal intrusion detection and prevention system.”.

13 **SEC. 224. ADVANCED INTERNAL DEFENSES.**

14 (a) ADVANCED NETWORK SECURITY TOOLS.—

15 (1) IN GENERAL.—The Secretary shall include,
16 in the efforts of the Department to continuously di-
17 agnose and mitigate cybersecurity risks, advanced
18 network security tools to improve visibility of net-
19 work activity, including through the use of commer-
20 cial and free or open source tools, and to detect and
21 mitigate intrusions and anomalous activity.

22 (2) DEVELOPMENT OF PLAN.—The Director
23 shall develop and the Secretary shall implement a

1 plan to ensure that each agency utilizes advanced
2 network security tools, including those described in
3 paragraph (1), to detect and mitigate intrusions and
4 anomalous activity.

5 (b) **PRIORITIZING ADVANCED SECURITY TOOLS.**—
6 The Director and the Secretary, in consultation with ap-
7 propriate agencies, shall—

8 (1) review and update Government-wide policies
9 and programs to ensure appropriate prioritization
10 and use of network security monitoring tools within
11 agency networks; and

12 (2) brief appropriate congressional committees
13 on such prioritization and use.

14 (c) **IMPROVED METRICS.**—The Secretary, in collabo-
15 ration with the Director, shall review and update the
16 metrics used to measure security under section 3554 of
17 title 44, United States Code, to include measures of intru-
18 sion and incident detection and response times.

19 (d) **TRANSPARENCY AND ACCOUNTABILITY.**—The
20 Director, in consultation with the Secretary, shall increase
21 transparency to the public on agency cybersecurity pos-
22 ture, including by increasing the number of metrics avail-
23 able on Federal Government performance websites and, to
24 the greatest extent practicable, displaying metrics for de-
25 partment components, small agencies, and micro-agencies.

1 (e) MAINTENANCE OF TECHNOLOGIES.—Section
2 3553(b)(6)(B) of title 44, United States Code, is amended
3 by inserting “, operating, and maintaining” after “deploy-
4 ing”.

5 (f) EXCEPTION.—The requirements under this sec-
6 tion shall not apply to the Department of Defense, a na-
7 tional security system, or an element of the intelligence
8 community.

9 **SEC. 225. FEDERAL CYBERSECURITY REQUIREMENTS.**

10 (a) IMPLEMENTATION OF FEDERAL CYBERSECURITY
11 STANDARDS.—Consistent with section 3553 of title 44,
12 United States Code, the Secretary, in consultation with
13 the Director, shall exercise the authority to issue binding
14 operational directives to assist the Director in ensuring
15 timely agency adoption of and compliance with policies
16 and standards promulgated under section 11331 of title
17 40, United States Code, for securing agency information
18 systems.

19 (b) CYBERSECURITY REQUIREMENTS AT AGEN-
20 CIES.—

21 (1) IN GENERAL.—Consistent with policies,
22 standards, guidelines, and directives on information
23 security under subchapter II of chapter 35 of title
24 44, United States Code, and the standards and
25 guidelines promulgated under section 11331 of title

1 40, United States Code, and except as provided in
2 paragraph (2), not later than 1 year after the date
3 of the enactment of this Act, the head of each agen-
4 cy shall—

5 (A) identify sensitive and mission critical
6 data stored by the agency consistent with the
7 inventory required under the first subsection (c)
8 (relating to the inventory of major information
9 systems) and the second subsection (c) (relating
10 to the inventory of information systems) of sec-
11 tion 3505 of title 44, United States Code;

12 (B) assess access controls to the data de-
13 scribed in subparagraph (A), the need for read-
14 ily accessible storage of the data, and individ-
15 uals' need to access the data;

16 (C) encrypt or otherwise render indecipher-
17 able to unauthorized users the data described in
18 subparagraph (A) that is stored on or
19 transiting agency information systems;

20 (D) implement a single sign-on trusted
21 identity platform for individuals accessing each
22 public website of the agency that requires user
23 authentication, as developed by the Adminis-
24 trator of General Services in collaboration with
25 the Secretary; and

1 (E) implement identity management con-
2 sistent with section 504 of the Cybersecurity
3 Enhancement Act of 2014 (Public Law 113–
4 274; 15 U.S.C. 7464), including multi-factor
5 authentication, for—

6 (i) remote access to an agency infor-
7 mation system; and

8 (ii) each user account with elevated
9 privileges on an agency information sys-
10 tem.

11 (2) EXCEPTION.—The requirements under
12 paragraph (1) shall not apply to an agency informa-
13 tion system for which—

14 (A) the head of the agency has personally
15 certified to the Director with particularity
16 that—

17 (i) operational requirements articu-
18 lated in the certification and related to the
19 agency information system would make it
20 excessively burdensome to implement the
21 cybersecurity requirement;

22 (ii) the cybersecurity requirement is
23 not necessary to secure the agency infor-
24 mation system or agency information
25 stored on or transiting it; and

1 (iii) the agency has taken all nec-
2 essary steps to secure the agency informa-
3 tion system and agency information stored
4 on or transiting it; and

5 (B) the head of the agency or the designee
6 of the head of the agency has submitted the
7 certification described in subparagraph (A) to
8 the appropriate congressional committees and
9 the agency's authorizing committees.

10 (3) CONSTRUCTION.—Nothing in this section
11 shall be construed to alter the authority of the Sec-
12 retary, the Director, or the Director of the National
13 Institute of Standards and Technology in imple-
14 menting subchapter II of chapter 35 of title 44,
15 United States Code. Nothing in this section shall be
16 construed to affect the National Institute of Stand-
17 ards and Technology standards process or the re-
18 quirement under section 3553(a)(4) of such title or
19 to discourage continued improvements and advance-
20 ments in the technology, standards, policies, and
21 guidelines used to promote Federal information se-
22 curity.

23 (c) EXCEPTION.—The requirements under this sec-
24 tion shall not apply to the Department of Defense, a na-

1 tional security system, or an element of the intelligence
2 community.

3 **SEC. 226. ASSESSMENT; REPORTS.**

4 (a) DEFINITIONS.—In this section:

5 (1) AGENCY INFORMATION.—The term “agency
6 information” has the meaning given the term in sec-
7 tion 230 of the Homeland Security Act of 2002, as
8 added by section 223(a)(6) of this division.

