

AMENDMENT NO. _____ Calendar No. _____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—114th Cong., 1st Sess.

S. 754

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

Referred to the Committee on _____ and
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended
to be proposed by _____

Viz:

- 1 Strike all after the enacting clause and insert the fol-
- 2 lowing:
- 3 **SECTION 1. TABLE OF CONTENTS.**
- 4 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.

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”—

1 (A) has the meaning given the term in sec-
2 tion 1 of the Clayton Act (15 U.S.C. 12);

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

7 (C) includes any State law that has the
8 same intent and effect as the laws under sub-
9 paragraphs (A) and (B).

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

13 (A) The Department of Commerce.

14 (B) The Department of Defense.

15 (C) The Department of Energy.

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

18 (E) The Department of Justice.

19 (F) The Department of the Treasury.

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

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

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

3 (5) CYBERSECURITY THREAT.—

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

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

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

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

1 ering technical information related to a cyberse-
2 curity threat or security vulnerability;

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

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

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

14 (E) malicious cyber command and control;

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

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

22 (H) any combination thereof.

23 (7) DEFENSIVE MEASURE.—

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

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

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

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

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

20 (8) ENTITY.—

21 (A) IN GENERAL.—Except as otherwise
22 provided in this paragraph, the term “entity”
23 means any private entity, non-Federal govern-
24 ment agency or department, or State, tribal, or

1 local government (including a political subdivi-
2 sion, department, or component thereof).

3 (B) INCLUSIONS.—The term “entity” in-
4 cludes a government agency or department of
5 the District of Columbia, the Commonwealth of
6 Puerto Rico, the Virgin Islands, Guam, Amer-
7 ican Samoa, the Northern Mariana Islands, and
8 any other territory or possession of the United
9 States.

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

14 (9) FEDERAL ENTITY.—The term “Federal en-
15 tity” means a department or agency of the United
16 States or any component of such department or
17 agency.

18 (10) INFORMATION SYSTEM.—The term “infor-
19 mation system”—

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

22 (B) includes industrial control systems,
23 such as supervisory control and data acquisition
24 systems, distributed control systems, and pro-
25 grammable logic controllers.

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

5 (12) MALICIOUS CYBER COMMAND AND CON-
6 TROL.—The term “malicious cyber command and
7 control” means a method for unauthorized remote
8 identification of, access to, or use of, an information
9 system or information that is stored on, processed
10 by, or transiting an information system.

11 (13) MALICIOUS RECONNAISSANCE.—The term
12 “malicious reconnaissance” means a method for ac-
13 tively probing or passively monitoring an information
14 system for the purpose of discerning security
15 vulnerabilities of the information system, if such
16 method is associated with a known or suspected cy-
17 bersecurity threat.

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

22 (15) PRIVATE ENTITY.—

23 (A) IN GENERAL.—Except as otherwise
24 provided in this paragraph, the term “private
25 entity” means any person or private group, or-

1 ganization, proprietorship, partnership, trust,
2 cooperative, corporation, or other commercial or
3 nonprofit entity, including an officer, employee,
4 or agent thereof.

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

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

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

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

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

1 **SEC. 103. SHARING OF INFORMATION BY THE FEDERAL**
2 **GOVERNMENT.**

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

11 (1) the timely sharing of classified cyber threat
12 indicators in the possession of the Federal Govern-
13 ment with cleared representatives of relevant enti-
14 ties;

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

19 (3) the sharing with relevant entities, or the
20 public if appropriate, of unclassified, including con-
21 trolled unclassified, cyber threat indicators in the
22 possession of the Federal Government;

23 (4) the sharing with entities, if appropriate, of
24 information in the possession of the Federal Govern-
25 ment about cybersecurity threats to such entities to

1 prevent or mitigate adverse effects from such cyber-
2 security threats; and

3 (5) the period sharing, through publication and
4 targeted outreach, of cybersecurity best practices
5 that are developed based on ongoing analysis of
6 cyber threat indicators and information in possession
7 of the Federal Government, with attention to acces-
8 sibility and implementation challenges faced by small
9 business concerns (as defined in section 3 of the
10 Small Business Act (15 U.S.C. 532)).

11 (b) DEVELOPMENT OF PROCEDURES.—

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

14 (A) ensure the Federal Government has
15 and maintains the capability to share cyber
16 threat indicators in real time consistent with
17 the protection of classified information;

18 (B) incorporate, to the greatest extent
19 practicable, existing processes and existing roles
20 and responsibilities of Federal and non-Federal
21 entities for information sharing by the Federal
22 Government, including sector specific informa-
23 tion sharing and analysis centers;

24 (C) include procedures for notifying, in a
25 timely manner, entities that have received a

1 cyber threat indicator from a Federal entity
2 under this title that is known or determined to
3 be in error or in contravention of the require-
4 ments of this title or another provision of Fed-
5 eral law or policy of such error or contraven-
6 tion;

7 (D) include requirements for Federal enti-
8 ties sharing cyber threat indicators or defensive
9 measures to implement and utilize security con-
10 trols to protect against unauthorized access to
11 or acquisition of such cyber threat indicators or
12 defensive measures;

13 (E) include procedures that require a Fed-
14 eral entity, prior to the sharing of a cyber
15 threat indicator—

16 (i) to review such cyber threat indi-
17 cator to assess whether such cyber threat
18 indicator contains any information that
19 such Federal entity knows at the time of
20 sharing to be personal information or in-
21 formation that identifies a specific person
22 not directly related to a cybersecurity
23 threat and remove such information; or

24 (ii) to implement and utilize a tech-
25 nical capability configured to remove any

1 personal information or information that
2 identifies a specific person not directly re-
3 lated to a cybersecurity threat; and

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

9 (2) COORDINATION.—In developing the proce-
10 dures required under this section, the Director of
11 National Intelligence, the Secretary of Homeland Se-
12 curity, the Secretary of Defense, and the Attorney
13 General shall coordinate with appropriate Federal
14 entities, including the Small Business Administra-
15 tion and the National Laboratories (as defined in
16 section 2 of the Energy Policy Act of 2005 (42
17 U.S.C. 15801)), to ensure that effective protocols
18 are implemented that will facilitate and promote the
19 sharing of cyber threat indicators by the Federal
20 Government in a timely manner.

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

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

4 (a) AUTHORIZATION FOR MONITORING.—

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

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

10 (B) an information system of another enti-
11 ty, upon the authorization and written consent
12 of such other entity;

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

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

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

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

1 (B) to limit otherwise lawful activity.

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

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

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

11 (B) an information system of another enti-
12 ty upon written consent of such entity for oper-
13 ation of such defensive measure to protect the
14 rights or property of such entity; and

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

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

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

25 (B) to limit otherwise lawful activity.

