

Calendar No. 470

112TH CONGRESS
2D SESSION**S. 3414**

To enhance the security and resiliency of the cyber and communications
infrastructure of the United States.

IN THE SENATE OF THE UNITED STATES

JULY 19, 2012

Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEIN-
STEIN, and Mr. CARPER) introduced the following bill; which was read
the first time

JULY 23, 2012

Read the second time and placed on the calendar

A BILL

To enhance the security and resiliency of the cyber and
communications infrastructure of the United States.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Cybersecurity Act of 2012” or the “CSA2012”.

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.

TITLE I—PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURE

- Sec. 101. National Cybersecurity Council.
- Sec. 102. Inventory of critical infrastructure.
- Sec. 103. Voluntary cybersecurity practices.
- Sec. 104. Voluntary cybersecurity program for critical infrastructure.
- Sec. 105. Rules of construction.
- Sec. 106. Protection of information.
- Sec. 107. Annual assessment of cybersecurity.
- Sec. 108. International cooperation.
- Sec. 109. Effect on other laws.
- Sec. 110. Definitions.

TITLE II—FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

- Sec. 201. FISMA Reform.
- Sec. 202. Management of information technology.
- Sec. 203. Savings provisions.
- Sec. 204. Consolidation of existing departmental cyber resources and authorities.

TITLE III—RESEARCH AND DEVELOPMENT

- Sec. 301. Federal cybersecurity research and development.
- Sec. 302. Homeland security cybersecurity research and development.
- Sec. 303. Research centers for cybersecurity.
- Sec. 304. Centers of excellence.

TITLE IV—EDUCATION, WORKFORCE, AND AWARENESS

- Sec. 401. Definitions.
- Sec. 402. Education and awareness.
- Sec. 403. National cybersecurity competition and challenge.
- Sec. 404. Federal Cyber Scholarship-for-Service program.
- Sec. 405. Assessment of cybersecurity Federal workforce.
- Sec. 406. Federal cybersecurity occupation classifications.
- Sec. 407. Training and education of Federal employees.
- Sec. 408. National Center for Cybersecurity and Communications acquisition authorities.
- Sec. 409. Reports on cyber incidents against Government networks.
- Sec. 410. Reports on prosecution for cybercrime.
- Sec. 411. Report on research relating to secure domain.
- Sec. 412. Report on preparedness of Federal courts to promote cybersecurity.
- Sec. 413. Report on impediments to public awareness.
- Sec. 414. Report on protecting the electrical grid of the United States.
- Sec. 415. Marketplace information.

TITLE V—FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

- Sec. 501. Federal acquisition risk management strategy.
- Sec. 502. Amendments to Clinger-Cohen provisions to enhance agency planning for information security needs.

TITLE VI—INTERNATIONAL COOPERATION

- Sec. 601. Definitions.
- Sec. 602. Findings.
- Sec. 603. Sense of Congress.
- Sec. 604. Coordination of international cyber issues within the United States Government.
- Sec. 605. Consideration of cybercrime in foreign policy and foreign assistance programs.

TITLE VII—INFORMATION SHARING

- Sec. 701. Affirmative authority to monitor and defend against cybersecurity threats.
- Sec. 702. Voluntary disclosure of cybersecurity threat indicators among private entities.
- Sec. 703. Cybersecurity exchanges.
- Sec. 704. Voluntary disclosure of cybersecurity threat indicators to a cybersecurity exchange.
- Sec. 705. Sharing of classified cybersecurity threat indicators.
- Sec. 706. Limitation on liability and good faith defense for cybersecurity activities.
- Sec. 707. Construction and federal preemption.
- Sec. 708. Definitions.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) CATEGORY OF CRITICAL CYBER INFRA-
 4 STRUCTURE.—The term “category of critical cyber
 5 infrastructure” means a category identified by the
 6 Council as critical cyber infrastructure in accordance
 7 with the procedure established under section 102.

8 (2) COMMERCIAL INFORMATION TECHNOLOGY
 9 PRODUCT.—The term “commercial information tech-
 10 nology product” means a commercial item that orga-
 11 nizes or communicates information electronically.