9 (2) CYBER THREAT INDICATOR; DEFENSIVE
10 MEASURE.—The terms “cyber threat indicator” and
11 “defensive measure” have the meanings given those
12 terms in section 102.

13 (3) INTRUSION ASSESSMENTS.—The term “in-
14 trusion assessments” means actions taken under the
15 intrusion assessment plan to identify and remove in-
16 truders in agency information systems.

17 (4) INTRUSION ASSESSMENT PLAN.—The term
18 “intrusion assessment plan” means the plan re-
19 quired under section 228(b)(1) of the Homeland Se-
20 curity Act of 2002, as added by section 223(a)(4) of
21 this division.

22 (5) INTRUSION DETECTION AND PREVENTION
23 CAPABILITIES.—The term “intrusion detection and
24 prevention capabilities” means the capabilities re-
25 quired under section 230(b) of the Homeland Secu-

1 rity Act of 2002, as added by section 223(a)(6) of
2 this division.

3 (b) THIRD-PARTY ASSESSMENT.—Not later than 3
4 years after the date of enactment of this Act, the Comp-
5 troller General of the United States shall conduct a study
6 and publish a report on the effectiveness of the approach
7 and strategy of the Federal Government to securing agen-
8 cy information systems, including the intrusion detection
9 and prevention capabilities and the intrusion assessment
10 plan.

11 (c) REPORTS TO CONGRESS.—

12 (1) INTRUSION DETECTION AND PREVENTION
13 CAPABILITIES.—

14 (A) SECRETARY OF HOMELAND SECURITY
15 REPORT.—Not later than 6 months after the
16 date of enactment of this Act, and annually
17 thereafter, the Secretary shall submit to the ap-
18 propriate congressional committees a report on
19 the status of implementation of the intrusion
20 detection and prevention capabilities, includ-
21 ing—

22 (i) a description of privacy controls;

23 (ii) a description of the technologies
24 and capabilities utilized to detect
25 cybersecurity risks in network traffic, in-

1 cluding the extent to which those tech-
2 nologies and capabilities include existing
3 commercial and noncommercial tech-
4 nologies;

5 (iii) a description of the technologies
6 and capabilities utilized to prevent network
7 traffic associated with cybersecurity risks
8 from transiting or traveling to or from
9 agency information systems, including the
10 extent to which those technologies and ca-
11 pabilities include existing commercial and
12 noncommercial technologies;

13 (iv) a list of the types of indicators or
14 other identifiers or techniques used to de-
15 tect cybersecurity risks in network traffic
16 transiting or traveling to or from agency
17 information systems on each iteration of
18 the intrusion detection and prevention ca-
19 pabilities and the number of each such
20 type of indicator, identifier, and technique;

21 (v) the number of instances in which
22 the intrusion detection and prevention ca-
23 pabilities detected a cybersecurity risk in
24 network traffic transiting or traveling to or
25 from agency information systems and the

1 number of times the intrusion detection
2 and prevention capabilities blocked net-
3 work traffic associated with cybersecurity
4 risk; and

5 (vi) a description of the pilot estab-
6 lished under section 230(c)(5) of the
7 Homeland Security Act of 2002, as added
8 by section 223(a)(6) of this division, in-
9 cluding the number of new technologies
10 tested and the number of participating
11 agencies.

12 (B) OMB REPORT.—Not later than 18
13 months after the date of enactment of this Act,
14 and annually thereafter, the Director shall sub-
15 mit to Congress, as part of the report required
16 under section 3553(c) of title 44, United States
17 Code, an analysis of agency application of the
18 intrusion detection and prevention capabilities,
19 including—

20 (i) a list of each agency and the de-
21 gree to which each agency has applied the
22 intrusion detection and prevention capabili-
23 ties to an agency information system; and

24 (ii) a list by agency of—

1 (I) the number of instances in
2 which the intrusion detection and pre-
3 vention capabilities detected a
4 cybersecurity risk in network traffic
5 transiting or traveling to or from an
6 agency information system and the
7 types of indicators, identifiers, and
8 techniques used to detect such
9 cybersecurity risks; and

10 (II) the number of instances in
11 which the intrusion detection and pre-
12 vention capabilities prevented network
13 traffic associated with a cybersecurity
14 risk from transiting or traveling to or
15 from an agency information system
16 and the types of indicators, identi-
17 fiers, and techniques used to detect
18 such agency information systems.

19 (C) CHIEF INFORMATION OFFICER.—Not
20 earlier than 18 months after the date of enact-
21 ment of this Act and not later than 2 years
22 after the date of enactment of this Act, the
23 Federal Chief Information Officer shall review
24 and submit to the appropriate congressional
25 committees a report assessing the intrusion de-

1 tection and intrusion prevention capabilities, in-
2 cluding—

3 (i) the effectiveness of the system in
4 detecting, disrupting, and preventing
5 cyber-threat actors, including advanced
6 persistent threats, from accessing agency
7 information and agency information sys-
8 tems;

9 (ii) whether the intrusion detection
10 and prevention capabilities, continuous
11 diagnostics and mitigation, and other sys-
12 tems deployed under subtitle D of title II
13 of the Homeland Security Act of 2002 (6
14 U.S.C. 231 et seq.) are effective in secur-
15 ing Federal information systems;

16 (iii) the costs and benefits of the in-
17 trusion detection and prevention capabili-
18 ties, including as compared to commercial
19 technologies and tools and including the
20 value of classified cyber threat indicators;
21 and

22 (iv) the capability of agencies to pro-
23 tect sensitive cyber threat indicators and
24 defensive measures if they were shared

1 through unclassified mechanisms for use in
2 commercial technologies and tools.

3 (2) OMB REPORT ON DEVELOPMENT AND IM-
4 PLEMENTATION OF INTRUSION ASSESSMENT PLAN,
5 ADVANCED INTERNAL DEFENSES, AND FEDERAL
6 CYBERSECURITY REQUIREMENTS.—The Director
7 shall—

8 (A) not later than 6 months after the date
9 of enactment of this Act, and 30 days after any
10 update thereto, submit the intrusion assessment
11 plan to the appropriate congressional commit-
12 tees;

13 (B) not later than 1 year after the date of
14 enactment of this Act, and annually thereafter,
15 submit to Congress, as part of the report re-
16 quired under section 3553(c) of title 44, United
17 States Code—

18 (i) a description of the implementation
19 of the intrusion assessment plan;

20 (ii) the findings of the intrusion as-
21 sessments conducted pursuant to the intru-
22 sion assessment plan;

23 (iii) a description of the advanced net-
24 work security tools included in the efforts
25 to continuously diagnose and mitigate

1 cybersecurity risks pursuant to section
2 224(a)(1); and

3 (iv) a list by agency of compliance
4 with the requirements of section 225(b);
5 and

6 (C) not later than 1 year after the date of
7 enactment of this Act, submit to the appro-
8 priate congressional committees—

9 (i) a copy of the plan developed pursu-
10 ant to section 224(a)(2); and

11 (ii) the improved metrics developed
12 pursuant to section 224(c).