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

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

11 (2) LAWFUL RESTRICTION.—An entity receiving
12 a cyber threat indicator or defensive measure from
13 another entity or Federal entity shall comply with
14 otherwise lawful restrictions placed on the sharing or
15 use of such cyber threat indicator or defensive meas-
16 ure by the sharing entity or Federal entity.

17 (3) CONSTRUCTION.—Nothing in this sub-
18 section shall be construed—

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

22 (B) to limit otherwise lawful activity.

23 (d) PROTECTION AND USE OF INFORMATION.—

24 (1) SECURITY OF INFORMATION.—An entity
25 monitoring an information system, operating a de-

1 fensive measure, or providing or receiving a cyber
2 threat indicator or defensive measure under this sec-
3 tion shall implement and utilize a security control to
4 protect against unauthorized access to or acquisition
5 of such cyber threat indicator or defensive measure.

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

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

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

23 (3) USE OF CYBER THREAT INDICATORS AND
24 DEFENSIVE MEASURES BY ENTITIES.—

1 (A) IN GENERAL.—Consistent with this
2 title, a cyber threat indicator or defensive meas-
3 ure shared or received under this section may,
4 for cybersecurity purposes—

5 (i) be used by an entity to monitor or
6 operate a defensive measure that is applied
7 to—

8 (I) an information system of the
9 entity; or

10 (II) an information system of an-
11 other entity or a Federal entity upon
12 the written consent of that other enti-
13 ty or that Federal entity; and

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

16 (I) an otherwise lawful restriction
17 placed by the sharing entity or Fed-
18 eral entity on such cyber threat indi-
19 cator or defensive measure; or

20 (II) an otherwise applicable pro-
21 vision of law.

22 (B) CONSTRUCTION.—Nothing in this
23 paragraph shall be construed to authorize the
24 use of a cyber threat indicator or defensive
25 measure other than as provided in this section.

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

3 (A) LAW ENFORCEMENT USE.—

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

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

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

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

1 (ii) exempt from disclosure under any
2 State, tribal, or local law requiring disclo-
3 sure of information or records.

4 (C) STATE, TRIBAL, AND LOCAL REGU-
5 LATORY AUTHORITY.—

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

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

1 to information systems, inform the devel-
2 opment or implementation of a regulation
3 relating to such information systems.

4 (e) ANTITRUST EXEMPTION.—

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

12 (2) APPLICABILITY.—Paragraph (1) shall apply
13 only to information that is exchanged or assistance
14 provided in order to assist with—

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

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

1 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber
2 threat indicator with an entity under this title shall not
3 create a right or benefit to similar information by such
4 entity or any other entity.

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

8 (a) REQUIREMENT FOR POLICIES AND PROCE-
9 DURES.—

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

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

1 receipt of cyber threat indicators and defensive meas-
2 ures by the Federal Government.

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

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

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

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

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

1 (II) carried out before any of the
2 appropriate Federal entities retains or
3 uses the cyber threat indicators or de-
4 fensive measures; and

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

9 (iii) may be provided to other Federal
10 entities;

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

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

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

23 (iii) may be provided to other Federal
24 entities;

1 (C) consistent with this title, any other ap-
2 plicable provisions of law, and the fair informa-
3 tion practice principles set forth in appendix A
4 of the document entitled “National Strategy for
5 Trusted Identities in Cyberspace” and pub-
6 lished by the President in April, 2011, govern
7 the retention, use, and dissemination by the
8 Federal Government of cyber threat indicators
9 shared with the Federal Government under this
10 title, including the extent, if any, to which such
11 cyber threat indicators may be used by the Fed-
12 eral Government; and

13 (D) ensure there are—

14 (i) audit capabilities; and

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

20 (4) GUIDELINES FOR ENTITIES SHARING CYBER
21 THREAT INDICATORS WITH FEDERAL GOVERN-
22 MENT.—

23 (A) IN GENERAL.—Not later than 60 days
24 after the date of the enactment of this Act, the
25 Attorney General and the Secretary of Home-

1 land Security shall develop and make publicly
2 available guidance to assist entities and pro-
3 mote sharing of cyber threat indicators with
4 Federal entities under this title.

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

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

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

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

25 (b) PRIVACY AND CIVIL LIBERTIES.—

1 (1) GUIDELINES OF ATTORNEY GENERAL.—Not
2 later than 60 days after the date of the enactment
3 of this Act, the Attorney General shall, in coordina-
4 tion with heads of the appropriate Federal entities
5 and in consultation with officers designated under
6 section 1062 of the National Security Intelligence
7 Reform Act of 2004 (42 U.S.C. 2000ee–1), develop,
8 submit to Congress, and make available to the public
9 interim guidelines relating to privacy and civil lib-
10 erties which shall govern the receipt, retention, use,
11 and dissemination of cyber threat indicators by a
12 Federal entity obtained in connection with activities
13 authorized in this title.

14 (2) FINAL GUIDELINES.—

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

1 receipt, retention, use, and dissemination of
2 cyber threat indicators by a Federal entity ob-
3 tained in connection with activities authorized
4 in this title.

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

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

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

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

1 (i) a process for the timely destruction
2 of such information that is known not to
3 be directly related to uses authorized under
4 this title; and

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

8 (C) include requirements to safeguard
9 cyber threat indicators containing personal in-
10 formation or information that identifies specific
11 persons from unauthorized access or acquisi-
12 tion, including appropriate sanctions for activi-
13 ties by officers, employees, or agents of the
14 Federal Government in contravention of such
15 guidelines;

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

21 (E) protect the confidentiality of cyber
22 threat indicators containing personal informa-
23 tion or information that identifies specific per-
24 sons to the greatest extent practicable and re-
25 quire recipients to be informed that such indica-

1 tors may only be used for purposes authorized
2 under this title; and

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

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

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

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

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

1 mail or media, an interactive form on an Inter-
2 net website, or a real time, automated process
3 between information systems except—

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

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

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

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

22 (E) does not limit or prohibit otherwise
23 lawful disclosures of communications, records,
24 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-
15 minent threat of death, serious bodily
16 harm, or serious economic harm, including
17 a terrorist act or a use of a weapon of
18 mass destruction;

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

23 (vi) the purpose of preventing, inves-
24 tigating, disrupting, or prosecuting an of-
25 fense 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 and

9 (7) the term “Secretary” means the Secretary
10 of Homeland Security.

