

114TH CONGRESS
1ST SESSION

S. 754

AN ACT

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 SECTION 1. TABLE OF CONTENTS.

2 The table of contents of this Act is as follows:

Sec. 1. 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. Conforming amendment.

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT

Sec. 201. Short title.

Sec. 202. Definitions.

Sec. 203. Improved Federal network security.

Sec. 204. Advanced internal defenses.

Sec. 205. Federal cybersecurity requirements.

Sec. 206. Assessment; reports.

Sec. 207. Termination.

Sec. 208. Identification of information systems relating to national security.

Sec. 209. 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 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. Strategy to protect critical infrastructure at greatest risk.

Sec. 408. Stopping the fraudulent sale of financial information of people of the United States.

Sec. 409. Effective period.

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 sec-
14 tion 1 of the Clayton Act (15 U.S.C. 12);

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

19 (C) includes any State law that has the
20 same intent and effect as the laws under sub-
21 paragraphs (A) and (B).

22 (3) **APPROPRIATE FEDERAL ENTITIES.**—The
23 term “appropriate Federal entities” means the fol-
24 lowing:

25 (A) The Department of Commerce.

1 (B) The Department of Defense.

2 (C) The Department of Energy.

3 (D) The Department of Homeland Secu-
4 rity.

5 (E) The Department of Justice.

6 (F) The Department of the Treasury.

7 (G) The Office of the Director of National
8 Intelligence.

9 (4) CYBERSECURITY PURPOSE.—The term “cy-
10 bersecurity purpose” means the purpose of pro-
11 tecting an information system or information that is
12 stored on, processed by, or transiting an information
13 system from a cybersecurity threat or security vul-
14 nerability.

15 (5) CYBERSECURITY THREAT.—

16 (A) IN GENERAL.—Except as provided in
17 subparagraph (B), the term “cybersecurity
18 threat” means an action, not protected by the
19 First Amendment to the Constitution of the
20 United States, on or through an information
21 system that may result in an unauthorized ef-
22 fort to adversely impact the security, avail-
23 ability, confidentiality, or integrity of an infor-
24 mation system or information that is stored on,

1 processed by, or transiting an information sys-
2 tem.

3 (B) EXCLUSION.—The term “cybersecurity
4 threat” does not include any action that solely
5 involves a violation of a consumer term of serv-
6 ice or a consumer licensing agreement.

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

10 (A) malicious reconnaissance, including
11 anomalous patterns of communications that ap-
12 pear to be transmitted for the purpose of gath-
13 ering technical information related to a cyberse-
14 curity threat or security vulnerability;

15 (B) a method of defeating a security con-
16 trol or exploitation of a security vulnerability;

17 (C) a security vulnerability, including
18 anomalous activity that appears to indicate the
19 existence of a security vulnerability;

20 (D) a method of causing a user with legiti-
21 mate access to an information system or infor-
22 mation that is stored on, processed by, or
23 transiting an information system to unwittingly
24 enable the defeat of a security control or exploi-
25 tation of a security vulnerability;

1 (E) malicious cyber command and control;

2 (F) the actual or potential harm caused by
3 an incident, including a description of the infor-
4 mation exfiltrated as a result of a particular cy-
5 bersecurity threat;

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

9 (H) any combination thereof.

10 (7) DEFENSIVE MEASURE.—

11 (A) IN GENERAL.—Except as provided in
12 subparagraph (B), the term “defensive meas-
13 ure” means an action, device, procedure, signa-
14 ture, technique, or other measure applied to an
15 information system or information that is
16 stored on, processed by, or transiting an infor-
17 mation system that detects, prevents, or miti-
18 gates a known or suspected cybersecurity threat
19 or security vulnerability.

20 (B) EXCLUSION.—The term “defensive
21 measure” does not include a measure that de-
22 stroys, renders unusable, provides unauthorized
23 access to, or substantially harms an information
24 system or data on an information system not
25 belonging to—

1 (i) the private entity operating the
2 measure; or

3 (ii) another entity or Federal entity
4 that is authorized to provide consent and
5 has provided consent to that private entity
6 for operation of such measure.

7 (8) ENTITY.—

8 (A) IN GENERAL.—Except as otherwise
9 provided in this paragraph, the term “entity”
10 means any private entity, non-Federal govern-
11 ment agency or department, or State, tribal, or
12 local government (including a political subdivi-
13 sion, department, or component thereof).

14 (B) INCLUSIONS.—The term “entity” in-
15 cludes a government agency or department of
16 the District of Columbia, the Commonwealth of
17 Puerto Rico, the Virgin Islands, Guam, Amer-
18 ican Samoa, the Northern Mariana Islands, and
19 any other territory or possession of the United
20 States.

21 (C) EXCLUSION.—The term “entity” does
22 not include a foreign power as defined in sec-
23 tion 101 of the Foreign Intelligence Surveil-
24 lance Act of 1978 (50 U.S.C. 1801).

1 (9) FEDERAL ENTITY.—The term “Federal en-
2 tity” means a department or agency of the United
3 States or any component of such department or
4 agency.

5 (10) INFORMATION SYSTEM.—The term “infor-
6 mation system”—

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

9 (B) includes industrial control systems,
10 such as supervisory control and data acquisition
11 systems, distributed control systems, and pro-
12 grammable logic controllers.

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

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

23 (13) MALICIOUS RECONNAISSANCE.—The term
24 “malicious reconnaissance” means a method for ac-
25 tively probing or passively monitoring an information

1 system for the purpose of discerning security
2 vulnerabilities of the information system, if such
3 method is associated with a known or suspected cy-
4 bersecurity threat.

5 (14) MONITOR.—The term “monitor” means to
6 acquire, identify, or scan, or to possess, information
7 that is stored on, processed by, or transiting an in-
8 formation system.

9 (15) PRIVATE ENTITY.—

10 (A) IN GENERAL.—Except as otherwise
11 provided in this paragraph, the term “private
12 entity” means any person or private group, or-
13 ganization, proprietorship, partnership, trust,
14 cooperative, corporation, or other commercial or
15 nonprofit entity, including an officer, employee,
16 or agent thereof.

17 (B) INCLUSION.—The term “private enti-
18 ty” includes a State, tribal, or local government
19 performing electric or other utility services.

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

24 (16) SECURITY CONTROL.—The term “security
25 control” means the management, operational, and

1 technical controls used to protect against an unau-
2 thORIZED effort to adversely affect the confidentiality,
3 integrity, and availability of an information system
4 or its information.

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

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

13 **SEC. 103. SHARING OF INFORMATION BY THE FEDERAL**
14 **GOVERNMENT.**

15 (a) IN GENERAL.—Consistent with the protection of
16 classified information, intelligence sources and methods,
17 and privacy and civil liberties, the Director of National
18 Intelligence, the Secretary of Homeland Security, the Sec-
19 retary of Defense, and the Attorney General, in consulta-
20 tion with the heads of the appropriate Federal entities,
21 shall develop and promulgate procedures to facilitate and
22 promote—

23 (1) the timely sharing of classified cyber threat
24 indicators in the possession of the Federal Govern-

1 ment with cleared representatives of relevant enti-
2 ties;

3 (2) the timely sharing with relevant entities of
4 cyber threat indicators or information in the posses-
5 sion of the Federal Government that may be declas-
6 sified and shared at an unclassified level;

7 (3) the sharing with relevant entities, or the
8 public if appropriate, of unclassified, including con-
9 trolled unclassified, cyber threat indicators in the
10 possession of the Federal Government;

11 (4) the sharing with entities, if appropriate, of
12 information in the possession of the Federal Govern-
13 ment about cybersecurity threats to such entities to
14 prevent or mitigate adverse effects from such cyber-
15 security 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 analysis of
19 cyber threat indicators and information in possession
20 of the Federal Government, with attention to acces-
21 sibility and implementation challenges faced by small
22 business concerns (as defined in section 3 of the
23 Small Business Act (15 U.S.C. 632)).

24 (b) DEVELOPMENT OF PROCEDURES.—

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

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

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

13 (C) include procedures for notifying, in a
14 timely manner, entities that have received a
15 cyber threat indicator from a Federal entity
16 under this title that is known or determined to
17 be in error or in contravention of the require-
18 ments of this title or another provision of Fed-
19 eral law or policy of such error or contraven-
20 tion;

21 (D) include requirements for Federal enti-
22 ties sharing cyber threat indicators or defensive
23 measures to implement and utilize security con-
24 trols to protect against unauthorized access to

1 or acquisition of such cyber threat indicators or
2 defensive measures;

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

6 (i) to review such cyber threat indi-
7 cator to assess whether such cyber threat
8 indicator contains any information that
9 such Federal entity knows at the time of
10 sharing to be personal information or in-
11 formation that identifies a specific person
12 not directly related to a cybersecurity
13 threat and remove such information; or

14 (ii) to implement and utilize a tech-
15 nical capability configured to remove any
16 personal information or information that
17 identifies a specific person not directly re-
18 lated to a cybersecurity threat; and

19 (F) include procedures for notifying, in a
20 timely manner, any United States person whose
21 personal information is known or determined to
22 have been shared by a Federal entity in viola-
23 tion of this Act.

24 (2) COORDINATION.—In developing the proce-
25 dures required under this section, the Director of

1 National Intelligence, the Secretary of Homeland Se-
2 curity, the Secretary of Defense, and the Attorney
3 General shall coordinate with appropriate Federal
4 entities, including the Small Business Administra-
5 tion and the National Laboratories (as defined in
6 section 2 of the Energy Policy Act of 2005 (42
7 U.S.C. 15801)), to ensure that effective protocols
8 are implemented that will facilitate and promote the
9 sharing of cyber threat indicators by the Federal
10 Government in a timely manner.

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

16 **SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
17 **ANALYZING, AND MITIGATING CYBERSECU-**
18 **RITY THREATS.**

19 (a) AUTHORIZATION FOR MONITORING.—

20 (1) IN GENERAL.—Notwithstanding any other
21 provision of law, a private entity may, for cybersecu-
22 rity purposes, monitor—

23 (A) an information system of such private
24 entity;

1 (B) an information system of another enti-
2 ty, upon the authorization and written consent
3 of such other entity;

4 (C) an information system of a Federal en-
5 tity, upon the authorization and written consent
6 of an authorized representative of the Federal
7 entity; and

8 (D) information that is stored on, proc-
9 essed by, or transiting an information system
10 monitored by the private entity under this para-
11 graph.

12 (2) CONSTRUCTION.—Nothing in this sub-
13 section shall be construed—

14 (A) to authorize the monitoring of an in-
15 formation system, or the use of any information
16 obtained through such monitoring, other than
17 as provided in this title; or

18 (B) to limit otherwise lawful activity.

19 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE
20 MEASURES.—

21 (1) IN GENERAL.—Notwithstanding any other
22 provision of law, a private entity may, for cybersecu-
23 rity purposes, operate a defensive measure that is
24 applied to—

1 (A) an information system of such private
2 entity in order to protect the rights or property
3 of the private entity;

4 (B) an information system of another enti-
5 ty upon written consent of such entity for oper-
6 ation of such defensive measure to protect the
7 rights or property of such entity; and

8 (C) an information system of a Federal en-
9 tity upon written consent of an authorized rep-
10 resentative of such Federal entity for operation
11 of such defensive measure to protect the rights
12 or property of the Federal Government.

13 (2) CONSTRUCTION.—Nothing in this sub-
14 section shall be construed—

15 (A) to authorize the use of a defensive
16 measure other than as provided in this sub-
17 section; or

18 (B) to limit otherwise lawful activity.

19 (c) AUTHORIZATION FOR SHARING OR RECEIVING
20 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-
21 URES.—

22 (1) IN GENERAL.—Except as provided in para-
23 graph (2) and notwithstanding any other provision
24 of law, an entity may, for a cybersecurity purpose
25 and consistent with the protection of classified infor-

1 mation, share with, or receive from, any other entity
2 or the Federal Government a cyber threat indicator
3 or defensive measure.

4 (2) **LAWFUL RESTRICTION.**—An entity receiving
5 a cyber threat indicator or defensive measure from
6 another entity or Federal entity shall comply with
7 otherwise lawful restrictions placed on the sharing or
8 use of such cyber threat indicator or defensive meas-
9 ure by the sharing entity or Federal entity.