13 (d) FORM.—Each report required under this section
14 shall be submitted in unclassified form, but may include
15 a classified annex.

16 **SEC. 227. TERMINATION.**

17 (a) IN GENERAL.—The authority provided under sec-
18 tion 230 of the Homeland Security Act of 2002, as added
19 by section 223(a)(6) of this division, and the reporting re-
20 quirements under section 226(c) of this division shall ter-
21minate on the date that is 7 years after the date of enact-
22ment of this Act.

23 (b) RULE OF CONSTRUCTION.—Nothing in sub-
24 section (a) shall be construed to affect the limitation of
25 liability of a private entity for assistance provided to the

1 Secretary under section 230(d)(2) of the Homeland Secu-
2 rity Act of 2002, as added by section 223(a)(6) of this
3 division, if such assistance was rendered before the termi-
4 nation date under subsection (a) or otherwise during a pe-
5 riod in which the assistance was authorized.

6 **SEC. 228. IDENTIFICATION OF INFORMATION SYSTEMS RE-**
7 **LATING TO NATIONAL SECURITY.**

8 (a) IN GENERAL.—Except as provided in subsection
9 (c), not later than 180 days after the date of enactment
10 of this Act—

11 (1) the Director of National Intelligence and
12 the Director of the Office of Management and Budg-
13 et, in coordination with the heads of other agencies,
14 shall—

15 (A) identify all unclassified information
16 systems that provide access to information that
17 may provide an adversary with the ability to de-
18 rive information that would otherwise be consid-
19 ered classified;

20 (B) assess the risks that would result from
21 the breach of each unclassified information sys-
22 tem identified in subparagraph (A); and

23 (C) assess the cost and impact on the mis-
24 sion carried out by each agency that owns an
25 unclassified information system identified in

1 subparagraph (A) if the system were to be sub-
2 sequently designated as a national security sys-
3 tem; and

4 (2) the Director of National Intelligence and
5 the Director of the Office of Management and Budg-
6 et shall submit to the appropriate congressional com-
7 mittees, the Select Committee on Intelligence of the
8 Senate, and the Permanent Select Committee on In-
9 telligence of the House of Representatives a report
10 that includes the findings under paragraph (1).

11 (b) FORM.—The report submitted under subsection
12 (a)(2) shall be in unclassified form, and shall include a
13 classified annex.

14 (c) EXCEPTION.—The requirements under subsection
15 (a)(1) shall not apply to the Department of Defense, a
16 national security system, or an element of the intelligence
17 community.

18 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
19 tion shall be construed to designate an information system
20 as a national security system.

21 **SEC. 229. DIRECTION TO AGENCIES.**

22 (a) IN GENERAL.—Section 3553 of title 44, United
23 States Code, is amended by adding at the end the fol-
24 lowing:

25 “(h) DIRECTION TO AGENCIES.—

1 “(1) AUTHORITY.—

2 “(A) IN GENERAL.—Subject to subpara-
3 graph (B), in response to a known or reason-
4 ably suspected information security threat, vul-
5 nerability, or incident that represents a sub-
6 stantial threat to the information security of an
7 agency, the Secretary may issue an emergency
8 directive to the head of an agency to take any
9 lawful action with respect to the operation of
10 the information system, including such systems
11 used or operated by another entity on behalf of
12 an agency, that collects, processes, stores,
13 transmits, disseminates, or otherwise maintains
14 agency information, for the purpose of pro-
15 tecting the information system from, or miti-
16 gating, an information security threat.

17 “(B) EXCEPTION.—The authorities of the
18 Secretary under this subsection shall not apply
19 to a system described subsection (d) or to a sys-
20 tem described in paragraph (2) or (3) of sub-
21 section (e).

22 “(2) PROCEDURES FOR USE OF AUTHORITY.—

23 The Secretary shall—

24 “(A) in coordination with the Director, and
25 in consultation with Federal contractors as ap-

1 appropriate, establish procedures governing the
2 circumstances under which a directive may be
3 issued under this subsection, which shall in-
4 clude—

5 “(i) thresholds and other criteria;

6 “(ii) privacy and civil liberties protec-
7 tions; and

8 “(iii) providing notice to potentially
9 affected third parties;

10 “(B) specify the reasons for the required
11 action and the duration of the directive;

12 “(C) minimize the impact of a directive
13 under this subsection by—

14 “(i) adopting the least intrusive
15 means possible under the circumstances to
16 secure the agency information systems;
17 and

18 “(ii) limiting directives to the shortest
19 period practicable;

20 “(D) notify the Director and the head of
21 any affected agency immediately upon the
22 issuance of a directive under this subsection;

23 “(E) consult with the Director of the Na-
24 tional Institute of Standards and Technology
25 regarding any directive under this subsection

1 that implements standards and guidelines devel-
2 oped by the National Institute of Standards
3 and Technology;

4 “(F) ensure that directives issued under
5 this subsection do not conflict with the stand-
6 ards and guidelines issued under section 11331
7 of title 40;

8 “(G) consider any applicable standards or
9 guidelines developed by the National Institute
10 of Standards and Technology issued by the Sec-
11 retary of Commerce under section 11331 of
12 title 40; and

13 “(H) not later than February 1 of each
14 year, submit to the appropriate congressional
15 committees a report regarding the specific ac-
16 tions the Secretary has taken pursuant to para-
17 graph (1)(A).