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

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

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

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

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

23 (4) by inserting after section 227, as so redesign-
24 nated, the following:

1 **“SEC. 228. CYBERSECURITY PLANS.**

2 “(a) DEFINITIONS.—In this section—

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

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

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

12 “(b) INTRUSION ASSESSMENT PLAN.—

13 “(1) REQUIREMENT.—The Secretary, in coordi-
14 nation with the Director of the Office of Manage-
15 ment and Budget, shall develop and implement an
16 intrusion assessment plan to identify and remove in-
17 truders in agency information systems.

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

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

25 (6) by inserting after section 229, as so redesi-
26 gnated, the following:

1 **“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVEN-**
2 **TION SYSTEM.**

3 “(a) DEFINITIONS.—In this section—

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

7 “(2) the term ‘agency information’ means infor-
8 mation collected or maintained by or on behalf of an
9 agency;

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

12 “(4) the terms ‘cybersecurity risk’ and ‘infor-
13 mation system’ have the meanings given those terms
14 in section 227.

15 “(b) REQUIREMENT.—

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

21 “(A) a capability to detect cybersecurity
22 risks in network traffic transiting or traveling
23 to or from an agency information system; and

24 “(B) a capability to prevent network traffic
25 associated with such cybersecurity risks from
26 transiting or traveling to or from an agency in-

1 formation system or modify such network traf-
2 fic to remove the cybersecurity risk.

3 “(2) REGULAR IMPROVEMENT.—The Secretary
4 shall regularly deploy new technologies and modify
5 existing technologies to the intrusion detection and
6 prevention capabilities described in paragraph (1) as
7 appropriate to improve the intrusion detection and
8 prevention capabilities.

9 “(c) ACTIVITIES.—In carrying out subsection (b), the
10 Secretary—

11 “(1) may access, and the head of an agency
12 may disclose to the Secretary or a private entity pro-
13 viding assistance to the Secretary under paragraph
14 (2), information transiting or traveling to or from an
15 agency information system, regardless of the location
16 from which the Secretary or a private entity pro-
17 viding assistance to the Secretary under paragraph
18 (2) accesses such information, notwithstanding any
19 other provision of law that would otherwise restrict
20 or prevent the head of an agency from disclosing
21 such information to the Secretary or a private entity
22 providing assistance to the Secretary under para-
23 graph (2);

24 “(2) may enter into contracts or other agree-
25 ments with, or otherwise request and obtain the as-

1 sistance of, private entities to deploy and operate
2 technologies in accordance with subsection (b);

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

7 “(4) shall regularly assess through operational
8 test and evaluation in real world or simulated envi-
9 ronments available advanced protective technologies
10 to improve detection and prevention capabilities, in-
11 cluding commercial and non-commercial technologies
12 and detection technologies beyond signature-based
13 detection, and utilize such technologies when appro-
14 priate;

15 “(5) shall establish a pilot to acquire, test, and
16 deploy, as rapidly as possible, technologies described
17 in paragraph (4);

18 “(6) shall periodically update the privacy im-
19 pact assessment required under section 208(b) of
20 the E-Government Act of 2002 (44 U.S.C. 3501
21 note); and

22 “(7) shall ensure that—

23 “(A) activities carried out under this sec-
24 tion are reasonably necessary for the purpose of

1 protecting agency information and agency infor-
2 mation systems from a cybersecurity risk;

3 “(B) information accessed by the Secretary
4 will be retained no longer than reasonably nec-
5 essary for the purpose of protecting agency in-
6 formation and agency information systems from
7 a cybersecurity risk;

8 “(C) notice has been provided to users of
9 an agency information system concerning access
10 to communications of users of the agency infor-
11 mation system for the purpose of protecting
12 agency information and the agency information
13 system; and

14 “(D) the activities are implemented pursu-
15 ant to policies and procedures governing the op-
16 eration of the intrusion detection and preven-
17 tion capabilities.

18 “(d) PRIVATE ENTITIES.—

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

21 “(A) disclose any network traffic transiting
22 or traveling to or from an agency information
23 system to any entity without the consent of the
24 Department or the agency that disclosed the in-
25 formation under subsection (c)(1); or

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

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

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

21 “(e) ATTORNEY GENERAL REVIEW.—Not later than
22 1 year after the date of enactment of this section, the At-
23 torney General shall review the policies and guidelines for
24 the program carried out under this section to ensure that
25 the policies and guidelines are consistent with applicable

1 law governing the acquisition, interception, retention, use,
2 and disclosure of communications.”.

3 (b) PRIORITIZING ADVANCED SECURITY TOOLS.—

4 The Director and the Secretary, in consultation with ap-
5 propriate agencies, shall—

6 (1) review and update governmentwide policies
7 and programs to ensure appropriate prioritization
8 and use of network security monitoring tools within
9 agency networks; and

10 (2) brief appropriate congressional committees
11 on such prioritization and use.

12 (c) AGENCY RESPONSIBILITIES.—

13 (1) IN GENERAL.—Except as provided in para-
14 graph (2)—

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

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

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

14 (3) DEFINITION.—Notwithstanding section
15 202, in this subsection, the term “agency informa-
16 tion system” means an information system owned or
17 operated by an agency.

18 (4) RULE OF CONSTRUCTION.—Nothing in this
19 subsection shall be construed to limit an agency
20 from applying the intrusion detection and prevention
21 capabilities under section 230(b)(1) of the Homeland
22 Security Act of 2002, as added by subsection (a), at
23 the discretion of the head of the agency or as pro-
24 vided in relevant policies, directives, and guidelines.

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

9 **SEC. 204. ADVANCED INTERNAL DEFENSES.**

10 (a) ADVANCED NETWORK SECURITY TOOLS.—

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

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

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

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

13 (d) MAINTENANCE OF TECHNOLOGIES.—Section
14 3553(b)(6)(B) of title 44, United States Code, is amended
15 by inserting “, operating, and maintaining” after “deploy-
16 ing”.

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

21 **SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.**

22 (a) IMPLEMENTATION OF FEDERAL CYBERSECURITY
23 STANDARDS.—Consistent with section 3553 of title 44,
24 United States Code, the Secretary, in consultation with
25 the Director, shall exercise the authority to issue binding

1 operational directives to assist the Director in ensuring
2 timely agency adoption of and compliance with policies
3 and standards promulgated under section 11331 of title
4 40, United States Code, for securing agency information
5 systems.