10 (3) **CONSTRUCTION.**—Nothing in this sub-
11 section shall be construed—

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

15 (B) to limit otherwise lawful activity.

16 (d) **PROTECTION AND USE OF INFORMATION.**—

17 (1) **SECURITY OF INFORMATION.**—An entity
18 monitoring an information system, operating a de-
19 fensive measure, or providing or receiving a cyber
20 threat indicator or defensive measure under this sec-
21 tion shall implement and utilize a security control to
22 protect against unauthorized access to or acquisition
23 of such cyber threat indicator or defensive measure.

1 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
2 TION.—An entity sharing a cyber threat indicator
3 pursuant to this title shall, prior to such sharing—

4 (A) review such cyber threat indicator to
5 assess whether such cyber threat indicator con-
6 tains any information that the entity knows at
7 the time of sharing to be personal information
8 or information that identifies a specific person
9 not directly related to a cybersecurity threat
10 and remove such information; or

11 (B) implement and utilize a technical capa-
12 bility configured to remove any information
13 contained within such indicator that the entity
14 knows at the time of sharing to be personal in-
15 formation or information that identifies a spe-
16 cific person not directly related to a cybersecu-
17 rity threat.

18 (3) USE OF CYBER THREAT INDICATORS AND
19 DEFENSIVE MEASURES BY ENTITIES.—

20 (A) IN GENERAL.—Consistent with this
21 title, a cyber threat indicator or defensive meas-
22 ure shared or received under this section may,
23 for cybersecurity purposes—

1 (i) be used by an entity to monitor or
2 operate a defensive measure that is applied
3 to—

4 (I) an information system of the
5 entity; or

6 (II) an information system of an-
7 other entity or a Federal entity upon
8 the written consent of that other enti-
9 ty or that Federal entity; and

10 (ii) be otherwise used, retained, and
11 further shared by an entity subject to—

12 (I) an otherwise lawful restriction
13 placed by the sharing entity or Fed-
14 eral entity on such cyber threat indi-
15 cator or defensive measure; or

16 (II) an otherwise applicable pro-
17 vision of law.

18 (B) CONSTRUCTION.—Nothing in this
19 paragraph shall be construed to authorize the
20 use of a cyber threat indicator or defensive
21 measure other than as provided in this section.

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

24 (A) LAW ENFORCEMENT USE.—

1 (i) PRIOR WRITTEN CONSENT.—Ex-
2 cept as provided in clause (ii), a cyber
3 threat indicator shared with a State, tribal,
4 or local government under this section
5 may, with the prior written consent of the
6 entity sharing such indicator, be used by a
7 State, tribal, or local government for the
8 purpose of preventing, investigating, or
9 prosecuting any of the offenses described
10 in section 105(d)(5)(A)(vi).

11 (ii) ORAL CONSENT.—If exigent cir-
12 cumstances prevent obtaining written con-
13 sent under clause (i), such consent may be
14 provided orally with subsequent docu-
15 mentation of the consent.

16 (B) EXEMPTION FROM DISCLOSURE.—A
17 cyber threat indicator shared with a State, trib-
18 al, or local government under this section shall
19 be—

20 (i) deemed voluntarily shared informa-
21 tion; and

22 (ii) exempt from disclosure under any
23 State, tribal, or local law requiring disclo-
24 sure of information or records.

1 (C) STATE, TRIBAL, AND LOCAL REGU-
2 LATORY AUTHORITY.—

3 (i) IN GENERAL.—Except as provided
4 in clause (ii), a cyber threat indicator or
5 defensive measure shared with a State,
6 tribal, or local government under this title
7 shall not be directly used by any State,
8 tribal, or local government to regulate, in-
9 cluding an enforcement action, the lawful
10 activity of any entity, including an activity
11 relating to monitoring, operating a defen-
12 sive measure, or sharing of a cyber threat
13 indicator.

14 (ii) REGULATORY AUTHORITY SPE-
15 CIFICALLY RELATING TO PREVENTION OR
16 MITIGATION OF CYBERSECURITY
17 THREATS.—A cyber threat indicator or de-
18 fensive measure shared as described in
19 clause (i) may, consistent with a State,
20 tribal, or local government regulatory au-
21 thority specifically relating to the preven-
22 tion or mitigation of cybersecurity threats
23 to information systems, inform the devel-
24 opment or implementation of a regulation
25 relating to such information systems.

1 (e) ANTITRUST EXEMPTION.—

2 (1) IN GENERAL.—Except as provided in sec-
3 tion 108(e), it shall not be considered a violation of
4 any provision of antitrust laws for 2 or more private
5 entities to exchange or provide a cyber threat indi-
6 cator, or assistance relating to the prevention, inves-
7 tigation, or mitigation of a cybersecurity threat, for
8 cybersecurity purposes under this title.

9 (2) APPLICABILITY.—Paragraph (1) shall apply
10 only to information that is exchanged or assistance
11 provided in order to assist with—

12 (A) facilitating the prevention, investiga-
13 tion, or mitigation of a cybersecurity threat to
14 an information system or information that is
15 stored on, processed by, or transiting an infor-
16 mation system; or

17 (B) communicating or disclosing a cyber
18 threat indicator to help prevent, investigate, or
19 mitigate the effect of a cybersecurity threat to
20 an information system or information that is
21 stored on, processed by, or transiting an infor-
22 mation system.

23 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber
24 threat indicator with an entity under this title shall not

1 create a right or benefit to similar information by such
2 entity or any other entity.

3 **SEC. 105. SHARING OF CYBER THREAT INDICATORS AND**
4 **DEFENSIVE MEASURES WITH THE FEDERAL**
5 **GOVERNMENT.**

6 (a) REQUIREMENT FOR POLICIES AND PROCE-
7 DURES.—

8 (1) INTERIM POLICIES AND PROCEDURES.—Not
9 later than 60 days after the date of the enactment
10 of this Act, the Attorney General and the Secretary
11 of Homeland Security shall, in coordination with the
12 heads of the appropriate Federal entities, develop
13 and submit to Congress interim policies and proce-
14 dures relating to the receipt of cyber threat indica-
15 tors and defensive measures by the Federal Govern-
16 ment.

17 (2) FINAL POLICIES AND PROCEDURES.—Not
18 later than 180 days after the date of the enactment
19 of this Act, the Attorney General and the Secretary
20 of Homeland Security shall, in coordination with the
21 heads of the appropriate Federal entities, promul-
22 gate final policies and procedures relating to the re-
23 ceipt of cyber threat indicators and defensive meas-
24 ures by the Federal Government.

1 (3) REQUIREMENTS CONCERNING POLICIES AND
2 PROCEDURES.—Consistent with the guidelines re-
3 quired by subsection (b), the policies and procedures
4 developed and promulgated under this subsection
5 shall—

6 (A) ensure that cyber threat indicators
7 shared with the Federal Government by any en-
8 tity pursuant to section 104(c) through the
9 real-time process described in subsection (c) of
10 this section—

11 (i) are shared in an automated man-
12 ner with all of the appropriate Federal en-
13 tities;

14 (ii) are only subject to a delay, modi-
15 fication, or other action due to controls es-
16 tablished for such real-time process that
17 could impede real-time receipt by all of the
18 appropriate Federal entities when the
19 delay, modification, or other action is due
20 to controls—

21 (I) agreed upon unanimously by
22 all of the heads of the appropriate
23 Federal entities;

24 (II) carried out before any of the
25 appropriate Federal entities retains or

1 uses the cyber threat indicators or de-
2 fensive measures; and

3 (III) uniformly applied such that
4 each of the appropriate Federal enti-
5 ties is subject to the same delay,
6 modification, or other action; and

7 (iii) may be provided to other Federal
8 entities;

9 (B) ensure that cyber threat indicators
10 shared with the Federal Government by any en-
11 tity pursuant to section 104 in a manner other
12 than the real time process described in sub-
13 section (c) of this section—

14 (i) are shared as quickly as operation-
15 ally practicable with all of the appropriate
16 Federal entities;

17 (ii) are not subject to any unnecessary
18 delay, interference, or any other action
19 that could impede receipt by all of the ap-
20 propriate Federal entities; and

21 (iii) may be provided to other Federal
22 entities;

23 (C) consistent with this title, any other ap-
24 plicable provisions of law, and the fair informa-
25 tion practice principles set forth in appendix A

1 of the document entitled “National Strategy for
2 Trusted Identities in Cyberspace” and pub-
3 lished by the President in April, 2011, govern
4 the retention, use, and dissemination by the
5 Federal Government of cyber threat indicators
6 shared with the Federal Government under this
7 title, including the extent, if any, to which such
8 cyber threat indicators may be used by the Fed-
9 eral Government; and

10 (D) ensure there are—

11 (i) audit capabilities; and

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

17 (4) GUIDELINES FOR ENTITIES SHARING CYBER
18 THREAT INDICATORS WITH FEDERAL GOVERN-
19 MENT.—

20 (A) IN GENERAL.—Not later than 60 days
21 after the date of the enactment of this Act, the
22 Attorney General and the Secretary of Home-
23 land Security shall develop and make publicly
24 available guidance to assist entities and pro-

1 mote sharing of cyber threat indicators with
2 Federal entities under this title.

3 (B) CONTENTS.—The guidelines developed
4 and made publicly available under subpara-
5 graph (A) shall include guidance on the fol-
6 lowing:

7 (i) Identification of types of informa-
8 tion that would qualify as a cyber threat
9 indicator under this title that would be un-
10 likely to include personal information or in-
11 formation that identifies a specific person
12 not directly related to a cyber security
13 threat.

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

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

23 (b) PRIVACY AND CIVIL LIBERTIES.—

24 (1) GUIDELINES OF ATTORNEY GENERAL.—Not
25 later than 60 days after the date of the enactment

1 of this Act, the Attorney General shall, in coordina-
2 tion with heads of the appropriate Federal entities
3 and in consultation with officers designated under
4 section 1062 of the National Security Intelligence
5 Reform Act of 2004 (42 U.S.C. 2000ee–1), develop,
6 submit to Congress, and make available to the public
7 interim guidelines relating to privacy and civil lib-
8 erties which shall govern the receipt, retention, use,
9 and dissemination of cyber threat indicators by a
10 Federal entity obtained in connection with activities
11 authorized in this title.

12 (2) FINAL GUIDELINES.—

13 (A) IN GENERAL.—Not later than 180
14 days after the date of the enactment of this
15 Act, the Attorney General shall, in coordination
16 with heads of the appropriate Federal entities
17 and in consultation with officers designated
18 under section 1062 of the National Security In-
19 telligence Reform Act of 2004 (42 U.S.C.
20 2000ee–1) and such private entities with indus-
21 try expertise as the Attorney General considers
22 relevant, promulgate final guidelines relating to
23 privacy and civil liberties which shall govern the
24 receipt, retention, use, and dissemination of
25 cyber threat indicators by a Federal entity ob-

1 tained in connection with activities authorized
2 in this title.

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

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

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

18 (B) limit the receipt, retention, use, and
19 dissemination of cyber threat indicators con-
20 taining personal information or information
21 that identifies specific persons, including by es-
22 tablishing—

23 (i) a process for the timely destruction
24 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 or information that identifies specific
9 persons from unauthorized access or acquisi-
10 tion, including appropriate sanctions for activi-
11 ties by officers, employees, or agents of the
12 Federal Government in contravention of such
13 guidelines;

14 (D) include procedures for notifying enti-
15 ties and Federal entities if information received
16 pursuant to this section is known or determined
17 by a Federal entity receiving such information
18 not to constitute a cyber threat indicator;

19 (E) protect the confidentiality of cyber
20 threat indicators containing personal informa-
21 tion or information that identifies specific per-
22 sons to the greatest extent practicable and re-
23 quire recipients to be informed that such indica-
24 tors may only be used for purposes authorized
25 under this title; and

1 (F) include steps that may be needed so
2 that dissemination of cyber threat indicators is
3 consistent with the protection of classified and
4 other sensitive national security information.