18 “(3) IMMINENT THREATS.—

19 “(A) IN GENERAL.—Notwithstanding sec-
20 tion 3554, the Secretary may authorize the use
21 under this subsection of the intrusion detection
22 and prevention capabilities established under
23 section 230(b)(1) of the Homeland Security Act
24 of 2002 for the purpose of ensuring the security
25 of agency information systems, if—

1 “(i) the Secretary determines there is
2 an imminent threat to agency information
3 systems;

4 “(ii) the Secretary determines a direc-
5 tive under subsection (b)(2)(C) or para-
6 graph (1)(A) is not reasonably likely to re-
7 sult in a timely response to the threat;

8 “(iii) the Secretary determines the
9 risk posed by the imminent threat out-
10 weighs any adverse consequences reason-
11 ably expected to result from the use of the
12 intrusion detection and prevention capabili-
13 ties under the control of the Secretary;

14 “(iv) the Secretary provides prior no-
15 tice to the Director, and the head and chief
16 information officer (or equivalent official)
17 of each agency to which specific actions
18 will be taken pursuant to this paragraph,
19 and notifies the appropriate congressional
20 committees and authorizing committees of
21 each such agency within 7 days of taking
22 an action under this paragraph of—

23 “(I) any action taken under this
24 paragraph; and

1 “(II) the reasons for and dura-
2 tion and nature of the action;

3 “(v) the action of the Secretary is
4 consistent with applicable law; and

5 “(vi) the Secretary authorizes the use
6 of the intrusion detection and prevention
7 capabilities in accordance with the advance
8 procedures established under subparagraph
9 (C).

10 “(B) LIMITATION ON DELEGATION.—The
11 authority under this paragraph may not be del-
12 egated by the Secretary.

13 “(C) ADVANCE PROCEDURES.—The Sec-
14 retary shall, in coordination with the Director,
15 and in consultation with the heads of Federal
16 agencies, establish procedures governing the cir-
17 cumstances under which the Secretary may au-
18 thorize the use of the intrusion detection and
19 prevention capabilities under subparagraph (A).
20 The Secretary shall submit the procedures to
21 Congress.

22 “(4) LIMITATION.—The Secretary may direct
23 or authorize lawful action or the use of the intrusion
24 detection and prevention capabilities under this sub-
25 section only to—

1 “(A) protect agency information from un-
2 authorized access, use, disclosure, disruption,
3 modification, or destruction; or

4 “(B) require the remediation of or protect
5 against identified information security risks
6 with respect to—

7 “(i) information collected or main-
8 tained by or on behalf of an agency; or

9 “(ii) that portion of an information
10 system used or operated by an agency or
11 by a contractor of an agency or other orga-
12 nization on behalf of an agency.

13 “(i) ANNUAL REPORT TO CONGRESS.—Not later
14 than February 1 of each year, the Director and the Sec-
15 retary shall submit to the appropriate congressional com-
16 mittees a report regarding the specific actions the Director
17 and the Secretary have taken pursuant to subsection
18 (a)(5), including any actions taken pursuant to section
19 11303(b)(5) of title 40.

20 “(j) APPROPRIATE CONGRESSIONAL COMMITTEES
21 DEFINED.—In this section, the term ‘appropriate congres-
22 sional committees’ means—

23 “(1) the Committee on Appropriations and the
24 Committee on Homeland Security and Governmental
25 Affairs of the Senate; and

1 (A) the Committee on Armed Services of
2 the Senate;

3 (B) the Committee on Homeland Security
4 and Governmental Affairs of the Senate;

5 (C) the Select Committee on Intelligence of
6 the Senate;

7 (D) the Committee on Commerce, Science,
8 and Transportation of the Senate;

9 (E) the Committee on Armed Services of
10 the House of Representatives;

11 (F) the Committee on Homeland Security
12 of the House of Representatives;

13 (G) the Committee on Oversight and Gov-
14 ernment Reform of the House of Representa-
15 tives; and

16 (H) the Permanent Select Committee on
17 Intelligence of the House of Representatives.

18 (2) DIRECTOR.—The term “Director” means
19 the Director of the Office of Personnel Management.

20 (3) NATIONAL INITIATIVE FOR CYBERSECURITY
21 EDUCATION.—The term “National Initiative for
22 Cybersecurity Education” means the initiative under
23 the national cybersecurity awareness and education
24 program, as authorized under section 401 of the

1 Cybersecurity Enhancement Act of 2014 (15 U.S.C.
2 7451).

3 (4) WORK ROLES.—The term “ work roles”
4 means a specialized set of tasks and functions re-
5 quiring specific knowledge, skills, and abilities.

6 **SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEAS-**
7 **UREMENT INITIATIVE.**

8 (a) IN GENERAL.—The head of each Federal agency
9 shall—

10 (1) identify all positions within the agency that
11 require the performance of cybersecurity or other
12 cyber-related functions; and

13 (2) assign the corresponding employment code
14 under the National Initiative for Cybersecurity Edu-
15 cation in accordance with subsection (b).

16 (b) EMPLOYMENT CODES.—

17 (1) PROCEDURES.—

18 (A) CODING STRUCTURE.—Not later than
19 180 days after the date of the enactment of this
20 Act, the Director, in coordination with the Na-
21 tional Institute of Standards and Technology,
22 shall develop a coding structure under the Na-
23 tional Initiative for Cybersecurity Education.

24 (B) IDENTIFICATION OF CIVILIAN CYBER
25 PERSONNEL.—Not later than 9 months after

1 the date of enactment of this Act, the Director,
2 in coordination with the Secretary of Homeland
3 Security, the Director of the National Institute
4 of Standards and Technology, and the Director
5 of National Intelligence, shall establish proce-
6 dures to implement the National Initiative for
7 Cybersecurity Education coding structure to
8 identify all Federal civilian positions that re-
9 quire the performance of information tech-
10 nology, cybersecurity, or other cyber-related
11 functions.

12 (C) IDENTIFICATION OF NONCIVILIAN
13 CYBER PERSONNEL.—Not later than 18 months
14 after the date of enactment of this Act, the Sec-
15 retary of Defense shall establish procedures to
16 implement the National Initiative for
17 Cybersecurity Education’s coding structure to
18 identify all Federal noncivilian positions that
19 require the performance of information tech-
20 nology, cybersecurity, or other cyber-related
21 functions.

22 (D) BASELINE ASSESSMENT OF EXISTING
23 CYBERSECURITY WORKFORCE.—Not later than
24 3 months after the date on which the proce-
25 dures are developed under subparagraphs (B)

1 and (C), respectively, the head of each Federal
2 agency shall submit to the appropriate congress-
3 sional committees of jurisdiction a report that
4 identifies—

5 (i) the percentage of personnel with
6 information technology, cybersecurity, or
7 other cyber-related job functions who cur-
8 rently hold the appropriate industry-recog-
9 nized certifications as identified under the
10 National Initiative for Cybersecurity Edu-
11 cation;

12 (ii) the level of preparedness of other
13 civilian and noncivilian cyber personnel
14 without existing credentials to take certifi-
15 cation exams; and

16 (iii) a strategy for mitigating any
17 gaps identified in clause (i) or (ii) with the
18 appropriate training and certification for
19 existing personnel.