6 (b) CYBERSECURITY REQUIREMENTS AT AGEN-
7 CIES.—

8 (1) IN GENERAL.—Consistent with policies,
9 standards, guidelines, and directives on information
10 security under subchapter II of chapter 35 of title
11 44, United States Code, and the standards and
12 guidelines promulgated under section 11331 of title
13 40, United States Code, and except as provided in
14 paragraph (2), not later than 1 year after the date
15 of the enactment of this Act, the head of each agen-
16 cy shall—

17 (A) identify sensitive and mission critical
18 data stored by the agency consistent with the
19 inventory required under the first subsection (c)
20 (relating to the inventory of major information
21 systems) and the second subsection (c) (relating
22 to the inventory of information systems) of sec-
23 tion 3505 of title 44, United States Code;

24 (B) assess access controls to the data de-
25 scribed in subparagraph (A), the need for read-

1 ily accessible storage of the data, and individ-
2 uals' need to access the data;

3 (C) encrypt or otherwise render indecipher-
4 able to unauthorized users the data described in
5 subparagraph (A) that is stored on or
6 transiting agency information systems;

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

13 (E) implement identity management con-
14 sistent with section 504 of the Cybersecurity
15 Enhancement Act of 2014 (Public Law 113-
16 274; 15 U.S.C. 7464), including multi-factor
17 authentication, for—

18 (i) remote access to an agency infor-
19 mation system; and

20 (ii) each user account with elevated
21 privileges on an agency information sys-
22 tem.

23 (2) EXCEPTION.—The requirements under
24 paragraph (1) shall not apply to an agency informa-
25 tion system for which—

1 (A) the head of the agency has personally
2 certified to the Director with particularity
3 that—

4 (i) operational requirements articu-
5 lated in the certification and related to the
6 agency information system would make it
7 excessively burdensome to implement the
8 cybersecurity requirement;

9 (ii) the cybersecurity requirement is
10 not necessary to secure the agency infor-
11 mation system or agency information
12 stored on or transiting it; and

13 (iii) the agency has all taken nec-
14 essary steps to secure the agency informa-
15 tion system and agency information stored
16 on or transiting it; and

17 (B) the head of the agency or the designee
18 of the head of the agency has submitted the
19 certification described in subparagraph (A) to
20 the appropriate congressional committees and
21 the agency's authorizing committees.

22 (3) CONSTRUCTION.—Nothing in this section
23 shall be construed to alter the authority of the Sec-
24 retary, the Director, or the Director of the National
25 Institute of Standards and Technology in imple-

1 menting subchapter II of chapter 35 of title 44,
2 United States Code. Nothing in this section shall be
3 construed to affect the National Institute of Stand-
4 ards and Technology standards process or the re-
5 quirement under section 3553(a)(4) of such title or
6 to discourage continued improvements and advance-
7 ments in the technology, standards, policies, and
8 guidelines used to promote Federal information se-
9 curity.

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

14 **SEC. 206. ASSESSMENT; REPORTS.**

15 (a) DEFINITIONS.—In this section—

16 (1) the term “intrusion assessments” means ac-
17 tions taken under the intrusion assessment plan to
18 identify and remove intruders in agency information
19 systems;

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

24 (3) the term “intrusion detection and preven-
25 tion capabilities” means the capabilities required

1 under section 230(b) of the Homeland Security Act
2 of 2002, as added by section 203(a) of this Act.

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

10 (c) REPORTS TO CONGRESS.—

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

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

21 (i) a description of privacy controls;

22 (ii) a description of the technologies
23 and capabilities utilized to detect cyberse-
24 curity risks in network traffic, including
25 the extent to which those technologies and

1 capabilities include existing commercial
2 and non-commercial technologies;

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

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

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

1 work traffic associated with cybersecurity
2 risk; and

3 (vi) a description of the pilot estab-
4 lished under section 230(e)(5) of the
5 Homeland Security Act of 2002, as added
6 by section 203(a) of this Act, including the
7 number of new technologies tested and the
8 number of participating agencies.

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

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

21 (ii) a list by agency of—

22 (I) the number of instances in
23 which the intrusion detection and pre-
24 vention capabilities detected a cyber-
25 security risk in network traffic

1 transiting or traveling to or from an
2 agency information system and the
3 types of indicators, identifiers, and
4 techniques used to detect such cyber-
5 security risks; and

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

15 (2) OMB REPORT ON DEVELOPMENT AND IM-
16 PLEMENTATION OF INTRUSION ASSESSMENT PLAN,
17 ADVANCED INTERNAL DEFENSES, AND FEDERAL CY-
18 BERSECURITY BEST PRACTICES.—The Director
19 shall—

20 (A) not later than 6 months after the date
21 of enactment of this Act, and 30 days after any
22 update thereto, submit the intrusion assessment
23 plan to the appropriate congressional commit-
24 tees;

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

6 (i) a description of the implementation
7 of the intrusion assessment plan;

8 (ii) the findings of the intrusion as-
9 sessments conducted pursuant to the intru-
10 sion assessment plan;

11 (iii) advanced network security tools
12 included in the Continuous Diagnostics
13 and Mitigation Program pursuant to sec-
14 tion 204(a)(1);

15 (iv) the results of the assessment of
16 the Secretary of best practices for Federal
17 cybersecurity pursuant to section 205(a);
18 and

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

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

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

1 (ii) the improved metrics developed
2 pursuant to section 204(b).

3 **SEC. 207. TERMINATION.**

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

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

17 **SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RE-**
18 **LATING TO NATIONAL SECURITY.**

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

22 (1) the Director of National Intelligence, in co-
23 ordination with the heads of other agencies, shall—

24 (A) identify all unclassified information
25 systems that provide access to information that

1 may provide an adversary with the ability to de-
2 rive information that would otherwise be consid-
3 ered classified;

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

7 (C) assess the cost and impact on the mis-
8 sion carried out by each agency that owns an
9 unclassified information system identified in
10 subparagraph (A) if the system were to be sub-
11 sequently designated as a national security sys-
12 tem, as defined in section 11103 of title 40,
13 United States Code; and

14 (2) the Director of National Intelligence shall
15 submit to the appropriate congressional committees,
16 the Select Committee on Intelligence of the Senate,
17 and the Permanent Select Committee on Intelligence
18 of the House of Representatives a report that in-
19 cludes the findings under paragraph (1).

20 (b) FORM.—The report submitted under subsection
21 (a)(2) shall be in unclassified form, and shall include a
22 classified annex.

23 (c) EXCEPTION.—The requirements under subsection
24 (a)(1) shall not apply to the Department of Defense, a

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

3 **SEC. 209. DIRECTION TO AGENCIES.**

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

7 “(h) DIRECTION TO AGENCIES.—

8 “(1) AUTHORITY.—

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

24 “(B) EXCEPTION.—The authorities of the
25 Secretary under this subsection shall not apply

1 to a system described subsection (d) or to a sys-
2 tem described in paragraph (2) or (3) of sub-
3 section (e).