12 (3) COMMERCIAL ITEM.—The term “commer-
 13 cial item” has the meaning given the term in section
 14 103 of title 41, United States Code.

1 (4) COUNCIL.—The term “Council” means the
2 National Cybersecurity Council established under
3 section 101.

4 (5) CRITICAL CYBER INFRASTRUCTURE.—The
5 term “critical cyber infrastructure” means critical
6 infrastructure identified by the Council under sec-
7 tion 102(b)(3)(A).

8 (6) CRITICAL INFRASTRUCTURE.—The term
9 “critical infrastructure” has the meaning given that
10 term in section 1016(e) of the USA PATRIOT Act
11 (42 U.S.C. 5195c(e)).

12 (7) CRITICAL INFRASTRUCTURE PARTNERSHIP
13 ADVISORY COUNCIL.—The term “Critical Infrastruc-
14 ture Partnership Advisory Council” means the Crit-
15 ical Infrastructure Partnership Advisory Council es-
16 tablished by the Department under section 871 of
17 the Homeland Security Act of 2002 (6 U.S.C. 451)
18 to coordinate critical infrastructure protection activi-
19 ties within the Federal Government and with the
20 private sector and State, local, territorial, and tribal
21 governments.

22 (8) DEPARTMENT.—The term “Department”
23 means the Department of Homeland Security.

1 (9) FEDERAL AGENCY.—The term “Federal
2 agency” has the meaning given the term “agency”
3 in section 3502 of title 44, United States Code.

4 (10) FEDERAL INFORMATION INFRASTRUC-
5 TURE.—The term “Federal information infrastruc-
6 ture”—

7 (A) means information and information
8 systems that are owned, operated, controlled, or
9 licensed for use by, or on behalf of, any Federal
10 agency, including information systems used or
11 operated by another entity on behalf of a Fed-
12 eral agency; and

13 (B) does not include—

14 (i) a national security system; or

15 (ii) information and information sys-
16 tems that are owned, operated, controlled,
17 or licensed solely for use by, or on behalf
18 of, the Department of Defense, a military
19 department, or an element of the intel-
20 ligence community.

21 (11) INCIDENT.—The term “incident” has the
22 meaning given that term in section 3552 of title 44,
23 United States Code, as added by section 201 of this
24 Act.

1 (12) INFORMATION INFRASTRUCTURE.—The
2 term “information infrastructure” means the under-
3 lying framework that information systems and assets
4 rely on to process, transmit, receive, or store infor-
5 mation electronically, including programmable elec-
6 tronic devices, communications networks, and indus-
7 trial or supervisory control systems and any associ-
8 ated hardware, software, or data.

9 (13) INFORMATION SHARING AND ANALYSIS OR-
10 GANIZATION.—The term “Information Sharing and
11 Analysis Organization” has the meaning given that
12 term in section 212 of the Homeland Security Act
13 of 2002 (6 U.S.C. 131).

14 (14) INFORMATION SYSTEM.—The term “infor-
15 mation system” has the meaning given that term in
16 section 3502 of title 44, United States Code.

17 (15) INSTITUTION OF HIGHER EDUCATION.—
18 The term “institution of higher education” has the
19 meaning given that term in section 102 of the High-
20 er Education Act of 1965 (20 U.S.C. 1002).

21 (16) INTELLIGENCE COMMUNITY.—The term
22 “intelligence community” has the meaning given
23 that term under section 3(4) of the National Secu-
24 rity Act of 1947 (50 U.S.C. 401a(4)).

1 (17) MEMBER AGENCY.—The term “member
2 agency” means a Federal agency from which a mem-
3 ber of the Council is appointed.

4 (18) NATIONAL INFORMATION INFRASTRUC-
5 TURE.—The term “national information infrastruc-
6 ture” means information and information systems—

7 (A) that are owned, operated, or con-
8 trolled, in whole or in part, within or from the
9 United States; and

10 (B) that are not owned, operated, con-
11 trolled, or licensed for use by a Federal agency.