20 (E) PROCEDURES FOR ASSIGNING
21 CODES.—Not later than 3 months after the
22 date on which the procedures are developed
23 under subparagraphs (B) and (C), respectively,
24 the head of each Federal agency shall establish
25 procedures—

1 (i) to identify all encumbered and va-
2 cant positions with information technology,
3 cybersecurity, or other cyber-related func-
4 tions (as defined in the National Initiative
5 for Cybersecurity Education’s coding struc-
6 ture); and

7 (ii) to assign the appropriate employ-
8 ment code to each such position, using
9 agreed standards and definitions.

10 (2) CODE ASSIGNMENTS.—Not later than 1
11 year after the date after the procedures are estab-
12 lished under paragraph (1)(E), the head of each
13 Federal agency shall complete assignment of the ap-
14 propriate employment code to each position within
15 the agency with information technology,
16 cybersecurity, or other cyber-related functions.

17 (c) PROGRESS REPORT.—Not later than 180 days
18 after the date of enactment of this Act, the Director shall
19 submit a progress report on the implementation of this
20 section to the appropriate congressional committees.

21 **SEC. 304. IDENTIFICATION OF CYBER-RELATED WORK**
22 **ROLES OF CRITICAL NEED.**

23 (a) IN GENERAL.—Beginning not later than 1 year
24 after the date on which the employment codes are assigned
25 to employees pursuant to section 303(b)(2), and annually

1 thereafter through 2022, the head of each Federal agency,
2 in consultation with the Director, the Director of the Na-
3 tional Institute of Standards and Technology, and the Sec-
4 retary of Homeland Security, shall—

5 (1) identify information technology,
6 cybersecurity, or other cyber-related work roles of
7 critical need in the agency's workforce; and

8 (2) submit a report to the Director that—

9 (A) describes the information technology,
10 cybersecurity, or other cyber-related roles iden-
11 tified under paragraph (1); and

12 (B) substantiates the critical need designa-
13 tions.

14 (b) GUIDANCE.—The Director shall provide Federal
15 agencies with timely guidance for identifying information
16 technology, cybersecurity, or other cyber-related roles of
17 critical need, including—

18 (1) current information technology,
19 cybersecurity, and other cyber-related roles with
20 acute skill shortages; and

21 (2) information technology, cybersecurity, or
22 other cyber-related roles with emerging skill short-
23 ages.

24 (c) CYBERSECURITY NEEDS REPORT.—Not later
25 than 2 years after the date of the enactment of this Act,

1 the Director, in consultation with the Secretary of Home-
2 land Security, shall—

3 (1) identify critical needs for information tech-
4 nology, cybersecurity, or other cyber-related work-
5 force across all Federal agencies; and

6 (2) submit a progress report on the implemen-
7 tation of this section to the appropriate congres-
8 sional committees.

9 **SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS**
10 **REPORTS.**

11 The Comptroller General of the United States shall—

12 (1) analyze and monitor the implementation of
13 sections 303 and 304; and

14 (2) not later than 3 years after the date of the
15 enactment of this Act, submit a report to the appro-
16 priate congressional committees that describes the
17 status of such implementation.

18 **TITLE IV—OTHER CYBER**
19 **MATTERS**

20 **SEC. 401. STUDY ON MOBILE DEVICE SECURITY.**

21 (a) IN GENERAL.—Not later than 1 year after the
22 date of the enactment of this Act, the Secretary of Home-
23 land Security, in consultation with the Director of the Na-
24 tional Institute of Standards and Technology, shall—

1 (1) complete a study on threats relating to the
2 security of the mobile devices of the Federal Govern-
3 ment; and

4 (2) submit an unclassified report to Congress,
5 with a classified annex if necessary, that contains
6 the findings of such study, the recommendations de-
7 veloped under paragraph (3) of subsection (b), the
8 deficiencies, if any, identified under (4) of such sub-
9 section, and the plan developed under paragraph (5)
10 of such subsection.

11 (b) MATTERS STUDIED.—In carrying out the study
12 under subsection (a)(1), the Secretary, in consultation
13 with the Director of the National Institute of Standards
14 and Technology, shall—

15 (1) assess the evolution of mobile security tech-
16 niques from a desktop-centric approach, and whether
17 such techniques are adequate to meet current mobile
18 security challenges;

19 (2) assess the effect such threats may have on
20 the cybersecurity of the information systems and
21 networks of the Federal Government (except for na-
22 tional security systems or the information systems
23 and networks of the Department of Defense and the
24 intelligence community);

1 (1) A review of actions and activities under-
2 taken by the Secretary of State to date to support
3 the goal of the President’s International Strategy for
4 Cyberspace, released in May 2011, to “work inter-
5 nationally to promote an open, interoperable, secure,
6 and reliable information and communications infra-
7 structure that supports international trade and com-
8 merce, strengthens international security, and fos-
9 ters free expression and innovation.”.

10 (2) A plan of action to guide the diplomacy of
11 the Secretary of State, with regard to foreign coun-
12 tries, including conducting bilateral and multilateral
13 activities to develop the norms of responsible inter-
14 national behavior in cyberspace, and status review of
15 existing discussions in multilateral fora to obtain
16 agreements on international norms in cyberspace.

17 (3) A review of the alternative concepts with re-
18 gard to international norms in cyberspace offered by
19 foreign countries that are prominent actors, includ-
20 ing China, Russia, Brazil, and India.

21 (4) A detailed description of threats to United
22 States national security in cyberspace from foreign
23 countries, state-sponsored actors, and private actors
24 to Federal and private sector infrastructure of the
25 United States, intellectual property in the United

1 States, and the privacy of citizens of the United
2 States.

3 (5) A review of policy tools available to the
4 President to deter foreign countries, state-sponsored
5 actors, and private actors, including those outlined
6 in Executive Order 13694, released on April 1,
7 2015.

8 (6) A review of resources required by the Sec-
9 retary, including the Office of the Coordinator for
10 Cyber Issues, to conduct activities to build respon-
11 sible norms of international cyber behavior.