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

5 The Secretary shall—

6 “(A) in coordination with the Director, es-
7 tablish procedures governing the circumstances
8 under which a directive may be issued under
9 this subsection, which shall include—

10 “(i) thresholds and other criteria;

11 “(ii) privacy and civil liberties protec-
12 tions; and

13 “(iii) providing notice to potentially
14 affected third parties;

15 “(B) specify the reasons for the required
16 action and the duration of the directive;

17 “(C) minimize the impact of a directive
18 under this subsection by—

19 “(i) adopting the least intrusive
20 means possible under the circumstances to
21 secure the agency information systems;
22 and

23 “(ii) limiting directives to the shortest
24 period practicable;

1 “(D) notify the Director and the head of
2 any affected agency immediately upon the
3 issuance of a directive under this subsection;

4 “(E) consult with the Director of the Na-
5 tional Institute of Standards and Technology
6 regarding any directive under this subsection
7 that implements standards and guidelines devel-
8 oped by the National Institute of Standards
9 and Technology;

10 “(F) ensure that directives issued under
11 this subsection do not conflict with the stand-
12 ards and guidelines issued under section 11331
13 of title 40;

14 “(G) consider any applicable standards or
15 guidelines developed by the National Institute
16 of Standards and issued by the Secretary of
17 Commerce under section 11331 of title 40; and

18 “(H) not later than February 1 of each
19 year, submit to the appropriate congressional
20 committees a report regarding the specific ac-
21 tions the Secretary has taken pursuant to para-
22 graph (1)(A).

23 “(3) IMMINENT THREATS.—

24 “(A) IN GENERAL.—Notwithstanding sec-
25 tion 3554, the Secretary may authorize the use

1 of protective capabilities under the control of
2 the Secretary for communications or other sys-
3 tem traffic transiting to or from or stored on an
4 agency information system for the purpose of
5 ensuring the security of the information or in-
6 formation system or other agency information
7 systems, if—

8 “(i) the Secretary determines there is
9 an imminent threat to agency information
10 systems;

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

15 “(iii) the Secretary determines the
16 risk posed by the imminent threat out-
17 weighs any adverse consequences reason-
18 ably expected to result from the use of pro-
19 tective capabilities under the control of the
20 Secretary;

21 “(iv) the Secretary provides prior no-
22 tice to the Director, and the head and chief
23 information officer (or equivalent official)
24 of each agency to which specific actions
25 will be taken pursuant to subparagraph

1 (A), and notifies the appropriate congres-
2 sional committees and authorizing commit-
3 tees of each such agencies within seven
4 days of taking an action under this sub-
5 section of—

6 “(I) any action taken under this
7 subsection; and

8 “(II) the reasons for and dura-
9 tion and nature of the action;

10 “(v) the action of the Secretary is
11 consistent with applicable law; and

12 “(vi) the Secretary authorizes the use
13 of protective capabilities in accordance
14 with the advance procedures established
15 under subparagraph (C).

16 “(B) LIMITATION ON DELEGATION.—The
17 authority under this subsection may not be del-
18 egated by the Secretary.

19 “(C) ADVANCE PROCEDURES.—The Sec-
20 retary shall, in coordination with the Director,
21 and in consultation with the heads of Federal
22 agencies, establish procedures governing the cir-
23 cumstances under which the Secretary may au-
24 thorize the use of protective capabilities sub-

1 paragraph (A). The Secretary shall submit the
2 procedures to Congress.

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

6 “(A) protect agency information from un-
7 authorized access, use, disclosure, disruption,
8 modification, or destruction; or

9 “(B) require the remediation of or protect
10 against identified information security risks
11 with respect to—

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

14 “(ii) that portion of an information
15 system used or operated by an agency or
16 by a contractor of an agency or other orga-
17 nization on behalf of an agency.

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

1 “(j) APPROPRIATE CONGRESSIONAL COMMITTEES
2 DEFINED.—In this section, the term ‘appropriate congress-
3 sional committees’ means—

4 “(1) the Committee on Appropriations and the
5 Committee on Homeland Security and Governmental
6 Affairs of the Senate; and

7 “(2) the Committee on Appropriations, the
8 Committee on Homeland Security, the Committee on
9 Oversight and Government Reform, and the Com-
10 mittee on Science, Space, and Technology of the
11 House of Representatives.”.

12 (b) CONFORMING AMENDMENT.—Section
13 3554(a)(1)(B) of title 44, United States Code, is amend-
14 ed—

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

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

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

20 **TITLE III—FEDERAL CYBERSE-**
21 **CURITY WORKFORCE ASSESS-**
22 **MENT**

23 **SEC. 301. SHORT TITLE.**

24 This title may be cited as the “Federal Cybersecurity
25 Workforce Assessment Act”.

1 **SEC. 302. DEFINITIONS.**

2 In this title:

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

6 (A) the Committee on Armed Services of
7 the Senate;

8 (B) the Committee on Homeland Security
9 and Governmental Affairs of the Senate;

10 (C) the Select Committee on Intelligence of
11 the Senate;

12 (D) the Committee on Armed Services in
13 the House of Representatives;

14 (E) the Committee on Homeland Security
15 of the House of Representatives;

16 (F) the Committee on Oversight and Gov-
17 ernment Reform of the House of Representa-
18 tives; and

19 (G) the Permanent Select Committee on
20 Intelligence of the House of Representatives.

21 (2) **DIRECTOR.**—The term “Director” means
22 the Director of the Office of Personnel Management.

23 (3) **ROLES.**—The term “roles” has the meaning
24 given the term in the National Initiative for Cyber-
25 security Education’s Cybersecurity Workforce
26 Framework.

1 **SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEAS-**
2 **UREMENT INITIATIVE.**

3 (a) IN GENERAL.—The head of each Federal agency
4 shall—

5 (1) identify all positions within the agency that
6 require the performance of cybersecurity or other
7 cyber-related functions; and

8 (2) assign the corresponding employment code,
9 which shall be added to the National Initiative for
10 Cybersecurity Education’s National Cybersecurity
11 Workforce Framework, in accordance with sub-
12 section (b).

13 (b) EMPLOYMENT CODES.—

14 (1) PROCEDURES.—

15 (A) CODING STRUCTURE.—Not later than
16 180 days after the date of the enactment of this
17 Act, the Secretary of Commerce, acting through
18 the National Institute of Standards and Tech-
19 nology, shall update the National Initiative for
20 Cybersecurity Education’s Cybersecurity Work-
21 force Framework to include a corresponding
22 coding structure.