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

7 (1) IN GENERAL.—Not later than 90 days after
8 the date of the enactment of this Act, the Secretary
9 of Homeland Security, in coordination with the
10 heads of the appropriate Federal entities, shall de-
11 velop and implement a capability and process within
12 the Department of Homeland Security that—

13 (A) shall accept from any entity in real
14 time cyber threat indicators and defensive
15 measures, pursuant to this section;

16 (B) shall, upon submittal of the certifi-
17 cation under paragraph (2) that such capability
18 and process fully and effectively operates as de-
19 scribed in such paragraph, be the process by
20 which the Federal Government receives cyber
21 threat indicators and defensive measures under
22 this title that are shared by a private entity
23 with the Federal Government through electronic
24 mail or media, an interactive form on an Inter-

1 net website, or a real time, automated process
2 between information systems except—

3 (i) consistent with section 104, com-
4 munications between a Federal entity and
5 a private entity regarding a previously
6 shared cyber threat indicator to describe
7 the relevant cybersecurity threat or develop
8 a defensive measure based on such cyber
9 threat indicator; and

10 (ii) communications by a regulated en-
11 tity with such entity's Federal regulatory
12 authority regarding a cybersecurity threat;

13 (C) ensures that all of the appropriate
14 Federal entities receive in an automated man-
15 ner such cyber threat indicators shared through
16 the real-time process within the Department of
17 Homeland Security;

18 (D) is in compliance with the policies, pro-
19 cedures, and guidelines required by this section;
20 and

21 (E) does not limit or prohibit otherwise
22 lawful disclosures of communications, records,
23 or other information, including—

1 (i) reporting of known or suspected
2 criminal activity, by an entity to any other
3 entity or a Federal entity;

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

6 (iii) providing cyber threat indicators
7 or defensive measures as part of a statu-
8 tory or authorized contractual requirement.

9 (2) CERTIFICATION.—Not later than 10 days
10 prior to the implementation of the capability and
11 process required by paragraph (1), the Secretary of
12 Homeland Security shall, in consultation with the
13 heads of the appropriate Federal entities, certify to
14 Congress whether such capability and process fully
15 and effectively operates—

16 (A) as the process by which the Federal
17 Government receives from any entity a cyber
18 threat indicator or defensive measure under this
19 title; and

20 (B) in accordance with the policies, proce-
21 dures, and guidelines developed under this sec-
22 tion.

23 (3) PUBLIC NOTICE AND ACCESS.—The Sec-
24 retary of Homeland Security shall ensure there is
25 public notice of, and access to, the capability and

1 process developed and implemented under paragraph
2 (1) so that—

3 (A) any entity may share cyber threat indi-
4 cators and defensive measures through such
5 process with the Federal Government; and

6 (B) all of the appropriate Federal entities
7 receive such cyber threat indicators and defen-
8 sive measures in real time with receipt through
9 the process within the Department of Home-
10 land Security.

11 (4) OTHER FEDERAL ENTITIES.—The process
12 developed and implemented under paragraph (1)
13 shall ensure that other Federal entities receive in a
14 timely manner any cyber threat indicators and de-
15 fensive measures shared with the Federal Govern-
16 ment through such process.

17 (5) REPORT ON DEVELOPMENT AND IMPLE-
18 MENTATION.—

19 (A) IN GENERAL.—Not later than 60 days
20 after the date of the enactment of this Act, the
21 Secretary of Homeland Security shall submit to
22 Congress a report on the development and im-
23 plementation of the capability and process re-
24 quired by paragraph (1), including a description

1 of such capability and process and the public
2 notice of, and access to, such process.

3 (B) CLASSIFIED ANNEX.—The report re-
4 quired by subparagraph (A) shall be submitted
5 in unclassified form, but may include a classi-
6 fied annex.

7 (d) INFORMATION SHARED WITH OR PROVIDED TO
8 THE FEDERAL GOVERNMENT.—

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

15 (2) PROPRIETARY INFORMATION.—Consistent
16 with section 104(c)(2), a cyber threat indicator or
17 defensive measure provided by an entity to the Fed-
18 eral Government under this title shall be considered
19 the commercial, financial, and proprietary informa-
20 tion of such entity when so designated by the origi-
21 nating entity or a third party acting in accordance
22 with the written authorization of the originating en-
23 tity.

1 (3) EXEMPTION FROM DISCLOSURE.—Cyber
2 threat indicators and defensive measures provided to
3 the Federal Government under this title shall be—

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

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

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

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

21 (A) AUTHORIZED ACTIVITIES.—Cyber
22 threat indicators and defensive measures pro-
23 vided to the Federal Government under this
24 title may be disclosed to, retained by, and used
25 by, consistent with otherwise applicable provi-

1 sions of Federal law, any Federal agency or de-
2 partment, component, officer, employee, or
3 agent of the Federal Government solely for—

4 (i) a cybersecurity purpose;

5 (ii) the purpose of identifying a cyber-
6 security threat, including the source of
7 such cybersecurity threat, or a security
8 vulnerability;

9 (iii) the purpose of identifying a cy-
10 bersecurity threat involving the use of an
11 information system by a foreign adversary
12 or terrorist;

13 (iv) the purpose of responding to, or
14 otherwise preventing or mitigating, an im-
15minent threat of death, serious bodily
16harm, or serious economic harm, including
17a terrorist act or a use of a weapon of
18mass destruction;

19 (v) the purpose of responding to, or
20 otherwise preventing or mitigating, a seri-
21ous threat to a minor, including sexual ex-
22ploitation and threats to physical safety; or

23 (vi) the purpose of preventing, inves-
24tigating, disrupting, or prosecuting an of-
25fense arising out of a threat described in

1 clause (iv) or any of the offenses listed
2 in—

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

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

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

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

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

22 (i) in accordance with the policies,
23 procedures, and guidelines required by sub-
24 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 personal
4 information or information that identifies
5 specific persons; and

6 (iii) in a manner that protects the
7 confidentiality of cyber threat indicators
8 containing personal information or infor-
9 mation that identifies a specific person.

10 (D) FEDERAL REGULATORY AUTHORITY.—

11 (i) IN GENERAL.—Except as provided
12 in clause (ii), cyber threat indicators and
13 defensive measures provided to the Federal
14 Government under this title shall not be
15 directly used by any Federal, State, tribal,
16 or local government to regulate, including
17 an enforcement action, the lawful activities
18 of any entity, including activities relating
19 to monitoring, operating defensive meas-
20 ures, or sharing cyber threat indicators.

21 (ii) EXCEPTIONS.—

22 (I) REGULATORY AUTHORITY
23 SPECIFICALLY RELATING TO PREVEN-
24 TION OR MITIGATION OF CYBERSECU-
25 RITY THREATS.—Cyber threat indica-

1 tors and defensive measures provided
2 to the Federal Government under this
3 title may, consistent with Federal or
4 State regulatory authority specifically
5 relating to the prevention or mitiga-
6 tion of cybersecurity threats to infor-
7 mation systems, inform the develop-
8 ment or implementation of regulations
9 relating to such information systems.

10 (II) PROCEDURES DEVELOPED
11 AND IMPLEMENTED UNDER THIS
12 TITLE.—Clause (i) shall not apply to
13 procedures developed and imple-
14 mented under this title.

15 **SEC. 106. PROTECTION FROM LIABILITY.**

16 (a) MONITORING OF INFORMATION SYSTEMS.—No
17 cause of action shall lie or be maintained in any court
18 against any private entity, and such action shall be
19 promptly dismissed, for the monitoring of information sys-
20 tems and information under section 104(a) that is con-
21 ducted in accordance with this title.

22 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
23 CATORS.—No cause of action shall lie or be maintained
24 in any court against any entity, and such action shall be
25 promptly dismissed, for the sharing or receipt of cyber

1 threat indicators or defensive measures under section
2 104(c) if—

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

5 (2) in a case in which a cyber threat indicator
6 or defensive measure is shared with the Federal
7 Government, the cyber threat indicator or defensive
8 measure is shared in a manner that is consistent
9 with section 105(c)(1)(B) and the sharing or receipt,
10 as the case may be, occurs after the earlier of—

11 (A) the date on which the interim policies
12 and procedures are submitted to Congress
13 under section 105(a)(1) and guidelines are sub-
14 mitted to Congress under section 105(b)(1); or

15 (B) the date that is 60 days after the date
16 of the enactment of this Act.

17 (c) CONSTRUCTION.—Nothing in this section shall be
18 construed—

19 (1) to require dismissal of a cause of action
20 against an entity that has engaged in gross neg-
21 ligence or willful misconduct in the course of con-
22 ducting activities authorized by this title; or

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

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

2 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

3 (1) IN GENERAL.—Not later than 1 year after
4 the date of the enactment of this Act, and not less
5 frequently than once every 2 years thereafter, the
6 heads of the appropriate Federal entities shall joint-
7 ly submit and the Inspector General of the Depart-
8 ment of Homeland Security, the Inspector General
9 of the Intelligence Community, the Inspector Gen-
10 eral of the Department of Justice, the Inspector
11 General of the Department of Defense, and the In-
12 spector General of the Department of Energy, in
13 consultation with the Council of Inspectors General
14 on Financial Oversight, shall jointly submit to Con-
15 gress a detailed report concerning the implementa-
16 tion of this title during—

17 (A) in the case of the first report sub-
18 mitted under this paragraph, the most recent 1-
19 year period; and

20 (B) in the case of any subsequent report
21 submitted under this paragraph, the most re-
22 cent 2-year period.

23 (2) CONTENTS.—Each report submitted under
24 paragraph (1) shall include, for the period covered
25 by the report, the following:

1 (A) An assessment of the sufficiency of the
2 policies, procedures, and guidelines required by
3 section 105 in ensuring that cyber threat indi-
4 cators are shared effectively and responsibly
5 within the Federal Government.

6 (B) An evaluation of the effectiveness of
7 real-time information sharing through the capa-
8 bility and process developed under section
9 105(c), including any impediments to such real-
10 time sharing.

11 (C) An assessment of the sufficiency of the
12 procedures developed under section 103 in en-
13 suring that cyber threat indicators in the pos-
14 session of the Federal Government are shared
15 in a timely and adequate manner with appro-
16 priate entities, or, if appropriate, are made pub-
17 licly available.

18 (D) An assessment of whether cyber threat
19 indicators have been properly classified and an
20 accounting of the number of security clearances
21 authorized by the Federal Government for the
22 purposes of this title.

23 (E) A review of the type of cyber threat in-
24 dicators shared with the appropriate Federal
25 entities under this title, including the following:

1 (i) The number of cyber threat indica-
2 tors received through the capability and
3 process developed under section 105(c).

4 (ii) The number of times that infor-
5 mation shared under this title was used by
6 a Federal entity to prosecute an offense
7 consistent with section 105(d)(5)(A).

8 (iii) The degree to which such infor-
9 mation may affect the privacy and civil lib-
10 erties of specific persons.

11 (iv) A quantitative and qualitative as-
12 sessment of the effect of the sharing of
13 such cyber threat indicators with the Fed-
14 eral Government on privacy and civil lib-
15 erties of specific persons, including the
16 number of notices that were issued with re-
17 spect to a failure to remove personal infor-
18 mation or information that identified a
19 specific person not directly related to a cy-
20 bersecurity threat in accordance with the
21 procedures required by section
22 105(b)(3)(D).

23 (v) The adequacy of any steps taken
24 by the Federal Government to reduce such
25 effect.

1 (F) A review of actions taken by the Fed-
2 eral Government based on cyber threat indica-
3 tors shared with the Federal Government under
4 this title, including the appropriateness of any
5 subsequent use or dissemination of such cyber
6 threat indicators by a Federal entity under sec-
7 tion 105.

8 (G) A description of any significant viola-
9 tions of the requirements of this title by the
10 Federal Government.

11 (H) A summary of the number and type of
12 entities that received classified cyber threat in-
13 dicators from the Federal Government under
14 this title and an evaluation of the risks and
15 benefits of sharing such cyber threat indicators.

16 (3) RECOMMENDATIONS.—Each report sub-
17 mitted under paragraph (1) may include rec-
18 ommendations for improvements or modifications to
19 the authorities and processes under this title.

20 (4) FORM OF REPORT.—Each report required
21 by paragraph (1) shall be submitted in unclassified
22 form, but may include a classified annex.

23 (b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

24 (1) BIENNIAL REPORT FROM PRIVACY AND
25 CIVIL LIBERTIES OVERSIGHT BOARD.—Not later

1 than 2 years after the date of the enactment of this
2 Act and not less frequently than once every 2 years
3 thereafter, the Privacy and Civil Liberties Oversight
4 Board shall submit to Congress and the President a
5 report providing—

6 (A) an assessment of the effect on privacy
7 and civil liberties by the type of activities car-
8 ried out under this title; and

9 (B) an assessment of the sufficiency of the
10 policies, procedures, and guidelines established
11 pursuant to section 105 in addressing concerns
12 relating to privacy and civil liberties.