12 (19) NATIONAL LABORATORY.—The term “na-
13 tional laboratory” has the meaning given the term in
14 section 2 of the Energy Policy Act of 2005 (42
15 U.S.C. 15801).

16 (20) NATIONAL SECURITY SYSTEM.—The term
17 “national security system” has the meaning given
18 that term in section 3552 of title 44, United States
19 Code, as added by section 201 of this Act.

20 (21) OWNER.—The term “owner”—

21 (A) means an entity that owns critical in-
22 frastructure; and

23 (B) does not include a company contracted
24 by the owner to manage, run, or operate that
25 critical infrastructure, or to provide a specific

1 information technology product or service that
2 is used or incorporated into that critical infra-
3 structure.

4 (22) OPERATOR.—The term “operator”—

5 (A) means an entity that manages, runs,
6 or operates, in whole or in part, the day-to-day
7 operations of critical infrastructure; and

8 (B) may include the owner of critical infra-
9 structure.

10 (23) SECRETARY.—The term “Secretary”
11 means the Secretary of Homeland Security.

12 (24) SIGNIFICANT CYBER INCIDENT.—The term
13 “significant cyber incident” means an incident re-
14 sulting in, or an attempted to cause an incident
15 that, if successful, would have resulted in—

16 (A) the exfiltration of data that is essential
17 to the operation of critical cyber infrastructure;
18 or

19 (B) the defeat of an operational control or
20 technical control, as those terms are defined in
21 section 708, essential to the security or oper-
22 ation of critical cyber infrastructure.

1 **TITLE I—PUBLIC-PRIVATE PART-**
2 **nership TO PROTECT CRIT-**
3 **ICAL INFRASTRUCTURE**

4 **SEC. 101. NATIONAL CYBERSECURITY COUNCIL.**

5 (a) IN GENERAL.—There is established a National
6 Cybersecurity Council.

7 (b) RESPONSIBILITIES.—The Council shall—

8 (1) conduct sector-by-sector risk assessments in
9 partnership with owners and operators, private sec-
10 tor entities, relevant Federal agencies, and appro-
11 priate non-governmental entities and institutions of
12 higher education;

13 (2) identify categories of critical cyber infra-
14 structure, in partnership with relevant Federal agen-
15 cies, owners and operators, other appropriate private
16 sector entities, and appropriate non-governmental
17 entities and institutions of higher education;

18 (3) coordinate the adoption of private-sector
19 recommended voluntary outcome-based cybersecurity
20 practices with owners and operators, private sector
21 entities, relevant Federal agencies, the Critical In-
22 frastructure Partnership Advisory Council, institu-
23 tions of higher education, and appropriate non-gov-
24 ernmental cybersecurity experts, in accordance with
25 this title;

1 (4) establish an incentives-based voluntary cy-
2 bersecurity program for critical infrastructure to en-
3 courage owners to adopt voluntary outcome-based
4 cybersecurity practices under section 103;

5 (5) develop procedures to inform owners and
6 operators of cyber threats, vulnerabilities, and con-
7 sequences; and

8 (6) upon request and to the maximum extent
9 possible, provide any technical guidance or assist-
10 ance to owners and operators consistent with this
11 title.

12 (c) PROCEDURES.—The President shall establish pro-
13 cedures, consistent with this section, for the operation of
14 the Council, which shall include procedures that—

15 (1) prescribe the responsibilities of the Council
16 and the member agencies;

17 (2) ensure the timely implementation of deci-
18 sions of the Council;

19 (3) delegate authority to the Chairperson to
20 take action to fulfill the responsibilities of the Coun-
21 cil if—

22 (A) the Council is not fulfilling the respon-
23 sibilities of the Council in a timely fashion; or

24 (B) necessary to prevent or mitigate an
25 imminent cybersecurity threat.

1 (d) MEMBERSHIP.—The Council shall be comprised
2 of appropriate representatives appointed by the President
3 from—

4 (1) the Department of Commerce;

5 (2) the Department of Defense;

6 (3) the Department of Justice;

7 (4) the intelligence community;

8 (5) sector-specific Federal agencies, as appro-
9 priate;

10 (6) Federal agencies with responsibility for reg-
11 ulating the security of critical cyber infrastructure,
12 as appropriate; and

13 (7) the Department.