12 (c) CONSULTATION.—In preparing the strategy re-
13 quired by subsection (a), the Secretary of State shall con-
14 sult, as appropriate, with other agencies and departments
15 of the United States and the private sector and nongovern-
16 mental organizations in the United States with recognized
17 credentials and expertise in foreign policy, national secu-
18 rity, and cybersecurity.

19 (d) FORM OF STRATEGY.—The strategy required by
20 subsection (a) shall be in unclassified form, but may in-
21 clude a classified annex.

22 (e) AVAILABILITY OF INFORMATION.—The Secretary
23 of State shall—

24 (1) make the strategy required in subsection (a)
25 available the public; and

1 (2) brief the Committee on Foreign Relations of
2 the Senate and the Committee on Foreign Affairs of
3 the House of Representatives on the strategy, in-
4 cluding any material contained in a classified annex.

5 **SEC. 403. APPREHENSION AND PROSECUTION OF INTER-**
6 **NATIONAL CYBER CRIMINALS.**

7 (a) INTERNATIONAL CYBER CRIMINAL DEFINED.—
8 In this section, the term “international cyber criminal”
9 means an individual—

10 (1) who is believed to have committed a
11 cybercrime or intellectual property crime against the
12 interests of the United States or the citizens of the
13 United States; and

14 (2) for whom—

15 (A) an arrest warrant has been issued by
16 a judge in the United States; or

17 (B) an international wanted notice (com-
18 monly referred to as a “Red Notice”) has been
19 circulated by Interpol.

20 (b) CONSULTATIONS FOR NONCOOPERATION.—The
21 Secretary of State, or designee, shall consult with the ap-
22 propriate government official of each country from which
23 extradition is not likely due to the lack of an extradition
24 treaty with the United States or other reasons, in which
25 one or more international cyber criminals are physically

1 present, to determine what actions the government of such
2 country has taken—

3 (1) to apprehend and prosecute such criminals;

4 and

5 (2) to prevent such criminals from carrying out
6 cybercrimes or intellectual property crimes against
7 the interests of the United States or its citizens.

8 (c) ANNUAL REPORT.—

9 (1) IN GENERAL.—The Secretary of State shall
10 submit to the appropriate congressional committees
11 an annual report that includes—

12 (A) the number of international cyber
13 criminals located in other countries,
14 disaggregated by country, and indicating from
15 which countries extradition is not likely due to
16 the lack of an extradition treaty with the
17 United States or other reasons;

18 (B) the nature and number of significant
19 discussions by an official of the Department of
20 State on ways to thwart or prosecute inter-
21 national cyber criminals with an official of an-
22 other country, including the name of each such
23 country; and

1 (C) for each international cyber criminal
2 who was extradited to the United States during
3 the most recently completed calendar year—

4 (i) his or her name;

5 (ii) the crimes for which he or she was
6 charged;

7 (iii) his or her previous country of res-
8 idence; and

9 (iv) the country from which he or she
10 was extradited into the United States.

11 (2) FORM.—The report required by this sub-
12 section shall be in unclassified form to the maximum
13 extent possible, but may include a classified annex.

14 (3) APPROPRIATE CONGRESSIONAL COMMIT-
15 TEES.—For purposes of this subsection, the term
16 “appropriate congressional committees” means—

17 (A) the Committee on Foreign Relations,
18 the Committee on Appropriations, the Com-
19 mittee on Homeland Security and Govern-
20 mental Affairs, the Committee on Banking,
21 Housing, and Urban Affairs, the Select Com-
22 mittee on Intelligence, and the Committee on
23 the Judiciary of the Senate; and

24 (B) the Committee on Foreign Affairs, the
25 Committee on Appropriations, the Committee

1 on Homeland Security, the Committee on Fi-
2 nancial Services, the Permanent Select Com-
3 mittee on Intelligence, and the Committee on
4 the Judiciary of the House of Representatives.

5 **SEC. 404. ENHANCEMENT OF EMERGENCY SERVICES.**

6 (a) COLLECTION OF DATA.—Not later than 90 days
7 after the date of the enactment of this Act, the Secretary
8 of Homeland Security, acting through the center estab-
9 lished under section 227 of the Homeland Security Act
10 of 2002, as redesignated by section 223(a)(3) of this divi-
11 sion, in coordination with appropriate Federal entities and
12 the Director for Emergency Communications, shall estab-
13 lish a process by which a Statewide Interoperability Coor-
14 dinator may report data on any cybersecurity risk or inci-
15 dent involving any information system or network used by
16 emergency response providers (as defined in section 2 of
17 the Homeland Security Act of 2002 (6 U.S.C. 101)) with-
18 in the State.

19 (b) ANALYSIS OF DATA.—Not later than 1 year after
20 the date of the enactment of this Act, the Secretary of
21 Homeland Security, acting through the Director of the
22 National Cybersecurity and Communications Integration
23 Center, in coordination with appropriate entities and the
24 Director for Emergency Communications, and in consulta-
25 tion with the Secretary of Commerce, acting through the

1 Director of the National Institute of Standards and Tech-
2 nology, shall conduct integration and analysis of the data
3 reported under subsection (a) to develop information and
4 recommendations on security and resilience measures for
5 any information system or network used by State emer-
6 gency response providers.

7 (c) BEST PRACTICES.—

8 (1) IN GENERAL.—Using the results of the in-
9 tegration and analysis conducted under subsection
10 (b), and any other relevant information, the Director
11 of the National Institute of Standards and Tech-
12 nology shall, on an ongoing basis, facilitate and sup-
13 port the development of methods for reducing
14 cybersecurity risks to emergency response providers
15 using the process described in section 2(e) of the
16 National Institute of Standards and Technology Act
17 (15 U.S.C. 272(e)).

18 (2) REPORT.—The Director of the National In-
19 stitute of Standards and Technology shall submit to
20 Congress a report on the result of the activities of
21 the Director under paragraph (1), including any
22 methods developed by the Director under such para-
23 graph, and shall make such report publicly available
24 on the website of the National Institute of Stand-
25 ards and Technology.

1 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion shall be construed to—

3 (1) require a State to report data under sub-
4 section (a); or

5 (2) require a non-Federal entity (as defined in
6 section 102) to—

7 (A) adopt a recommended measure devel-
8 oped under subsection (b); or

9 (B) follow the result of the activities car-
10 ried out under subsection (c), including any
11 methods developed under such subsection.