13 (2) BIENNIAL REPORT OF INSPECTORS GEN-
14 ERAL.—

15 (A) IN GENERAL.—Not later than 2 years
16 after the date of the enactment of this Act and
17 not less frequently than once every 2 years
18 thereafter, the Inspector General of the Depart-
19 ment of Homeland Security, the Inspector Gen-
20 eral of the Intelligence Community, the Inspec-
21 tor General of the Department of Justice, the
22 Inspector General of the Department of De-
23 fense, and the Inspector General of the Depart-
24 ment of Energy shall, in consultation with the
25 Council of Inspectors General on Financial

1 Oversight, jointly submit to Congress a report
2 on the receipt, use, and dissemination of cyber
3 threat indicators and defensive measures that
4 have been shared with Federal entities under
5 this title.

6 (B) CONTENTS.—Each report submitted
7 under subparagraph (A) shall include the fol-
8 lowing:

9 (i) A review of the types of cyber
10 threat indicators shared with Federal enti-
11 ties.

12 (ii) A review of the actions taken by
13 Federal entities as a result of the receipt
14 of such cyber threat indicators.

15 (iii) A list of Federal entities receiving
16 such cyber threat indicators.

17 (iv) A review of the sharing of such
18 cyber threat indicators among Federal en-
19 tities to identify inappropriate barriers to
20 sharing information.

21 (3) RECOMMENDATIONS.—Each report sub-
22 mitted under this subsection may include such rec-
23 ommendations as the Privacy and Civil Liberties
24 Oversight Board, with respect to a report submitted
25 under paragraph (1), or the Inspectors General re-

1 ferred to in paragraph (2)(A), with respect to a re-
2 port submitted under paragraph (2), may have for
3 improvements or modifications to the authorities
4 under this title.

5 (4) FORM.—Each report required under this
6 subsection shall be submitted in unclassified form,
7 but may include a classified annex.

8 **SEC. 108. CONSTRUCTION AND PREEMPTION.**

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

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

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

20 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in
21 this title shall be construed to prohibit or limit the disclo-
22 sure of information protected under section 2302(b)(8) of
23 title 5, United States Code (governing disclosures of ille-
24 gality, waste, fraud, abuse, or public health or safety
25 threats), section 7211 of title 5, United States Code (gov-

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

7 (c) PROTECTION OF SOURCES AND METHODS.—
8 Nothing in this title shall be construed—

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

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

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

21 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in
22 this title shall be construed to affect any requirement
23 under any other provision of law for an entity to provide
24 information to the Federal Government.

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

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

9 (1) to limit or modify an existing information
10 sharing relationship;

11 (2) to prohibit a new information sharing rela-
12 tionship;

13 (3) to require a new information sharing rela-
14 tionship between any entity and another entity or a
15 Federal entity; or

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

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

21 (1) to amend, repeal, or supersede any current
22 or future contractual agreement, terms of service
23 agreement, or other contractual relationship between
24 any entities, or between any entity and a Federal en-
25 tity; or

1 (2) to abrogate trade secret or intellectual prop-
2 erty rights of any entity or Federal entity.

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

5 (1) to require an entity to provide information
6 to a Federal entity or another entity;

7 (2) to condition the sharing of cyber threat in-
8 dicators with an entity on such entity’s provision of
9 cyber threat indicators to a Federal entity or an-
10 other entity; or

11 (3) to condition the award of any Federal
12 grant, contract, or purchase on the provision of a
13 cyber threat indicator to a Federal entity or another
14 entity.

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

19 (j) USE AND RETENTION OF INFORMATION.—Noth-
20 ing in this title shall be construed to authorize, or to mod-
21 ify any existing authority of, a department or agency of
22 the Federal Government to retain or use any information
23 shared under this title for any use other than permitted
24 in this title.

25 (k) FEDERAL PREEMPTION.—

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

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

11 (l) REGULATORY AUTHORITY.—Nothing in this title
12 shall be construed—

13 (1) to authorize the promulgation of any regu-
14 lations not specifically authorized by this title;

15 (2) to establish or limit any regulatory author-
16 ity not specifically established or limited under this
17 title; or

18 (3) to authorize regulatory actions that would
19 duplicate or conflict with regulatory requirements,
20 mandatory standards, or related processes under an-
21 other provision of Federal law.

22 (m) AUTHORITY OF SECRETARY OF DEFENSE TO
23 RESPOND TO CYBER ATTACKS.—Nothing in this title
24 shall be construed to limit the authority of the Secretary
25 of Defense to develop, prepare, coordinate, or, when au-

1 thORIZED by the President to do so, conduct a military
2 cyber operation in response to a malicious cyber activity
3 carried out against the United States or a United States
4 person by a foreign government or an organization spon-
5 sored by a foreign government or a terrorist organization.

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

7 (a) **REPORT REQUIRED.**—Not later than 180 days
8 after the date of the enactment of this Act, the Director
9 of National Intelligence, in coordination with the heads of
10 other appropriate elements of the intelligence community,
11 shall submit to the Select Committee on Intelligence of
12 the Senate and the Permanent Select Committee on Intel-
13 ligence of the House of Representatives a report on cyber-
14 security threats, including cyber attacks, theft, and data
15 breaches.

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

18 (1) An assessment of the current intelligence
19 sharing and cooperation relationships of the United
20 States with other countries regarding cybersecurity
21 threats, including cyber attacks, theft, and data
22 breaches, directed against the United States and
23 which threaten the United States national security
24 interests and economy and intellectual property, spe-
25 cifically identifying the relative utility of such rela-

1 tionships, which elements of the intelligence commu-
2 nity participate in such relationships, and whether
3 and how such relationships could be improved.

4 (2) A list and an assessment of the countries
5 and nonstate actors that are the primary threats of
6 carrying out a cybersecurity threat, including a
7 cyber attack, theft, or data breach, against the
8 United States and which threaten the United States
9 national security, economy, and intellectual property.

10 (3) A description of the extent to which the ca-
11 pabilities of the United States Government to re-
12 spond to or prevent cybersecurity threats, including
13 cyber attacks, theft, or data breaches, directed
14 against the United States private sector are de-
15 graded by a delay in the prompt notification by pri-
16 vate entities of such threats or cyber attacks, theft,
17 and breaches.

18 (4) An assessment of additional technologies or
19 capabilities that would enhance the ability of the
20 United States to prevent and to respond to cyberse-
21 curity threats, including cyber attacks, theft, and
22 data breaches.

23 (5) An assessment of any technologies or prac-
24 tices utilized by the private sector that could be rap-

1 idly fielded to assist the intelligence community in
2 preventing and responding to cybersecurity threats.

3 (c) ADDITIONAL REPORT.—At the time the report re-
4 quired by subsection (a) is submitted, the Director of Na-
5 tional Intelligence shall submit to the Committee on For-
6 eign Relations of the Senate and the Committee on For-
7 eign Affairs of the House of Representatives a report con-
8 taining the information required by subsection (b)(2).

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

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

16 **SEC. 110. CONFORMING AMENDMENT.**

17 Section 941(c)(3) of the National Defense Authoriza-
18 tion Act for Fiscal Year 2013 (Public Law 112–239; 10
19 U.S.C. 2224 note) is amended by inserting at the end the
20 following: “The Secretary may share such information
21 with other Federal entities if such information consists of
22 cyber threat indicators and defensive measures and such
23 information is shared consistent with the policies and pro-
24 cedures promulgated by the Attorney General and the Sec-

1 retary of Homeland Security under section 105 of the Cy-
2 bersecurity Information Sharing Act of 2015.”.

3 **TITLE II—FEDERAL CYBERSECU-**
4 **RITY ENHANCEMENT**

5 **SEC. 201. SHORT TITLE.**

6 This title may be cited as the “Federal Cybersecurity
7 Enhancement Act of 2015”.

8 **SEC. 202. DEFINITIONS.**

9 In this title—

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

13 (2) the term “agency information system” has
14 the meaning given the term in section 228 of the
15 Homeland Security Act of 2002, as added by section
16 203(a);

17 (3) the term “appropriate congressional com-
18 mittees” means—

19 (A) the Committee on Homeland Security
20 and Governmental Affairs of the Senate; and

21 (B) the Committee on Homeland Security
22 of the House of Representatives;

23 (4) the terms “cybersecurity risk” and “infor-
24 mation system” have the meanings given those

1 terms in section 227 of the Homeland Security Act
2 of 2002, as so redesignated by section 203(a);

3 (5) the term “Director” means the Director of
4 the Office of Management and Budget;

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

8 (7) the term “national security system” has the
9 meaning given the term in section 11103 of title 40,
10 United States Code; and

11 (8) the term “Secretary” means the Secretary
12 of Homeland Security.

13 **SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.**

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

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

18 (2) by redesignating section 227 as subsection
19 (c) of section 228, as added by paragraph (4), and
20 adjusting the margins accordingly;

21 (3) by redesignating the second section des-
22 igned as section 226 (relating to the national cy-
23 bersecurity and communications integration center)
24 as section 227;

1 (4) by inserting after section 227, as so redesignated, the following:

3 **“SEC. 228. CYBERSECURITY PLANS.**

4 “(a) DEFINITIONS.—In this section—

5 “(1) the term ‘agency information system’
6 means an information system used or operated by an
7 agency or by another entity on behalf of an agency;

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

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

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

18 “(b) INTRUSION ASSESSMENT PLAN.—

19 “(1) REQUIREMENT.—The Secretary, in coordi-
20 nation with the Director of the Office of Manage-
21 ment and Budget, shall develop and implement an
22 intrusion assessment plan to identify and remove in-
23 truders in agency information systems.

24 “(2) EXCEPTION.—The intrusion assessment
25 plan required under paragraph (1) shall not apply to

1 the Department of Defense, a national security sys-
2 tem, or an element of the intelligence community.”;

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

6 (6) by inserting after section 229, as so redesign-
7 nated, the following:

8 **“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVEN-**
9 **TION SYSTEM.**

10 “(a) DEFINITIONS.—In this section—

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

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

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

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

22 “(b) REQUIREMENT.—

23 “(1) IN GENERAL.—Not later than 1 year after
24 the date of enactment of this section, the Secretary
25 shall deploy, operate, and maintain, to make avail-

1 able for use by any agency, with or without reim-
2 bursement—

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

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

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

17 “(c) ACTIVITIES.—In carrying out subsection (b), the
18 Secretary—

19 “(1) may access, and the head of an agency
20 may disclose to the Secretary or a private entity pro-
21 viding assistance to the Secretary under paragraph
22 (2), information transiting or traveling to or from an
23 agency information system, regardless of the location
24 from which the Secretary or a private entity pro-
25 viding assistance to the Secretary under paragraph

1 (2) accesses such information, notwithstanding any
2 other provision of law that would otherwise restrict
3 or prevent the head of an agency from disclosing
4 such information to the Secretary or a private entity
5 providing assistance to the Secretary under para-
6 graph (2);

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

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

15 “(4) shall regularly assess through operational
16 test and evaluation in real world or simulated envi-
17 ronments available advanced protective technologies
18 to improve detection and prevention capabilities, in-
19 cluding commercial and non-commercial technologies
20 and detection technologies beyond signature-based
21 detection, and utilize such technologies when appro-
22 priate;

23 “(5) shall establish a pilot to acquire, test, and
24 deploy, as rapidly as possible, technologies described
25 in paragraph (4);

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); and

5 “(7) shall ensure that—

6 “(A) activities carried out under this sec-
7 tion are reasonably necessary for the purpose of
8 protecting agency information and agency infor-
9 mation systems from a cybersecurity risk;

10 “(B) information accessed by the Secretary
11 will be retained no longer than reasonably nec-
12 essary for the purpose of protecting agency in-
13 formation and agency information systems from
14 a cybersecurity risk;

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

21 “(D) the activities are implemented pursu-
22 ant to policies and procedures governing the op-
23 eration of the intrusion detection and preven-
24 tion capabilities.