23 (B) IDENTIFICATION OF CIVILIAN CYBER
24 PERSONNEL.—Not later than 9 months after
25 the date of enactment of this Act, the Director,
26 in coordination with the Director of National

1 Intelligence, shall establish procedures to imple-
2 ment the National Initiative for Cybersecurity
3 Education’s coding structure to identify all
4 Federal civilian positions that require the per-
5 formance of information technology, cybersecu-
6 rity, or other cyber-related functions.

7 (C) IDENTIFICATION OF NONCIVILIAN
8 CYBER PERSONNEL.—Not later than 18 months
9 after the date of enactment of this Act, the Sec-
10 retary of Defense shall establish procedures to
11 implement the National Initiative for Cyberse-
12 curity Education’s coding structure to identify
13 all Federal noncivilian positions that require the
14 performance of information technology, cyberse-
15 curity, or other cyber-related functions.

16 (D) BASELINE ASSESSMENT OF EXISTING
17 CYBERSECURITY WORKFORCE.—Not later than
18 3 months after the date on which the proce-
19 dures are developed under subparagraphs (B)
20 and (C), respectively, the head of each Federal
21 agency shall submit to the appropriate congres-
22 sional committees of jurisdiction a report that
23 identifies—

24 (i) the percentage of personnel with
25 information technology, cybersecurity, or

1 other cyber-related job functions who cur-
2 rently hold the appropriate industry-recog-
3 nized certifications as identified in the Na-
4 tional Initiative for Cybersecurity Edu-
5 cation's Cybersecurity Workforce Frame-
6 work;

7 (ii) the level of preparedness of other
8 civilian and non-civilian cyber personnel
9 without existing credentials to take certifi-
10 cation exams; and

11 (iii) a strategy for mitigating any
12 gaps identified in clause (i) or (ii) with the
13 appropriate training and certification for
14 existing personnel.

15 (E) PROCEDURES FOR ASSIGNING
16 CODES.—Not later than 3 months after the
17 date on which the procedures are developed
18 under subparagraphs (B) and (C), respectively,
19 the head of each Federal agency shall establish
20 procedures—

21 (i) to identify all encumbered and va-
22 cant positions with information technology,
23 cybersecurity, or other cyber-related func-
24 tions (as defined in the National Initiative

1 for Cybersecurity Education’s coding struc-
2 ture); and

3 (ii) to assign the appropriate employ-
4 ment code to each such position, using
5 agreed standards and definitions.

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

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

17 **SEC. 304. IDENTIFICATION OF CYBER-RELATED ROLES OF**
18 **CRITICAL NEED.**

19 (a) IN GENERAL.—Beginning not later than 1 year
20 after the date on which the employment codes are assigned
21 to employees pursuant to section 203(b)(2), and annually
22 through 2022, the head of each Federal agency, in con-
23 sultation with the Director and the Secretary of Homeland
24 Security, shall—

1 (1) identify information technology, cybersecu-
2 rity, or other cyber-related roles of critical need in
3 the agency's workforce; and

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

5 (A) describes the information technology,
6 cybersecurity, or other cyber-related roles iden-
7 tified under paragraph (1); and

8 (B) substantiates the critical need designa-
9 tions.

10 (b) GUIDANCE.—The Director shall provide Federal
11 agencies with timely guidance for identifying information
12 technology, cybersecurity, or other cyber-related roles of
13 critical need, including—

14 (1) current information technology, cybersecu-
15 rity, and other cyber-related roles with acute skill
16 shortages; and

17 (2) information technology, cybersecurity, or
18 other cyber-related roles with emerging skill short-
19 ages.

20 (c) CYBERSECURITY NEEDS REPORT.—Not later
21 than 2 years after the date of the enactment of this Act,
22 the Director, in consultation with the Secretary of Home-
23 land Security, shall—

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

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

7 **SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS**
8 **REPORTS.**

9 The Comptroller General of the United States shall—

10 (1) analyze and monitor the implementation of
11 sections 203 and 204; and

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

16 **TITLE IV—OTHER CYBER**
17 **MATTERS**

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

19 (a) IN GENERAL.—Not later than 1 year after the
20 date of the enactment of this Act, the Secretary of Home-
21 land Security shall—

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

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

8 (b) MATTERS STUDIED.—In carrying out the study
9 under subsection (a)(1), the Secretary shall—

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

14 (2) assess the effect such threats may have on
15 the cybersecurity of the information systems and
16 networks of the Federal Government (except for na-
17 tional security systems or the information systems
18 and networks of the Department of Defense and the
19 intelligence community);

20 (3) develop recommendations for addressing
21 such threats based on industry standards and best
22 practices;

23 (4) identify any deficiencies in the current au-
24 thorities of the Secretary that may inhibit the ability
25 of the Secretary to address mobile device security

1 throughout the Federal Government (except for na-
2 tional security systems and the information systems
3 and networks of the Department of Defense and in-
4 telligence community); and

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

8 (c) INTELLIGENCE COMMUNITY DEFINED.—In this
9 section, the term “intelligence community” has the mean-
10 ing given such term in section 3 of the National Security
11 Act of 1947 (50 U.S.C. 3003).

12 **SEC. 402. DEPARTMENT OF STATE INTERNATIONAL CYBER-**
13 **SPACE POLICY STRATEGY.**

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

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

20 (1) A review of actions and activities under-
21 taken by the Secretary of State to date to support
22 the goal of the President’s International Strategy for
23 Cyberspace, released in May 2011, to “work inter-
24 nationally to promote an open, interoperable, secure,
25 and reliable information and communications infra-

1 structure that supports international trade and com-
2 merce, strengthens international security, and fos-
3 ters free expression and innovation.”.

4 (2) A plan of action to guide the diplomacy of
5 the Secretary of State, with regard to foreign coun-
6 tries, including conducting bilateral and multilateral
7 activities to develop the norms of responsible inter-
8 national behavior in cyberspace, and status review of
9 existing discussions in multilateral fora to obtain
10 agreements on international norms in cyberspace.

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

15 (4) A detailed description of threats to United
16 States national security in cyberspace from foreign
17 countries, state-sponsored actors, and private actors
18 to Federal and private sector infrastructure of the
19 United States, intellectual property in the United
20 States, and the privacy of citizens of the United
21 States.

22 (5) A review of policy tools available to the
23 President to deter foreign countries, state-sponsored
24 actors, and private actors, including those outlined

1 in Executive Order 13694, released on April 1,
2 2015.

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

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

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

17 (e) AVAILABILITY OF INFORMATION.—The Secretary
18 of State shall—

19 (1) make the strategy required in subsection (a)
20 available the public; and

21 (2) brief the Committee on Foreign Relations of
22 the Senate and the Committee on Foreign Affairs of
23 the House of Representatives on the strategy, in-
24 cluding any material contained in a classified annex.