14 (e) COORDINATION.—The Council shall coordinate
15 the activities of the Council with—

16 (1) appropriate representatives of the private
17 sector; and

18 (2) owners and operators.

19 (f) CHAIRPERSON.—

20 (1) IN GENERAL.—The Secretary shall serve as
21 Chairperson of the Council (referred to in this sec-
22 tion as the “Chairperson”).

23 (2) RESPONSIBILITIES OF THE CHAIR-
24 PERSON.—The Chairperson shall—

1 (A) ensure the responsibilities of the Coun-
 2 cil are expeditiously fulfilled;

3 (B) provide expertise and support to the
 4 Council; and

5 (C) provide recommendations to the Coun-
 6 cil.

7 (g) PARTICIPATION OF SECTOR-SPECIFIC FEDERAL
 8 AGENCIES AND FEDERAL REGULATORY AGENCIES.—A
 9 sector-specific Federal agency and a Federal agency with
 10 responsibility for regulating the security of critical cyber
 11 infrastructure shall participate on the Council on matters
 12 directly relating to the sector of critical infrastructure for
 13 which the Federal agency has responsibility to ensure that
 14 any cybersecurity practice adopted by the Council under
 15 section 103—

16 (1) does not contradict any regulation or com-
 17 pulsory standard in effect before the adoption of the
 18 cybersecurity practice; and

19 (2) to the extent possible, complements or oth-
 20 erwise improves the regulation or compulsory stand-
 21 ard described in paragraph (1).

22 **SEC. 102. INVENTORY OF CRITICAL INFRASTRUCTURE.**

23 (a) RISK ASSESSMENTS.—

24 (1) IN GENERAL.—

1 (A) DESIGNATION OF MEMBER AGENCY.—

2 The Council shall designate a member agency
3 to conduct top-level cybersecurity assessments
4 of cyber risks to critical infrastructure with vol-
5 untary participation from private sector enti-
6 ties.

7 (B) RULE OF CONSTRUCTION.—Nothing in
8 this subsection shall be construed to give new
9 authority to a Federal agency to require owners
10 or operators to provide information to the Fed-
11 eral Government.

12 (2) RESPONSIBILITY.—The member agency
13 designated under paragraph (1), in consultation with
14 owners and operators, the Critical Infrastructure
15 Partnership Advisory Council, and appropriate In-
16 formation Sharing and Analysis Organizations, and
17 in coordination with other member agencies, the in-
18 telligence community, and the Department of Com-
19 merce, shall—

20 (A) not later than 180 days after the date
21 of enactment of this Act, conduct a top-level as-
22 sessment of the cybersecurity threats,
23 vulnerabilities, and consequences and the prob-
24 ability of a catastrophic incident and associated
25 risk across all critical infrastructure sectors to

determine which sectors pose the greatest immediate risk, in order to guide the allocation of resources for the implementation of this Act; and

(B) beginning with the highest priority sectors identified under subparagraph (A), conduct, on an ongoing, sector-by-sector basis, cyber risk assessments of the threats to, vulnerabilities of, and consequences of a cyber attack on critical infrastructure.

(3) VOLUNTARY INPUT OF OWNERS AND OPERATORS.—The member agency designated under paragraph (1) shall—

(A) establish a process under which owners and operators and other relevant private sector experts may provide input into the risk assessments conducted under this section; and

(B) seek and incorporate private sector expertise available through established public-private partnerships, including the Critical Infrastructure Partnership Advisory Council and appropriate Information Sharing and Analysis Organizations.

(4) PROTECTION OF INFORMATION.—Any information submitted as part of the process established

1 under paragraph (3) shall be protected in accord-
2 ance with section 106.