12 **SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH**
13 **CARE INDUSTRY.**

14 (a) DEFINITIONS.—In this section:

15 (1) APPROPRIATE CONGRESSIONAL COMMIT-
16 TEES.—The term “appropriate congressional com-
17 mittees” means—

18 (A) the Committee on Health, Education,
19 Labor, and Pensions, the Committee on Home-
20 land Security and Governmental Affairs, and
21 the Select Committee on Intelligence of the
22 Senate; and

23 (B) the Committee on Energy and Com-
24 merce, the Committee on Homeland Security,

1 and the Permanent Select Committee on Intel-
2 ligence of the House of Representatives.

3 (2) BUSINESS ASSOCIATE.—The term “business
4 associate” has the meaning given such term in sec-
5 tion 160.103 of title 45, Code of Federal Regula-
6 tions (as in effect on the day before the date of the
7 enactment of this Act).

8 (3) COVERED ENTITY.—The term “covered en-
9 tity” has the meaning given such term in section
10 160.103 of title 45, Code of Federal Regulations (as
11 in effect on the day before the date of the enactment
12 of this Act).

13 (4) CYBERSECURITY THREAT; CYBER THREAT
14 INDICATOR; DEFENSIVE MEASURE; FEDERAL ENTI-
15 TY; NON-FEDERAL ENTITY; PRIVATE ENTITY.—The
16 terms “cybersecurity threat”, “cyber threat indi-
17 cator”, “defensive measure”, “Federal entity”,
18 “non-Federal entity”, and “private entity” have the
19 meanings given such terms in section 102 of this di-
20 vision.

21 (5) HEALTH CARE CLEARINGHOUSE; HEALTH
22 CARE PROVIDER; HEALTH PLAN.—The terms
23 “health care clearinghouse”, “health care provider”,
24 and “health plan” have the meanings given such
25 terms in section 160.103 of title 45, Code of Federal

1 Regulations (as in effect on the day before the date
2 of the enactment of this Act).

3 (6) HEALTH CARE INDUSTRY STAKEHOLDER.—

4 The term “health care industry stakeholder” means
5 any—

6 (A) health plan, health care clearinghouse,
7 or health care provider;

8 (B) advocate for patients or consumers;

9 (C) pharmacist;

10 (D) developer or vendor of health informa-
11 tion technology;

12 (E) laboratory;

13 (F) pharmaceutical or medical device man-
14 ufacturer; or

15 (G) additional stakeholder the Secretary
16 determines necessary for purposes of subsection
17 (b)(1), (c)(1), (c)(3), or (d)(1).

18 (7) SECRETARY.—The term “Secretary” means
19 the Secretary of Health and Human Services.

20 (b) REPORT.—

21 (1) IN GENERAL.—Not later than 1 year after
22 the date of enactment of this Act, the Secretary
23 shall submit to the Committee on Health, Edu-
24 cation, Labor, and Pensions of the Senate and the
25 Committee on Energy and Commerce of the House

1 of Representatives a report on the preparedness of
2 the Department of Health and Human Services and
3 health care industry stakeholders in responding to
4 cybersecurity threats.

5 (2) CONTENTS OF REPORT.—With respect to
6 the internal response of the Department of Health
7 and Human Services to emerging cybersecurity
8 threats, the report under paragraph (1) shall in-
9 clude—

10 (A) a clear statement of the official within
11 the Department of Health and Human Services
12 to be responsible for leading and coordinating
13 efforts of the Department regarding
14 cybersecurity threats in the health care indus-
15 try; and

16 (B) a plan from each relevant operating di-
17 vision and subdivision of the Department of
18 Health and Human Services on how such divi-
19 sion or subdivision will address cybersecurity
20 threats in the health care industry, including a
21 clear delineation of how each such division or
22 subdivision will divide responsibility among the
23 personnel of such division or subdivision and
24 communicate with other such divisions and sub-

1 divisions regarding efforts to address such
2 threats.

3 (c) HEALTH CARE INDUSTRY CYBERSECURITY TASK
4 FORCE.—

5 (1) IN GENERAL.—Not later than 90 days after
6 the date of the enactment of this Act, the Secretary,
7 in consultation with the Director of the National In-
8 stitute of Standards and Technology and the Sec-
9 retary of Homeland Security, shall convene health
10 care industry stakeholders, cybersecurity experts,
11 and any Federal agencies or entities the Secretary
12 determines appropriate to establish a task force to—

13 (A) analyze how industries, other than the
14 health care industry, have implemented strate-
15 gies and safeguards for addressing
16 cybersecurity threats within their respective in-
17 dustries;

18 (B) analyze challenges and barriers private
19 entities (excluding any State, tribal, or local
20 government) in the health care industry face se-
21 curing themselves against cyber attacks;

22 (C) review challenges that covered entities
23 and business associates face in securing
24 networked medical devices and other software

1 or systems that connect to an electronic health
2 record;

3 (D) provide the Secretary with information
4 to disseminate to health care industry stake-
5 holders of all sizes for purposes of improving
6 their preparedness for, and response to,
7 cybersecurity threats affecting the health care
8 industry;

9 (E) establish a plan for implementing title
10 I of this division, so that the Federal Govern-
11 ment and health care industry stakeholders may
12 in real time, share actionable cyber threat indi-
13 cators and defensive measures; and

14 (F) report to the appropriate congressional
15 committees on the findings and recommenda-
16 tions of the task force regarding carrying out
17 subparagraphs (A) through (E).

18 (2) TERMINATION.—The task force established
19 under this subsection shall terminate on the date
20 that is 1 year after the date on which such task
21 force is established.

22 (3) DISSEMINATION.—Not later than 60 days
23 after the termination of the task force established
24 under this subsection, the Secretary shall dissemi-
25 nate the information described in paragraph (1)(D)

1 to health care industry stakeholders in accordance
2 with such paragraph.