1 **SEC. 403. APPREHENSION AND PROSECUTION OF INTER-**
2 **NATIONAL CYBER CRIMINALS.**

3 (a) INTERNATIONAL CYBER CRIMINAL DEFINED.—

4 In this section, the term “international cyber criminal”
5 means an individual—

6 (1) who is believed to have committed a
7 cybercrime or intellectual property crime against the
8 interests of the United States or the citizens of the
9 United States; and

10 (2) for whom—

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

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

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

24 (1) to apprehend and prosecute such criminals;
25 and

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

4 (c) ANNUAL REPORT.—

5 (1) IN GENERAL.—The Secretary of State shall
6 submit to the appropriate congressional committees
7 an annual report that includes—

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

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

20 (C) for each international cyber criminal
21 who was extradited to the United States during
22 the most recently completed calendar year—

23 (i) his or her name;

24 (ii) the crimes for which he or she was
25 charged;

1 (iii) his or her previous country of res-
2 idence; and

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

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

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

11 (A) the Committee on Foreign Relations,
12 the Committee on Appropriations, the Com-
13 mittee on Homeland Security and Govern-
14 mental Affairs, the Committee on Banking,
15 Housing, and Urban Affairs, the Select Com-
16 mittee on Intelligence, and the Committee on
17 the Judiciary of the Senate; and

18 (B) the Committee on Foreign Affairs, the
19 Committee on Appropriations, the Committee
20 on Homeland Security, the Committee on Fi-
21 nancial Services, the Permanent Select Com-
22 mittee on Intelligence, and the Committee on
23 the Judiciary of the House of Representatives.

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

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

13 (b) ANALYSIS OF DATA.—Not later than 1 year after
14 the date of enactment of this Act, the Secretary of Home-
15 land Security, acting through the Director of the National
16 Cybersecurity and Communications Integration Center, in
17 coordination with appropriate entities and the Director for
18 Emergency Communications, and in consultation with the
19 Director of the National Institute of Standards and Tech-
20 nology, shall conduct integration and analysis of the data
21 reported under subsection (a) to develop information and
22 recommendations on security and resilience measures for
23 any information system or network used by State emer-
24 gency response providers.

25 (c) BEST PRACTICES.—

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

11 (2) REPORT.—The Director of the National In-
12 stitute of Standards and Technology shall submit a
13 report to Congress on the methods developed under
14 paragraph (1) and shall make such report publically
15 available on the website of the National Institute of
16 Standards and Technology.

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

19 (1) require a State to report data under sub-
20 section (a); or

21 (2) require an entity to—

22 (A) adopt a recommended measure devel-
23 oped under subsection (b); or

24 (B) follow the best practices developed
25 under subsection (c).

1 **SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH**
2 **CARE INDUSTRY.**

3 (a) DEFINITIONS.—In this section:

4 (1) BUSINESS ASSOCIATE.—The term “business
5 associate” has the meaning given such term in sec-
6 tion 160.103 of title 45, Code of Federal Regula-
7 tions.

8 (2) COVERED ENTITY.—The term “covered en-
9 tity” has the meaning given such term in section
10 160.103 of title 45, Code of Federal Regulations.

11 (3) HEALTH CARE CLEARINGHOUSE; HEALTH
12 CARE PROVIDER; HEALTH PLAN.—The terms
13 “health care clearinghouse”, “health care provider”,
14 and “health plan” have the meanings given the
15 terms in section 160.103 of title 45, Code of Federal
16 Regulations.

17 (4) HEALTH CARE INDUSTRY STAKEHOLDER.—
18 The term “health care industry stakeholder” means
19 any—

20 (A) health plan, health care clearinghouse,
21 or health care provider;

22 (B) patient advocate;

23 (C) pharmacist;

24 (D) developer of health information tech-
25 nology;

26 (E) laboratory;

1 (F) pharmaceutical or medical device man-
2 ufacturer; or

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

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

8 (b) REPORT.—Not later than 1 year after the date
9 of enactment of this Act, the Secretary shall submit, to
10 the Committee on Health, Education, Labor, and Pen-
11 sions of the Senate and the Committee on Energy and
12 Commerce of the House of Representatives, a report on
13 the preparedness of the health care industry in responding
14 to cybersecurity threats.

15 (c) CONTENTS OF REPORT.—With respect to the in-
16 ternal response of the Department of Health and Human
17 Services to emerging cybersecurity threats, the report
18 shall include—

19 (1) a clear statement of the official within the
20 Department of Health and Human Services to be re-
21 sponsible for leading and coordinating efforts of the
22 Department regarding cybersecurity threats in the
23 health care industry; and

24 (2) a plan from each relevant operating division
25 and subdivision of the Department of Health and

1 Human Services on how such division or subdivision
2 will address cybersecurity threats in the health care
3 industry, including a clear delineation of how each
4 such division or subdivision will divide responsibility
5 among the personnel of such division or subdivision
6 and communicate with other such divisions and sub-
7 divisions regarding efforts to address such threats.

8 (d) HEALTH CARE INDUSTRY CYBERSECURITY TASK
9 FORCE.—

10 (1) IN GENERAL.—Not later than 60 days after
11 the date of enactment of this Act, the Secretary, in
12 consultation with the Secretary of Homeland Secu-
13 rity, shall convene health care industry stakeholders,
14 cybersecurity experts, and any Federal agencies or
15 entities the Secretary determines appropriate to es-
16 tablish a task force to—

17 (A) analyze how industries, other than the
18 health care industry, have implemented strate-
19 gies and safeguards for addressing cybersecu-
20 rity threats within their respective industries;

21 (B) analyze challenges and barriers private
22 entities (notwithstanding section 2(15)(B), ex-
23 cluding any State, tribal, or local government)
24 in the health care industry face securing them-
25 selves against cyber attacks;

1 (C) review challenges that covered entities
2 and business associates face in securing
3 networked medical devices and other software
4 or systems that connect to an electronic health
5 record;

6 (D) provide the Secretary with information
7 to disseminate to health care industry stake-
8 holders for purposes of improving their pre-
9 paredness for, and response to, cybersecurity
10 threats affecting the health care industry;

11 (E) establish a plan for creating a single
12 system for the Federal Government to share in-
13 formation on actionable intelligence regarding
14 cybersecurity threats to the private sector in
15 near real time, at no cost to the recipients of
16 such information, including which Federal
17 agency or other entity may be best suited to be
18 the central conduit to facilitate the sharing of
19 such information; and

20 (F) report to Congress on the findings and
21 recommendations of the task force regarding
22 carrying out subparagraphs (A) through (E).