25 “(d) 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 without the consent of the
6 Department or the agency that disclosed the in-
7 formation under subsection (c)(1); or

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

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

23 “(3) RULE OF CONSTRUCTION.—Nothing in
24 paragraph (2) shall be construed to authorize an
25 Internet service provider to break a user agreement

1 with a customer without the consent of the cus-
2 tomer.

3 “(e) ATTORNEY GENERAL REVIEW.—Not later than
4 1 year after the date of enactment of this section, the At-
5 torney General shall review the policies and guidelines for
6 the program carried out under this section to ensure that
7 the policies and guidelines are consistent with applicable
8 law governing the acquisition, interception, retention, use,
9 and disclosure of communications.”.

10 (b) PRIORITIZING ADVANCED SECURITY TOOLS.—
11 The Director and the Secretary, in consultation with ap-
12 propriate agencies, shall—

13 (1) review and update governmentwide policies
14 and programs to ensure appropriate prioritization
15 and use of network security monitoring tools within
16 agency networks; and

17 (2) brief appropriate congressional committees
18 on such prioritization and use.

19 (c) AGENCY RESPONSIBILITIES.—

20 (1) IN GENERAL.—Except as provided in para-
21 graph (2)—

22 (A) not later than 1 year after the date of
23 enactment of this Act or 2 months after the
24 date on which the Secretary makes available the
25 intrusion detection and prevention capabilities

1 under section 230(b)(1) of the Homeland Security
2 Act of 2002, as added by subsection (a),
3 whichever is later, the head of each agency shall
4 apply and continue to utilize the capabilities to
5 all information traveling between an agency in-
6 formation system and any information system
7 other than an agency information system; and

8 (B) not later than 6 months after the date
9 on which the Secretary makes available im-
10 provements to the intrusion detection and pre-
11 vention capabilities pursuant to section
12 230(b)(2) of the Homeland Security Act of
13 2002, as added by subsection (a), the head of
14 each agency shall apply and continue to utilize
15 the improved intrusion detection and prevention
16 capabilities.

17 (2) EXCEPTION.—The requirements under
18 paragraph (1) shall not apply to the Department of
19 Defense, a national security system, or an element
20 of the intelligence community.

21 (3) DEFINITION.—In this subsection only, the
22 term “agency information system” means an infor-
23 mation system owned or operated by an agency.

24 (4) RULE OF CONSTRUCTION.—Nothing in this
25 subsection shall be construed to limit an agency

1 from applying the intrusion detection and prevention
2 capabilities under section 230(b)(1) of the Homeland
3 Security Act of 2002, as added by subsection (a), at
4 the discretion of the head of the agency or as pro-
5 vided in relevant policies, directives, and guidelines.

6 (d) TABLE OF CONTENTS AMENDMENT.—The table
7 of contents in section 1(b) of the Homeland Security Act
8 of 2002 (6 U.S.C. 101 note) is amended by striking the
9 items relating to the first section designated as section
10 226, the second section designated as section 226 (relating
11 to the national cybersecurity and communications integra-
12 tion center), section 227, and section 228 and inserting
13 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.”.

14 **SEC. 204. ADVANCED INTERNAL DEFENSES.**

15 (a) ADVANCED NETWORK SECURITY TOOLS.—

16 (1) IN GENERAL.—The Secretary shall include
17 in the Continuous Diagnostics and Mitigation Pro-
18 gram advanced network security tools to improve
19 visibility of network activity, including through the
20 use of commercial and free or open source tools, to
21 detect and mitigate intrusions and anomalous activ-
22 ity.

1 (2) DEVELOPMENT OF PLAN.—The Director
2 shall develop and implement a plan to ensure that
3 each agency utilizes advanced network security tools,
4 including those described in paragraph (1), to detect
5 and mitigate intrusions and anomalous activity.

6 (b) IMPROVED METRICS.—The Secretary, in collabo-
7 ration with the Director, shall review and update the
8 metrics used to measure security under section 3554 of
9 title 44, United States Code, to include measures of intru-
10 sion and incident detection and response times.

11 (c) TRANSPARENCY AND ACCOUNTABILITY.—The Di-
12 rector, in consultation with the Secretary, shall increase
13 transparency to the public on agency cybersecurity pos-
14 ture, including by increasing the number of metrics avail-
15 able on Federal Government performance websites and, to
16 the greatest extent practicable, displaying metrics for de-
17 partment components, small agencies, and micro agencies.

18 (d) MAINTENANCE OF TECHNOLOGIES.—Section
19 3553(b)(6)(B) of title 44, United States Code, is amended
20 by inserting “, operating, and maintaining” after “deploy-
21 ing”.

22 (e) EXCEPTION.—The requirements under this sec-
23 tion shall not apply to the Department of Defense, a na-
24 tional security system, or an element of the intelligence
25 community.

1 **SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.**

2 (a) IMPLEMENTATION OF FEDERAL CYBERSECURITY
3 STANDARDS.—Consistent with section 3553 of title 44,
4 United States Code, the Secretary, in consultation with
5 the Director, shall exercise the authority to issue binding
6 operational directives to assist the Director in ensuring
7 timely agency adoption of and compliance with policies
8 and standards promulgated under section 11331 of title
9 40, United States Code, for securing agency information
10 systems.

11 (b) CYBERSECURITY REQUIREMENTS AT AGEN-
12 CIES.—

13 (1) IN GENERAL.—Consistent with policies,
14 standards, guidelines, and directives on information
15 security under subchapter II of chapter 35 of title
16 44, United States Code, and the standards and
17 guidelines promulgated under section 11331 of title
18 40, United States Code, and except as provided in
19 paragraph (2), not later than 1 year after the date
20 of the enactment of this Act, the head of each agen-
21 cy shall—

22 (A) identify sensitive and mission critical
23 data stored by the agency consistent with the
24 inventory required under the first subsection (c)
25 (relating to the inventory of major information
26 systems) and the second subsection (c) (relating

1 to the inventory of information systems) of sec-
2 tion 3505 of title 44, United States Code;

3 (B) assess access controls to the data de-
4 scribed in subparagraph (A), the need for read-
5 ily accessible storage of the data, and individ-
6 uals' need to access the data;

7 (C) encrypt or otherwise render indecipher-
8 able to unauthorized users the data described in
9 subparagraph (A) that is stored on or
10 transiting agency information systems;

11 (D) implement a single sign-on trusted
12 identity platform for individuals accessing each
13 public website of the agency that requires user
14 authentication, as developed by the Adminis-
15 trator of General Services in collaboration with
16 the Secretary; and

17 (E) implement identity management con-
18 sistent with section 504 of the Cybersecurity
19 Enhancement Act of 2014 (Public Law 113-
20 274; 15 U.S.C. 7464), including multi-factor
21 authentication, for—

22 (i) remote access to an agency infor-
23 mation system; and

1 (ii) each user account with elevated
2 privileges on an agency information sys-
3 tem.

4 (2) EXCEPTION.—The requirements under
5 paragraph (1) shall not apply to an agency informa-
6 tion system for which—

7 (A) the head of the agency has personally
8 certified to the Director with particularity
9 that—

10 (i) operational requirements articu-
11 lated in the certification and related to the
12 agency information system would make it
13 excessively burdensome to implement the
14 cybersecurity requirement;

15 (ii) the cybersecurity requirement is
16 not necessary to secure the agency infor-
17 mation system or agency information
18 stored on or transiting it; and

19 (iii) the agency has taken all nec-
20 essary steps to secure the agency informa-
21 tion system and agency information stored
22 on or transiting it; and

23 (B) the head of the agency or the designee
24 of the head of the agency has submitted the
25 certification described in subparagraph (A) to

1 the appropriate congressional committees and
2 the agency’s authorizing committees.

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

16 (c) EXCEPTION.—The requirements under this sec-
17 tion shall not apply to the Department of Defense, a na-
18 tional security system, or an element of the intelligence
19 community.

20 **SEC. 206. ASSESSMENT; REPORTS.**

21 (a) DEFINITIONS.—In this section—

22 (1) the term “intrusion assessments” means ac-
23 tions taken under the intrusion assessment plan to
24 identify and remove intruders in agency information
25 systems;

1 (2) the term “intrusion assessment plan”
2 means the plan required under section 228(b)(1) of
3 the Homeland Security Act of 2002, as added by
4 section 203(a) of this Act; and

5 (3) the term “intrusion detection and preven-
6 tion capabilities” means the capabilities required
7 under section 230(b) of the Homeland Security Act
8 of 2002, as added by section 203(a) of this Act.

9 (b) THIRD PARTY ASSESSMENT.—Not later than 3
10 years after the date of enactment of this Act, the Govern-
11 ment Accountability Office shall conduct a study and pub-
12 lish a report on the effectiveness of the approach and
13 strategy of the Federal Government to securing agency in-
14 formation systems, including the intrusion detection and
15 prevention capabilities and the intrusion assessment plan.

16 (c) REPORTS TO CONGRESS.—

17 (1) INTRUSION DETECTION AND PREVENTION
18 CAPABILITIES.—

19 (A) SECRETARY OF HOMELAND SECURITY
20 REPORT.—Not later than 6 months after the
21 date of enactment of this Act, and annually
22 thereafter, the Secretary shall submit to the ap-
23 propriate congressional committees a report on
24 the status of implementation of the intrusion

1 detection and prevention capabilities, includ-
2 ing—

3 (i) a description of privacy controls;

4 (ii) a description of the technologies
5 and capabilities utilized to detect cyberse-
6 curity risks in network traffic, including
7 the extent to which those technologies and
8 capabilities include existing commercial
9 and non-commercial technologies;

10 (iii) a description of the technologies
11 and capabilities utilized to prevent network
12 traffic associated with cybersecurity risks
13 from transiting or traveling to or from
14 agency information systems, including the
15 extent to which those technologies and ca-
16 pabilities include existing commercial and
17 non-commercial technologies;

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

1 (v) the number of instances in which
2 the intrusion detection and prevention ca-
3 pabilities detected a cybersecurity risk in
4 network traffic transiting or traveling to or
5 from agency information systems and the
6 number of times the intrusion detection
7 and prevention capabilities blocked net-
8 work traffic associated with cybersecurity
9 risk; and

10 (vi) a description of the pilot estab-
11 lished under section 230(e)(5) of the
12 Homeland Security Act of 2002, as added
13 by section 203(a) of this Act, including the
14 number of new technologies tested and the
15 number of participating agencies.

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

24 (i) a list of each agency and the de-
25 gree to which each agency has applied the

1 intrusion detection and prevention capabili-
2 ties to an agency information system; and

3 (ii) a list by agency of—

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

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

22 (2) OMB REPORT ON DEVELOPMENT AND IM-
23 PLEMENTATION OF INTRUSION ASSESSMENT PLAN,
24 ADVANCED INTERNAL DEFENSES, AND FEDERAL CY-

1 BERSECURITY BEST PRACTICES.—The Director
2 shall—

3 (A) not later than 6 months after the date
4 of enactment of this Act, and 30 days after any
5 update thereto, submit the intrusion assessment
6 plan to the appropriate congressional commit-
7 tees;

8 (B) not later than 1 year after the date of
9 enactment of this Act, and annually thereafter,
10 submit to Congress, as part of the report re-
11 quired under section 3553(c) of title 44, United
12 States Code—

13 (i) a description of the implementation
14 of the intrusion assessment plan;

15 (ii) the findings of the intrusion as-
16 sessments conducted pursuant to the intru-
17 sion assessment plan;

18 (iii) advanced network security tools
19 included in the Continuous Diagnostics
20 and Mitigation Program pursuant to sec-
21 tion 204(a)(1);

22 (iv) the results of the assessment of
23 the Secretary of best practices for Federal
24 cybersecurity pursuant to section 205(a);
25 and

1 (v) a list by agency of compliance with
2 the requirements of section 205(b); and

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

6 (i) a copy of the plan developed pursu-
7 ant to section 204(a)(2); and

8 (ii) the improved metrics developed
9 pursuant to section 204(b).

10 **SEC. 207. TERMINATION.**

11 (a) IN GENERAL.—The authority provided under sec-
12 tion 230 of the Homeland Security Act of 2002, as added
13 by section 203(a) of this Act, and the reporting require-
14 ments under section 206(c) shall terminate on the date
15 that is 7 years after the date of enactment of this Act.