3 (d) ALIGNING HEALTH CARE INDUSTRY SECURITY
4 APPROACHES.—

5 (1) IN GENERAL.—The Secretary shall estab-
6 lish, through a collaborative process with the Sec-
7 retary of Homeland Security, health care industry
8 stakeholders, the Director of the National Institute
9 of Standards and Technology, and any Federal enti-
10 ty or non-Federal entity the Secretary determines
11 appropriate, a common set of voluntary, consensus-
12 based, and industry-led guidelines, best practices,
13 methodologies, procedures, and processes that—

14 (A) serve as a resource for cost-effectively
15 reducing cybersecurity risks for a range of
16 health care organizations;

17 (B) support voluntary adoption and imple-
18 mentation efforts to improve safeguards to ad-
19 dress cybersecurity threats;

20 (C) are consistent with—

21 (i) the standards, guidelines, best
22 practices, methodologies, procedures, and
23 processes developed under section 2(c)(15)
24 of the National Institute of Standards and
25 Technology Act (15 U.S.C. 272(c)(15));

1 (ii) the security and privacy regula-
2 tions promulgated under section 264(e) of
3 the Health Insurance Portability and Ac-
4 countability Act of 1996 (42 U.S.C.
5 1320d–2 note); and

6 (iii) the provisions of the Health In-
7 formation Technology for Economic and
8 Clinical Health Act (title XIII of division
9 A, and title IV of division B, of Public
10 Law 111–5), and the amendments made
11 by such Act; and

12 (D) are updated on a regular basis and ap-
13 plicable to a range of health care organizations.

14 (2) LIMITATION.—Nothing in this subsection
15 shall be interpreted as granting the Secretary au-
16 thority to—

17 (A) provide for audits to ensure that
18 health care organizations are in compliance
19 with this subsection; or

20 (B) mandate, direct, or condition the
21 award of any Federal grant, contract, or pur-
22 chase, on compliance with this subsection.

23 (3) NO LIABILITY FOR NONPARTICIPATION.—
24 Nothing in this section shall be construed to subject
25 a health care industry stakeholder to liability for

1 choosing not to engage in the voluntary activities au-
2 thorized or guidelines developed under this sub-
3 section.

4 (e) INCORPORATING ONGOING ACTIVITIES.—In car-
5 rying out the activities under this section, the Secretary
6 may incorporate activities that are ongoing as of the day
7 before the date of enactment of this Act and that are con-
8 sistent with the objectives of this section.

9 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
10 tion shall be construed to limit the antitrust exemption
11 under section 104(e) or the protection from liability under
12 section 106.

13 **SEC. 406. FEDERAL COMPUTER SECURITY.**

14 (a) DEFINITIONS.—In this section:

15 (1) COVERED SYSTEM.—The term “covered sys-
16 tem” shall mean a national security system as de-
17 fined in section 11103 of title 40, United States
18 Code, or a Federal computer system that provides
19 access to personally identifiable information.

20 (2) COVERED AGENCY.—The term “covered
21 agency” means an agency that operates a covered
22 system.

23 (3) LOGICAL ACCESS CONTROL.—The term
24 “logical access control” means a process of granting

1 or denying specific requests to obtain and use infor-
2 mation and related information processing services.

3 (4) MULTI-FACTOR AUTHENTICATION.—The
4 term “multi-factor authentication” means the use of
5 not fewer than 2 authentication factors, such as the
6 following:

7 (A) Something that is known to the user,
8 such as a password or personal identification
9 number.

10 (B) An access device that is provided to
11 the user, such as a cryptographic identification
12 device or token.

13 (C) A unique biometric characteristic of
14 the user.

15 (5) PRIVILEGED USER.—The term “privileged
16 user” means a user who has access to system con-
17 trol, monitoring, or administrative functions.

18 (b) INSPECTOR GENERAL REPORTS ON COVERED
19 SYSTEMS.—

20 (1) IN GENERAL.—Not later than 240 days
21 after the date of enactment of this Act, the Inspec-
22 tor General of each covered agency shall submit to
23 the appropriate committees of jurisdiction in the
24 Senate and the House of Representatives a report,
25 which shall include information collected from the

1 covered agency for the contents described in para-
2 graph (2) regarding the Federal computer systems
3 of the covered agency.

4 (2) CONTENTS.—The report submitted by each
5 Inspector General of a covered agency under para-
6 graph (1) shall include, with respect to the covered
7 agency, the following:

8 (A) A description of the logical access poli-
9 cies and practices used by the covered agency to
10 access a covered system, including whether ap-
11 propriate standards were followed.

12 (B) A description and list of the logical ac-
13 cess controls and multi-factor authentication
14 used by the covered agency to govern access to
15 covered systems by privileged users.

16 (C) If the covered agency does not use log-
17 ical access controls or multi-factor authentica-
18 tion to access a covered system, a description of
19 the reasons for not using such logical access
20 controls or multi-factor authentication.

21 (D) A description of the following informa-
22 tion security management practices used by the
23 covered agency regarding covered systems:

24 (i) The policies and procedures fol-
25 lowed to conduct inventories of the soft-

1 ware present on the covered systems of the
2 covered agency and the licenses associated
3 with such software.

4 (ii) What capabilities the covered
5 agency utilizes to monitor and detect
6 exfiltration and other threats, including—

7 (I) data loss prevention capabili-
8 ties;

9 (II) forensics and visibility capa-
10 bilities; or

11 (III) digital rights management
12 capabilities.

13 (iii) A description of how the covered
14 agency is using the capabilities described
15 in clause (ii).

16 (iv) If the covered agency is not uti-
17 lizing capabilities described in clause (ii), a
18 description of the reasons for not utilizing
19 such capabilities.

20 (E) A description of the policies and proce-
21 dures of the covered agency with respect to en-
22 suring that entities, including contractors, that
23 provide services to the covered agency are im-
24 plementing the information security manage-
25 ment practices described in subparagraph (D).

1 (3) **EXISTING REVIEW.**—The reports required
2 under this subsection may be based in whole or in
3 part on an audit, evaluation, or report relating to
4 programs or practices of the covered agency, and
5 may be submitted as part of another report, includ-
6 ing the report required under section 3555 of title
7 44, United States Code.

8 (4) **CLASSIFIED INFORMATION.**—Reports sub-
9 mitted under this subsection shall be in unclassified
10 form, but may include a classified annex.

11 **SEC. 407. STOPPING THE FRAUDULENT SALE OF FINANCIAL**
12 **INFORMATION OF PEOPLE OF THE UNITED**
13 **STATES.**

14 Section 1029(h) of title 18, United States Code, is
15 amended by striking “title if—” and all that follows
16 through “therefrom.” and inserting “title if the offense
17 involves an access device issued, owned, managed, or con-
18 trolled by a financial institution, account issuer, credit
19 card system member, or other entity organized under the
20 laws of the United States, or any State, the District of
21 Columbia, or other territory of the United States.”.

22 **DIVISION O—OTHER MATTERS**

23 **SEC. 1. TABLE OF CONTENTS.**

24 The table of contents for this division is as follows:

 Sec. 1. Table of contents.