23 (2) TERMINATION.—The task force established
24 under this subsection shall terminate on the date

1 that is 1 year after the date of enactment of this
2 Act.

3 (3) DISSEMINATION.—Not later than 60 days
4 after the termination of the task force established
5 under this subsection, the Secretary shall dissemi-
6 nate the information described in paragraph (1)(D)
7 to health care industry stakeholders in accordance
8 with such paragraph.

9 (e) CYBERSECURITY FRAMEWORK.—The Secretary
10 shall establish, through a collaborative process with the
11 Secretary of Homeland Security, health care industry
12 stakeholders, the National Institute of Standards and
13 Technology, and any Federal agency or entity the Sec-
14 retary determines appropriate, a single, voluntary, na-
15 tional health-specific cybersecurity framework that—

16 (1) establishes a common set of security prac-
17 tices and standards that specifically pertain to a
18 range of health care organizations;

19 (2) supports voluntary adoption and implemen-
20 tation efforts to improve safeguards to address cy-
21 bersecurity threats; and

22 (3) is consistently updated and applicable to the
23 range of health care organizations described in para-
24 graph (1).

1 **SEC. 406. FEDERAL COMPUTER SECURITY.**

2 (a) DEFINITIONS.—In this section:

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

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

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

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

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

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

25 (C) A unique biometric characteristic of
26 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 each submit
11 to each Comptroller General of the United States
12 and the appropriate committees of jurisdiction in the
13 Senate and the House of Representatives a report,
14 which shall include information collected from the
15 covered agency for the contents described in para-
16 graph (2) regarding the Federal computer systems
17 of the covered agency.

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

22 (A) A description of the logical access
23 standards used by the covered agency to access
24 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 (c) GAO ECONOMIC ANALYSIS AND REPORT ON FED-
7 ERAL COMPUTER SYSTEMS.—

8 (1) REPORT.—Not later than 1 year after the
9 date of enactment of this Act, the Comptroller Gen-
10 eral of the United States shall submit to Congress
11 a report examining, including an economic analysis
12 of, any impediments to agency use of effective secu-
13 rity software and security devices.

14 (2) CLASSIFIED INFORMATION.—A report sub-
15 mitted under this subsection shall be in unclassified
16 form, but may include a classified annex.

17 **SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUC-**
18 **TURE AT GREATEST RISK.**

19 (a) DEFINITIONS.—In this section:

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

23 (A) except as provided in subparagraph

24 (B), the applicable sector-specific agency; or

1 (B) in the case of a covered entity that is
2 regulated by a Federal entity, such Federal en-
3 tity.

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

7 (3) COVERED ENTITY.—The term “covered en-
8 tity” means an entity identified under subsection
9 (b).

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

13 (A) the Select Committee on Intelligence of
14 the Senate;

15 (B) the Permanent Select Committee on
16 Intelligence of the House of Representatives;

17 (C) the Committee on Homeland Security
18 and Governmental Affairs of the Senate;

19 (D) the Committee on Homeland Security
20 of the House of Representatives;

21 (E) the Committee on Energy and Natural
22 Resources of the Senate; and

23 (F) the Committee on Energy and Com-
24 merce of the House of Representatives;

1 (5) SECRETARY.—The term “Secretary” means
2 the Secretary of the Department of Homeland Secu-
3 rity

4 (b) IDENTIFICATION OF CRITICAL INFRASTRUCTURE
5 AT GREATEST RISK REQUIRED.—No later than 60 days
6 after the date of the enactment of this Act, the Secretary
7 shall identify critical infrastructure entities where a cyber-
8 security incident could reasonably result in catastrophic
9 regional or national effects on public health or safety, eco-
10 nomic security, or national security.

11 (c) STATUS OF EXISTING CYBER INCIDENT REPORT-
12 ING.—

13 (1) IN GENERAL.—No later than 120 days after
14 the date of the enactment of this Act, the Secretary,
15 in conjunction with the appropriate agency head (as
16 the case may be), shall submit to the appropriate
17 congressional committees describing the extent to
18 which each covered entity reports significant intru-
19 sions of information systems essential to the oper-
20 ation of critical infrastructure to the Department of
21 Homeland Security or the appropriate agency head
22 in a timely manner.

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

1 (d) MITIGATION STRATEGY REQUIRED FOR CRITICAL
2 INFRASTRUCTURE AT GREATEST RISK.—

3 (1) IN GENERAL.—No later than 180 days after
4 the date of the enactment of this Act, the Secretary,
5 in conjunction with the appropriate agency head (as
6 the case may be), shall conduct an assessment and
7 develop a strategy that addresses each of the covered
8 entities, to ensure that, to the greatest extent fea-
9 sible, a cyber security incident affecting such entity
10 would no longer reasonably result in catastrophic re-
11 gional or national effects on public health or safety,
12 economic security, or national security.

13 (2) ELEMENTS.—The strategy submitted by the
14 Secretary with respect to a covered entity intrusion
15 shall include the following:

16 (A) An assessment of whether each entity
17 should be required to report cyber security inci-
18 dents.

19 (B) A description of any identified security
20 gaps that must be addressed.

21 (C) Additional statutory authority nec-
22 essary to reduce the likelihood that a cyber inci-
23 dent could cause catastrophic regional or na-
24 tional effects on public health or safety, eco-
25 nomic security, or national security.

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

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

7 (e) SENATE OF CONGRESS.—To the extent that the
8 Secretary proposes to require the reporting of significant
9 cyber intrusions of any covered entity pursuant to a rec-
10 ommendation identified in subsection (d) it is the Sense
11 of Congress that—

12 (1) the Secretary should ensure that the policies
13 and procedures established for such reporting incor-
14 porate, to the greatest extent practicable, processes,
15 roles, and responsibilities of appropriate agencies
16 and entities, including sector specific information
17 sharing and analysis centers, that were in effect on
18 the day before the date of the enactment of this Act;

19 (2) no cause of action should lie or be main-
20 tained in any court against a covered entity, and
21 such action should be promptly dismissed for shar-
22 ing information with the Secretary or the appro-
23 priate agency head for sharing such information;

24 (3) the Secretary or appropriate agency head,
25 as the case may be, should, under section 103 and

1 to the greatest extent practicable, make available to
2 any covered entity submitting a report such cyber
3 threat indicators as the Secretary or appropriate
4 agency head considers appropriate; and

5 (4) the Secretary or the appropriate agency
6 head (as the case may be) should take such actions
7 as the Secretary or the appropriate agency head (as
8 the case may be) considers appropriate to protect
9 from disclosure the identity of the covered entity.