16 (b) RULE OF CONSTRUCTION.—Nothing in sub-
17 section (a) shall be construed to affect the limitation of
18 liability of a private entity for assistance provided to the
19 Secretary under section 230(d)(2) of the Homeland Secu-
20 rity Act of 2002, as added by section 203(a) of this Act,
21 if such assistance was rendered before the termination
22 date under subsection (a) or otherwise during a period in
23 which the assistance was authorized.

1 **SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RE-**
2 **LATING TO NATIONAL SECURITY.**

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

6 (1) the Director of National Intelligence and
7 the Director of the Office of Management and Budg-
8 et, in coordination with the heads of other agencies,
9 shall—

10 (A) identify all unclassified information
11 systems that provide access to information that
12 may provide an adversary with the ability to de-
13 rive information that would otherwise be consid-
14 ered classified;

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

18 (C) assess the cost and impact on the mis-
19 sion carried out by each agency that owns an
20 unclassified information system identified in
21 subparagraph (A) if the system were to be sub-
22 sequently designated as a national security sys-
23 tem; and

24 (2) the Director of National Intelligence and
25 the Director of the Office of Management and Budg-
26 et shall submit to the appropriate congressional com-

1 mittees, the Select Committee on Intelligence of the
2 Senate, and the Permanent Select Committee on In-
3 telligence of the House of Representatives a report
4 that includes the findings under paragraph (1).

5 (b) FORM.—The report submitted under subsection
6 (a)(2) shall be in unclassified form, and shall include a
7 classified annex.

8 (c) EXCEPTION.—The requirements under subsection
9 (a)(1) shall not apply to the Department of Defense, a
10 national security system, or an element of the intelligence
11 community.

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

15 **SEC. 209. DIRECTION TO AGENCIES.**

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

19 “(h) DIRECTION TO AGENCIES.—

20 “(1) AUTHORITY.—

21 “(A) IN GENERAL.—Subject to subpara-
22 graph (B), in response to a known or reason-
23 ably suspected information security threat, vul-
24 nerability, or incident that represents a sub-
25 stantial threat to the information security of an

1 agency, the Secretary may issue an emergency
2 directive to the head of an agency to take any
3 lawful action with respect to the operation of
4 the information system, including such systems
5 used or operated by another entity on behalf of
6 an agency, that collects, processes, stores,
7 transmits, disseminates, or otherwise maintains
8 agency information, for the purpose of pro-
9 tecting the information system from, or miti-
10 gating, an information security threat.

11 “(B) EXCEPTION.—The authorities of the
12 Secretary under this subsection shall not apply
13 to a system described subsection (d) or to a sys-
14 tem described in paragraph (2) or (3) of sub-
15 section (e).

16 “(2) PROCEDURES FOR USE OF AUTHORITY.—
17 The Secretary shall—

18 “(A) in coordination with the Director, es-
19 tablish procedures governing the circumstances
20 under which a directive may be issued under
21 this subsection, which shall include—

22 “(i) thresholds and other criteria;

23 “(ii) privacy and civil liberties protec-
24 tions; and

1 “(iii) providing notice to potentially
2 affected third parties;

3 “(B) specify the reasons for the required
4 action and the duration of the directive;

5 “(C) minimize the impact of a directive
6 under this subsection by—

7 “(i) adopting the least intrusive
8 means possible under the circumstances to
9 secure the agency information systems;
10 and

11 “(ii) limiting directives to the shortest
12 period practicable;

13 “(D) notify the Director and the head of
14 any affected agency immediately upon the
15 issuance of a directive under this subsection;

16 “(E) consult with the Director of the Na-
17 tional Institute of Standards and Technology
18 regarding any directive under this subsection
19 that implements standards and guidelines devel-
20 oped by the National Institute of Standards
21 and Technology;

22 “(F) ensure that directives issued under
23 this subsection do not conflict with the stand-
24 ards and guidelines issued under section 11331
25 of title 40;

1 “(G) consider any applicable standards or
2 guidelines developed by the National Institute
3 of Standards and issued by the Secretary of
4 Commerce under section 11331 of title 40; and

5 “(H) not later than February 1 of each
6 year, submit to the appropriate congressional
7 committees a report regarding the specific ac-
8 tions the Secretary has taken pursuant to para-
9 graph (1)(A).

10 “(3) IMMINENT THREATS.—

11 “(A) IN GENERAL.—Notwithstanding sec-
12 tion 3554, the Secretary may authorize the in-
13 trusion detection and prevention capabilities
14 under section 230(b)(1) of the Homeland Secu-
15 rity Act of 2002 for the purpose of ensuring the
16 security of agency information systems, if—

17 “(i) the Secretary determines there is
18 an imminent threat to agency information
19 systems;

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

24 “(iii) the Secretary determines the
25 risk posed by the imminent threat out-

1 weighs any adverse consequences reason-
2 ably expected to result from the use of pro-
3 tective capabilities under the control of the
4 Secretary;

5 “(iv) the Secretary provides prior no-
6 tice to the Director, and the head and chief
7 information officer (or equivalent official)
8 of each agency to which specific actions
9 will be taken pursuant to subparagraph
10 (A), and notifies the appropriate congress-
11 sional committees and authorizing commit-
12 tees of each such agencies within seven
13 days of taking an action under this sub-
14 section of—

15 “(I) any action taken under this
16 subsection; and

17 “(II) the reasons for and dura-
18 tion and nature of the action;

19 “(v) the action of the Secretary is
20 consistent with applicable law; and

21 “(vi) the Secretary authorizes the use
22 of protective capabilities in accordance
23 with the advance procedures established
24 under subparagraph (C).

1 “(B) LIMITATION ON DELEGATION.—The
2 authority under this subsection may not be del-
3 egated by the Secretary.

4 “(C) ADVANCE PROCEDURES.—The Sec-
5 retary shall, in coordination with the Director,
6 and in consultation with the heads of Federal
7 agencies, establish procedures governing the cir-
8 cumstances under which the Secretary may au-
9 thorize the use of protective capabilities sub-
10 paragraph (A). The Secretary shall submit the
11 procedures to Congress.

12 “(4) LIMITATION.—The Secretary may direct
13 or authorize lawful action or protective capability
14 under this subsection only to—

15 “(A) protect agency information from un-
16 authorized access, use, disclosure, disruption,
17 modification, or destruction; or

18 “(B) require the remediation of or protect
19 against identified information security risks
20 with respect to—

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

23 “(ii) that portion of an information
24 system used or operated by an agency or

1 by a contractor of an agency or other orga-
2 nization on behalf of an agency.

3 “(i) ANNUAL REPORT TO CONGRESS.—Not later
4 than February 1 of each year, the Director shall submit
5 to the appropriate congressional committees a report re-
6 garding the specific actions the Director has taken pursu-
7 ant to subsection (a)(5), including any actions taken pur-
8 suant to section 11303(b)(5) of title 40.

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

12 “(1) the Committee on Appropriations and the
13 Committee on Homeland Security and Governmental
14 Affairs of the Senate; and

15 “(2) the Committee on Appropriations, the
16 Committee on Homeland Security, the Committee on
17 Oversight and Government Reform, and the Com-
18 mittee on Science, Space, and Technology of the
19 House of Representatives.”.

20 (b) CONFORMING AMENDMENT.—Section
21 3554(a)(1)(B) of title 44, United States Code, is amend-
22 ed—

23 (1) in clause (iii), by striking “and” at the end;

24 and

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

1 “(v) emergency directives issued by
2 the Secretary under section 3553(h); and”.

3 **TITLE III—FEDERAL CYBERSE-**
4 **CURITY WORKFORCE ASSESS-**
5 **MENT**

6 **SEC. 301. SHORT TITLE.**

7 This title may be cited as the “Federal Cybersecurity
8 Workforce Assessment Act of 2015”.

9 **SEC. 302. DEFINITIONS.**

10 In this title:

11 (1) APPROPRIATE CONGRESSIONAL COMMIT-
12 TEES.—The term “appropriate congressional com-
13 mittees” means—

14 (A) the Committee on Armed Services of
15 the Senate;

16 (B) the Committee on Homeland Security
17 and Governmental Affairs of the Senate;

18 (C) the Select Committee on Intelligence of
19 the Senate;

20 (D) the Committee on Commerce, Science,
21 and Transportation of the Senate;

22 (E) the Committee on Armed Services in
23 the House of Representatives;

24 (F) the Committee on Homeland Security
25 of the House of Representatives;

1 (G) the Committee on Oversight and Gov-
2 ernment Reform of the House of Representa-
3 tives; and

4 (H) the Permanent Select Committee on
5 Intelligence of the House of Representatives.

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

8 (3) ROLES.—The term “roles” has the meaning
9 given the term in the National Initiative for Cyber-
10 security Education’s Cybersecurity Workforce
11 Framework.

12 **SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEAS-**
13 **UREMENT INITIATIVE.**

14 (a) IN GENERAL.—The head of each Federal agency
15 shall—

16 (1) identify all positions within the agency that
17 require the performance of cybersecurity or other
18 cyber-related functions; and

19 (2) assign the corresponding employment code,
20 which shall be added to the National Initiative for
21 Cybersecurity Education’s National Cybersecurity
22 Workforce Framework, in accordance with sub-
23 section (b).

24 (b) EMPLOYMENT CODES.—

25 (1) PROCEDURES.—

1 (A) CODING STRUCTURE.—Not later than
2 180 days after the date of the enactment of this
3 Act, the Secretary of Commerce, acting through
4 the National Institute of Standards and Tech-
5 nology, shall update the National Initiative for
6 Cybersecurity Education’s Cybersecurity Work-
7 force Framework to include a corresponding
8 coding structure.

9 (B) IDENTIFICATION OF CIVILIAN CYBER
10 PERSONNEL.—Not later than 9 months after
11 the date of enactment of this Act, the Director,
12 in coordination with the Director of the Na-
13 tional Institute of Standards and Technology
14 and the Director of National Intelligence, shall
15 establish procedures to implement the National
16 Initiative for Cybersecurity Education’s coding
17 structure to identify all Federal civilian posi-
18 tions that require the performance of informa-
19 tion technology, cybersecurity, or other cyber-
20 related functions.

21 (C) IDENTIFICATION OF NONCIVILIAN
22 CYBER PERSONNEL.—Not later than 18 months
23 after the date of enactment of this Act, the Sec-
24 retary of Defense shall establish procedures to
25 implement the National Initiative for Cyberse-

1 curity Education’s coding structure to identify
2 all Federal noncivilian positions that require the
3 performance of information technology, cyberse-
4 curity, or other cyber-related functions.

5 (D) BASELINE ASSESSMENT OF EXISTING
6 CYBERSECURITY WORKFORCE.—Not later than
7 3 months after the date on which the proce-
8 dures are developed under subparagraphs (B)
9 and (C), respectively, the head of each Federal
10 agency shall submit to the appropriate congres-
11 sional committees of jurisdiction a report that
12 identifies—

13 (i) the percentage of personnel with
14 information technology, cybersecurity, or
15 other cyber-related job functions who cur-
16 rently hold the appropriate industry-recog-
17 nized certifications as identified in the Na-
18 tional Initiative for Cybersecurity Edu-
19 cation’s Cybersecurity Workforce Frame-
20 work;

21 (ii) the level of preparedness of other
22 civilian and noncivilian cyber personnel
23 without existing credentials to take certifi-
24 cation exams; and

1 (iii) a strategy for mitigating any
2 gaps identified in clause (i) or (ii) with the
3 appropriate training and certification for
4 existing personnel.

5 (E) PROCEDURES FOR ASSIGNING
6 CODES.—Not later than 3 months after the
7 date on which the procedures are developed
8 under subparagraphs (B) and (C), respectively,
9 the head of each Federal agency shall establish
10 procedures—

11 (i) to identify all encumbered and va-
12 cant positions with information technology,
13 cybersecurity, or other cyber-related func-
14 tions (as defined in the National Initiative
15 for Cybersecurity Education’s coding struc-
16 ture); and

17 (ii) to assign the appropriate employ-
18 ment code to each such position, using
19 agreed standards and definitions.

20 (2) CODE ASSIGNMENTS.—Not later than 1
21 year after the date after the procedures are estab-
22 lished under paragraph (1)(E), the head of each
23 Federal agency shall complete assignment of the ap-
24 propriate employment code to each position within

1 the agency with information technology, cybersecu-
2 rity, or other cyber-related functions.

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

7 **SEC. 304. IDENTIFICATION OF CYBER-RELATED ROLES OF**
8 **CRITICAL NEED.**

9 (a) IN GENERAL.—Beginning not later than 1 year
10 after the date on which the employment codes are assigned
11 to employees pursuant to section 203(b)(2), and annually
12 through 2022, the head of each Federal agency, in con-
13 sultation with the Director, the Director of the National
14 Institute of Standards and Technology, and the Secretary
15 of Homeland Security, shall—

16 (1) identify information technology, cybersecu-
17 rity, or other cyber-related roles of critical need in
18 the agency’s workforce; and

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

20 (A) describes the information technology,
21 cybersecurity, or other cyber-related roles iden-
22 tified under paragraph (1); and

23 (B) substantiates the critical need designa-
24 tions.

1 (b) GUIDANCE.—The Director shall provide Federal
2 agencies with timely guidance for identifying information
3 technology, cybersecurity, or other cyber-related roles of
4 critical need, including—

5 (1) current information technology, cybersecu-
6 rity, and other cyber-related roles with acute skill
7 shortages; and

8 (2) information technology, cybersecurity, or
9 other cyber-related roles with emerging skill short-
10 ages.

11 (c) CYBERSECURITY NEEDS REPORT.—Not later
12 than 2 years after the date of the enactment of this Act,
13 the Director, in consultation with the Secretary of Home-
14 land Security, shall—

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

18 (2) submit a progress report on the implemen-
19 tation of this section to the appropriate congres-
20 sional committees.

21 **SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS**
22 **REPORTS.**

23 The Comptroller General of the United States shall—

24 (1) analyze and monitor the implementation of
25 sections 303 and 304; and

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

5 **TITLE IV—OTHER CYBER**
6 **MATTERS**

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

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

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

15 (2) submit an unclassified report to Congress,
16 with a classified annex if necessary, that contains
17 the findings of such study, the recommendations de-
18 veloped under paragraph (3) of subsection (b), the
19 deficiencies, if any, identified under (4) of such sub-
20 section, and the plan developed under paragraph (5)
21 of such subsection.

22 (b) **MATTERS STUDIED.**—In carrying out the study
23 under subsection (a)(1), the Secretary, in consultation
24 with the Director of the National Institute of Standards
25 and Technology, shall—

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

5 (2) assess the effect such threats may have on
6 the cybersecurity of the information systems and
7 networks of the Federal Government (except for na-
8 tional security systems or the information systems
9 and networks of the Department of Defense and the
10 intelligence community);

11 (3) develop recommendations for addressing
12 such threats based on industry standards and best
13 practices;

14 (4) identify any deficiencies in the current au-
15 thorities of the Secretary that may inhibit the ability
16 of the Secretary to address mobile device security
17 throughout the Federal Government (except for na-
18 tional security systems and the information systems
19 and networks of the Department of Defense and in-
20 telligence community); and

21 (5) develop a plan for accelerated adoption of
22 secure mobile device technology by the Department
23 of Homeland Security.

24 (c) INTELLIGENCE COMMUNITY DEFINED.—In this
25 section, the term “intelligence community” has the mean-

1 ing given such term in section 3 of the National Security
2 Act of 1947 (50 U.S.C. 3003).

3 **SEC. 402. DEPARTMENT OF STATE INTERNATIONAL CYBER-**
4 **SPACE POLICY STRATEGY.**

5 (a) IN GENERAL.—Not later than 90 days after the
6 date of the enactment of this Act, the Secretary of State
7 shall produce a comprehensive strategy relating to United
8 States international policy with regard to cyberspace.

9 (b) ELEMENTS.—The strategy required by subsection
10 (a) shall include the following:

11 (1) A review of actions and activities under-
12 taken by the Secretary of State to date to support
13 the goal of the President’s International Strategy for
14 Cyberspace, released in May 2011, to “work inter-
15 nationally to promote an open, interoperable, secure,
16 and reliable information and communications infra-
17 structure that supports international trade and com-
18 merce, strengthens international security, and fos-
19 ters free expression and innovation.”.

20 (2) A plan of action to guide the diplomacy of
21 the Secretary of State, with regard to foreign coun-
22 tries, including conducting bilateral and multilateral
23 activities to develop the norms of responsible inter-
24 national behavior in cyberspace, and status review of

1 existing discussions in multilateral fora to obtain
2 agreements on international norms in cyberspace.

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

7 (4) A detailed description of threats to United
8 States national security in cyberspace from foreign
9 countries, state-sponsored actors, and private actors
10 to Federal and private sector infrastructure of the
11 United States, intellectual property in the United
12 States, and the privacy of citizens of the United
13 States.

14 (5) A review of policy tools available to the
15 President to deter foreign countries, state-sponsored
16 actors, and private actors, including those outlined
17 in Executive Order 13694, released on April 1,
18 2015.

19 (6) A review of resources required by the Sec-
20 retary, including the Office of the Coordinator for
21 Cyber Issues, to conduct activities to build respon-
22 sible norms of international cyber behavior.

23 (c) CONSULTATION.—In preparing the strategy re-
24 quired by subsection (a), the Secretary of State shall con-
25 sult, as appropriate, with other agencies and departments

1 of the United States and the private sector and nongovern-
2 mental organizations in the United States with recognized
3 credentials and expertise in foreign policy, national secu-
4 rity, and cybersecurity.

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

8 (e) AVAILABILITY OF INFORMATION.—The Secretary
9 of State shall—

10 (1) make the strategy required in subsection (a)
11 available the public; and

12 (2) brief the Committee on Foreign Relations of
13 the Senate and the Committee on Foreign Affairs of
14 the House of Representatives on the strategy, in-
15 cluding any material contained in a classified annex.

16 **SEC. 403. APPREHENSION AND PROSECUTION OF INTER-**
17 **NATIONAL CYBER CRIMINALS.**

18 (a) INTERNATIONAL CYBER CRIMINAL DEFINED.—
19 In this section, the term “international cyber criminal”
20 means an individual—

21 (1) who is believed to have committed a
22 cybercrime or intellectual property crime against the
23 interests of the United States or the citizens of the
24 United States; and

25 (2) for whom—

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

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

6 (b) CONSULTATIONS FOR NONCOOPERATION.—The
7 Secretary of State, or designee, shall consult with the ap-
8 propriate government official of each country from which
9 extradition is not likely due to the lack of an extradition
10 treaty with the United States or other reasons, in which
11 one or more international cyber criminals are physically
12 present, to determine what actions the government of such
13 country has taken—

14 (1) to apprehend and prosecute such criminals;
15 and

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

19 (c) ANNUAL REPORT.—

20 (1) IN GENERAL.—The Secretary of State shall
21 submit to the appropriate congressional committees
22 an annual report that includes—

23 (A) the number of international cyber
24 criminals located in other countries,
25 disaggregated by country, and indicating from

1 which countries extradition is not likely due to
2 the lack of an extradition treaty with the
3 United States or other reasons;

4 (B) the nature and number of significant
5 discussions by an official of the Department of
6 State on ways to thwart or prosecute inter-
7 national cyber criminals with an official of an-
8 other country, including the name of each such
9 country; and

10 (C) for each international cyber criminal
11 who was extradited to the United States during
12 the most recently completed calendar year—

13 (i) his or her name;

14 (ii) the crimes for which he or she was
15 charged;

16 (iii) his or her previous country of res-
17 idence; and

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

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

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

1 (A) the Committee on Foreign Relations,
2 the Committee on Appropriations, the Com-
3 mittee on Homeland Security and Govern-
4 mental Affairs, the Committee on Banking,
5 Housing, and Urban Affairs, the Select Com-
6 mittee on Intelligence, and the Committee on
7 the Judiciary of the Senate; and

8 (B) the Committee on Foreign Affairs, the
9 Committee on Appropriations, the Committee
10 on Homeland Security, the Committee on Fi-
11 nancial Services, the Permanent Select Com-
12 mittee on Intelligence, and the Committee on
13 the Judiciary of the House of Representatives.

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

15 (a) COLLECTION OF DATA.—Not later than 90 days
16 after the date of enactment of this Act, the Secretary of
17 Homeland Security, acting through the National Cyberse-
18 curity and Communications Integration Center, in coordi-
19 nation with appropriate Federal entities and the Director
20 for Emergency Communications, shall establish a process
21 by which a Statewide Interoperability Coordinator may re-
22 port data on any cybersecurity risk or incident involving
23 any information system or network used by emergency re-
24 sponse providers (as defined in section 2 of the Homeland
25 Security Act of 2002 (6 U.S.C. 101)) within the State.

1 (b) ANALYSIS OF DATA.—Not later than 1 year after
2 the date of enactment of this Act, the Secretary of Home-
3 land Security, acting through the Director of the National
4 Cybersecurity and Communications Integration Center, in
5 coordination with appropriate entities and the Director for
6 Emergency Communications, and in consultation with the
7 Director of the National Institute of Standards and Tech-
8 nology, shall conduct integration and analysis of the data
9 reported under subsection (a) to develop information and
10 recommendations on security and resilience measures for
11 any information system or network used by State emer-
12 gency response providers.

13 (c) BEST PRACTICES.—

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

24 (2) REPORT.—The Director of the National In-
25 stitute of Standards and Technology shall submit a

1 report to Congress on the methods developed under
2 paragraph (1) and shall make such report publically
3 available on the website of the National Institute of
4 Standards and Technology.

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

7 (1) require a State to report data under sub-
8 section (a); or

9 (2) require an entity to—

10 (A) adopt a recommended measure devel-
11 oped under subsection (b); or

12 (B) follow the best practices developed
13 under subsection (c).

14 **SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH**
15 **CARE INDUSTRY.**

16 (a) DEFINITIONS.—In this section:

17 (1) BUSINESS ASSOCIATE.—The term “business
18 associate” has the meaning given such term in sec-
19 tion 160.103 of title 45, Code of Federal Regula-
20 tions.

21 (2) COVERED ENTITY.—The term “covered en-
22 tity” has the meaning given such term in section
23 160.103 of title 45, Code of Federal Regulations.

24 (3) HEALTH CARE CLEARINGHOUSE; HEALTH
25 CARE PROVIDER; HEALTH PLAN.—The terms

1 “health care clearinghouse”, “health care provider”,
2 and “health plan” have the meanings given the
3 terms in section 160.103 of title 45, Code of Federal
4 Regulations.

5 (4) HEALTH CARE INDUSTRY STAKEHOLDER.—
6 The term “health care industry stakeholder” means
7 any—

8 (A) health plan, health care clearinghouse,
9 or health care provider;

10 (B) patient advocate;

11 (C) pharmacist;

12 (D) developer of health information tech-
13 nology;

14 (E) laboratory;

15 (F) pharmaceutical or medical device man-
16 ufacturer; or

17 (G) additional stakeholder the Secretary
18 determines necessary for purposes of subsection
19 (d)(1), (d)(3), or (e).

20 (5) SECRETARY.—The term “Secretary” means
21 the Secretary of Health and Human Services.

22 (b) REPORT.—Not later than 1 year after the date
23 of enactment of this Act, the Secretary shall submit, to
24 the Committee on Health, Education, Labor, and Pen-
25 sions of the Senate and the Committee on Energy and

1 Commerce of the House of Representatives, a report on
2 the preparedness of the health care industry in responding
3 to cybersecurity threats.

4 (c) CONTENTS OF REPORT.—With respect to the in-
5 ternal response of the Department of Health and Human
6 Services to emerging cybersecurity threats, the report
7 shall include—

8 (1) a clear statement of the official within the
9 Department of Health and Human Services to be re-
10 sponsible for leading and coordinating efforts of the
11 Department regarding cybersecurity threats in the
12 health care industry; and

13 (2) a plan from each relevant operating division
14 and subdivision of the Department of Health and
15 Human Services on how such division or subdivision
16 will address cybersecurity threats in the health care
17 industry, including a clear delineation of how each
18 such division or subdivision will divide responsibility
19 among the personnel of such division or subdivision
20 and communicate with other such divisions and sub-
21 divisions regarding efforts to address such threats.

22 (d) HEALTH CARE INDUSTRY CYBERSECURITY TASK
23 FORCE.—

24 (1) IN GENERAL.—Not later than 60 days after
25 the date of enactment of this Act, the Secretary, in

1 consultation with the Director of the National Insti-
2 tute of Standards and Technology and the Secretary
3 of Homeland Security, shall convene health care in-
4 dustry stakeholders, cybersecurity experts, and any
5 Federal agencies or entities the Secretary determines
6 appropriate to establish a task force to—

7 (A) analyze how industries, other than the
8 health care industry, have implemented strate-
9 gies and safeguards for addressing cybersecu-
10 rity threats within their respective industries;

11 (B) analyze challenges and barriers private
12 entities (notwithstanding section 102(15)(B),
13 excluding any State, tribal, or local govern-
14 ment) in the health care industry face securing
15 themselves against cyber attacks;

16 (C) review challenges that covered entities
17 and business associates face in securing
18 networked medical devices and other software
19 or systems that connect to an electronic health
20 record;

21 (D) provide the Secretary with information
22 to disseminate to health care industry stake-
23 holders for purposes of improving their pre-
24 paredness for, and response to, cybersecurity
25 threats affecting the health care industry;

1 (E) establish a plan for creating a single
2 system for the Federal Government to share in-
3 formation on actionable intelligence regarding
4 cybersecurity threats to the health care industry
5 in near real time, requiring no fee to the recipi-
6 ents of such information, including which Fed-
7 eral agency or other entity may be best suited
8 to be the central conduit to facilitate the shar-
9 ing of such information; and

10 (F) report to Congress on the findings and
11 recommendations of the task force regarding
12 carrying out subparagraphs (A) through (E).

13 (2) TERMINATION.—The task force established
14 under this subsection shall terminate on the date
15 that is 1 year after the date of enactment of this
16 Act.

17 (3) DISSEMINATION.—Not later than 60 days
18 after the termination of the task force established
19 under this subsection, the Secretary shall dissemi-
20 nate the information described in paragraph (1)(D)
21 to health care industry stakeholders in accordance
22 with such paragraph.

23 (4) RULE OF CONSTRUCTION.—Nothing in this
24 subsection shall be construed to limit the antitrust

1 exemption under section 104(e) or the protection
2 from liability under section 106.

3 (e) CYBERSECURITY FRAMEWORK.—

4 (1) IN GENERAL.—The Secretary shall estab-
5 lish, through a collaborative process with the Sec-
6 retary of Homeland Security, health care industry
7 stakeholders, the National Institute of Standards
8 and Technology, and any Federal agency or entity
9 the Secretary determines appropriate, a single, vol-
10 untary, national health-specific cybersecurity frame-
11 work that—

12 (A) establishes a common set of voluntary,
13 consensus-based, and industry-led standards,
14 security practices, guidelines, methodologies,
15 procedures, and processes that serve as a re-
16 source for cost-effectively reducing cybersecurity
17 risks for a range of health care organizations;

18 (B) supports voluntary adoption and im-
19 plementation efforts to improve safeguards to
20 address cybersecurity threats;

21 (C) is consistent with the security and pri-
22 vacy regulations promulgated under section
23 264(c) of the Health Insurance Portability and
24 Accountability Act of 1996 (42 U.S.C. 1320d-
25 2 note) and with the Health Information Tech-

1 nology for Economic and Clinical Health Act
2 (title XIII of division A, and title IV of division
3 B, of Public Law 111–5), and the amendments
4 made by such Act; and

5 (D) is updated on a regular basis and ap-
6 plicable to the range of health care organiza-
7 tions described in subparagraph (A).

8 (2) LIMITATION.—Nothing in this subsection
9 shall be interpreted as granting the Secretary au-
10 thority to—

11 (A) provide for audits to ensure that
12 health care organizations are in compliance
13 with the voluntary framework under this sub-
14 section; or

15 (B) mandate, direct, or condition the
16 award of any Federal grant, contract, or pur-
17 chase on compliance with such voluntary frame-
18 work.

19 (3) NO LIABILITY FOR NONPARTICIPATION.—
20 Nothing in this title shall be construed to subject a
21 health care organization to liability for choosing not
22 to engage in the voluntary activities authorized
23 under this subsection.

24 **SEC. 406. FEDERAL COMPUTER SECURITY.**

25 (a) DEFINITIONS.—In this section:

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

6 (2) COVERED AGENCY.—The term “covered
7 agency” means an agency that operates a covered
8 system.

9 (3) LOGICAL ACCESS CONTROL.—The term
10 “logical access control” means a process of granting
11 or denying specific requests to obtain and use infor-
12 mation and related information processing services.

13 (4) MULTI-FACTOR LOGICAL ACCESS CON-
14 TROLS.—The term “multi-factor logical access con-
15 trols” means a set of not less than 2 of the following
16 logical access controls:

17 (A) Information that is known to the user,
18 such as a password or personal identification
19 number.

20 (B) An access device that is provided to
21 the user, such as a cryptographic identification
22 device or token.

23 (C) A unique biometric characteristic of
24 the user.

1 (5) PRIVILEGED USER.—The term “privileged
2 user” means a user who, by virtue of function or se-
3 niority, has been allocated powers within a covered
4 system, which are significantly greater than those
5 available to the majority of users.

6 (b) INSPECTOR GENERAL REPORTS ON COVERED
7 SYSTEMS.—

8 (1) IN GENERAL.—Not later than 240 days
9 after the date of enactment of this Act, the Inspec-
10 tor General of each covered agency shall submit to
11 the appropriate committees of jurisdiction in the
12 Senate and the House of Representatives a report,
13 which shall include information collected from the
14 covered agency for the contents described in para-
15 graph (2) regarding the Federal computer systems
16 of the covered agency.

17 (2) CONTENTS.—The report submitted by each
18 Inspector General of a covered agency under para-
19 graph (1) shall include, with respect to the covered
20 agency, the following:

21 (A) A description of the logical access
22 standards used by the covered agency to access
23 a covered system, including—

1 (i) in aggregate, a list and description
2 of logical access controls used to access
3 such a covered system; and

4 (ii) whether the covered agency is
5 using multi-factor logical access controls to
6 access such a covered system.

7 (B) A description of the logical access con-
8 trols used by the covered agency to govern ac-
9 cess to covered systems by privileged users.

10 (C) If the covered agency does not use log-
11 ical access controls or multi-factor logical access
12 controls to access a covered system, a descrip-
13 tion of the reasons for not using such logical
14 access controls or multi-factor logical access
15 controls.

16 (D) A description of the following data se-
17 curity management practices used by the cov-
18 ered agency:

19 (i) The policies and procedures fol-
20 lowed to conduct inventories of the soft-
21 ware present on the covered systems of the
22 covered agency and the licenses associated
23 with such software.

1 (ii) What capabilities the covered
2 agency utilizes to monitor and detect
3 exfiltration and other threats, including—

4 (I) data loss prevention capabili-
5 ties; or

6 (II) digital rights management
7 capabilities.

8 (iii) A description of how the covered
9 agency is using the capabilities described
10 in clause (ii).

11 (iv) If the covered agency is not uti-
12 lizing capabilities described in clause (ii), a
13 description of the reasons for not utilizing
14 such capabilities.

15 (E) A description of the policies and proce-
16 dures of the covered agency with respect to en-
17 suring that entities, including contractors, that
18 provide services to the covered agency are im-
19 plementing the data security management prac-
20 tices described in subparagraph (D).

21 (3) EXISTING REVIEW.—The reports required
22 under this subsection may be based in whole or in
23 part on an audit, evaluation, or report relating to
24 programs or practices of the covered agency, and
25 may be submitted as part of another report, includ-

1 ing the report required under section 3555 of title
2 44, United States Code.

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

6 **SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUC-**
7 **TURE AT GREATEST RISK.**

8 (a) DEFINITIONS.—In this section:

9 (1) APPROPRIATE AGENCY.—The term “appro-
10 priate agency” means, with respect to a covered en-
11 tity—

12 (A) except as provided in subparagraph
13 (B), the applicable sector-specific agency; or

14 (B) in the case of a covered entity that is
15 regulated by a Federal entity, such Federal en-
16 tity.

17 (2) APPROPRIATE AGENCY HEAD.—The term
18 “appropriate agency head” means, with respect to a
19 covered entity, the head of the appropriate agency.

20 (3) COVERED ENTITY.—The term “covered en-
21 tity” means an entity identified pursuant to section
22 9(a) of Executive Order 13636 of February 12,
23 2013 (78 Fed. Reg. 11742), relating to identifica-
24 tion of critical infrastructure where a cybersecurity
25 incident could reasonably result in catastrophic re-

1 gional or national effects on public health or safety,
2 economic security, or national security.

3 (4) APPROPRIATE CONGRESSIONAL COMMIT-
4 TEES.—The term “appropriate congressional com-
5 mittees” means—

6 (A) the Select Committee on Intelligence of
7 the Senate;

8 (B) the Permanent Select Committee on
9 Intelligence of the House of Representatives;

10 (C) the Committee on Homeland Security
11 and Governmental Affairs of the Senate;

12 (D) the Committee on Homeland Security
13 of the House of Representatives;

14 (E) the Committee on Energy and Natural
15 Resources of the Senate;

16 (F) the Committee on Energy and Com-
17 merce of the House of Representatives; and

18 (G) the Committee on Commerce, Science,
19 and Transportation of the Senate.

20 (5) SECRETARY.—The term “Secretary” means
21 the Secretary of the Department of Homeland Secu-
22 rity.

23 (b) STATUS OF EXISTING CYBER INCIDENT REPORT-
24 ING.—

1 (1) IN GENERAL.—No later than 120 days after
2 the date of the enactment of this Act, the Secretary,
3 in conjunction with the appropriate agency head (as
4 the case may be), shall submit to the appropriate
5 congressional committees describing the extent to
6 which each covered entity reports significant intru-
7 sions of information systems essential to the oper-
8 ation of critical infrastructure to the Department of
9 Homeland Security or the appropriate agency head
10 in a timely manner.

11 (2) FORM.—The report submitted under para-
12 graph (1) may include a classified annex.

13 (c) MITIGATION STRATEGY REQUIRED FOR CRITICAL
14 INFRASTRUCTURE AT GREATEST RISK.—

15 (1) IN GENERAL.—No later than 180 days after
16 the date of the enactment of this Act, the Secretary,
17 in conjunction with the appropriate agency head (as
18 the case may be), shall conduct an assessment and
19 develop a strategy that addresses each of the covered
20 entities, to ensure that, to the greatest extent fea-
21 sible, a cyber security incident affecting such entity
22 would no longer reasonably result in catastrophic re-
23 gional or national effects on public health or safety,
24 economic security, or national security.

1 (2) ELEMENTS.—The strategy submitted by the
2 Secretary with respect to a covered entity shall in-
3 clude the following:

4 (A) An assessment of whether each entity
5 should be required to report cyber security inci-
6 dents.

7 (B) A description of any identified security
8 gaps that must be addressed.

9 (C) Additional statutory authority nec-
10 essary to reduce the likelihood that a cyber inci-
11 dent could cause catastrophic regional or na-
12 tional effects on public health or safety, eco-
13 nomic security, or national security.

14 (3) SUBMITTAL.—The Secretary shall submit to
15 the appropriate congressional committees the assess-
16 ment and strategy required by paragraph (1).

17 (4) FORM.—The assessment and strategy sub-
18 mitted under paragraph (3) may each include a clas-
19 sified annex.

20 **SEC. 408. STOPPING THE FRAUDULENT SALE OF FINANCIAL**
21 **INFORMATION OF PEOPLE OF THE UNITED**
22 **STATES.**

23 Section 1029(h) of title 18, United States Code, is
24 amended by striking “title if—” and all that follows
25 through “therefrom.” and inserting “title if the offense

1 involves an access device issued, owned, managed, or con-
2 trolled by a financial institution, account issuer, credit
3 card system member, or other entity organized under the
4 laws of the United States, or any State, the District of
5 Columbia, or other Territory of the United States.”.

6 **SEC. 409. EFFECTIVE PERIOD.**

7 (a) IN GENERAL.—Except as provided in subsection
8 (b), this Act and the amendments made by this Act shall
9 be in effect during the 10-year period beginning on the
10 date of the enactment of this Act.

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

Passed the Senate October 27, 2015.

Attest:

Secretary.

114TH CONGRESS
1ST SESSION

S. 754

AN ACT

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.