3 (5) SUBMISSION OF RISK ASSESSMENTS.—The
4 Council shall submit each risk assessment conducted
5 under this section, in a classified or unclassified
6 form as necessary, to—

7 (A) the President;

8 (B) appropriate Federal agencies; and

9 (C) appropriate congressional committees.

10 (b) IDENTIFICATION OF CRITICAL CYBER INFRA-
11 STRUCTURE CATEGORIES.—

12 (1) IN GENERAL.—The Council, in consultation
13 with owners and operators, the Critical Infrastruc-
14 ture Partnership Advisory Council, appropriate In-
15 formation Sharing and Analysis Organizations, and
16 other appropriate representatives of State and local
17 governments, shall establish procedures to identify
18 categories of critical cyber infrastructure within each
19 sector of critical infrastructure for the purposes of
20 this Act.

21 (2) DUTIES.—In establishing the procedure
22 under paragraph (1), the Council shall—

23 (A) prioritize efforts based on the
24 prioritization established under subsection (a);

1 (B) incorporate, to the extent practicable,
2 the input of owners and operators, the Critical
3 Infrastructure Partnership Advisory Council,
4 appropriate Information Sharing and Analysis
5 Organizations, and other appropriate represent-
6 atives of the private sector and State and local
7 governments;

8 (C) develop a voluntary mechanism for
9 owners to submit information to assist the
10 Council in making determinations under this
11 section;

12 (D) inform owners and operators of the
13 criteria used to identify categories of critical
14 cyber infrastructure;

15 (E) establish procedures for an owner of
16 critical infrastructure identified as critical cyber
17 infrastructure to challenge the identification;

18 (F) select a member agency to make rec-
19 ommendations to the Council on the identifica-
20 tion of categories of critical cyber infrastruc-
21 ture; and

22 (G) periodically review and update identi-
23 fications under this subsection.

24 (3) IDENTIFICATION REQUIREMENTS.—The
25 Council shall—

1 (A) identify categories of critical cyber in-
2 frastructure within each sector of critical infra-
3 structure and identify owners of critical infra-
4 structure within each category of critical cyber
5 infrastructure;

6 (B) only identify a category of critical in-
7 frastructure as critical cyber infrastructure if
8 damage to or unauthorized access to such crit-
9 ical infrastructure could reasonably result in—

10 (i) the interruption of life-sustaining
11 services, including energy, water, transpor-
12 tation, emergency services, or food, suffi-
13 cient to cause—

14 (I) a mass casualty event; or

15 (II) mass evacuations;

16 (ii) catastrophic economic damage to
17 the United States including—

18 (I) failure or substantial disrup-
19 tion of a financial market of the
20 United States;

21 (II) incapacitation or sustained
22 disruption of a transportation system;
23 or

1 (III) other systemic, long-term
2 damage to the economy of the United
3 States; or

4 (iii) severe degradation of national se-
5 curity or national security capabilities, in-
6 cluding intelligence and defense functions;
7 and

8 (C) consider the sector-by-sector risk as-
9 sessments developed in accordance with sub-
10 section (a).

11 (4) INCIDENT REPORTING.—The Council shall
12 establish procedures under which each owner of crit-
13 ical cyber infrastructure shall report significant
14 cyber incidents affecting critical cyber infrastruc-
15 ture.

16 (5) LIMITATIONS.—The Council may not iden-
17 tify as a category of critical cyber infrastructure
18 under this section—

19 (A) critical infrastructure based solely on
20 activities protected by the first amendment to
21 the Constitution of the United States;

22 (B) an information technology product
23 based solely on a finding that the product is ca-
24 pable of, or is actually, being used in critical
25 cyber infrastructure; or

1 (C) a commercial item that organizes or
2 communicates information electronically.

3 (6) NOTIFICATION OF IDENTIFICATION OF CAT-
4 EGORY OF CRITICAL CYBER INFRASTRUCTURE.—Not
5 later than 10 days after the Council identifies a cat-
6 egory of critical cyber infrastructure under this sec-
7 tion, the Council shall notify the relevant owners of
8 the identified critical cyber infrastructure.

9 (7) DEFINITION.—In this subsection, the term
10 “damage” has the meaning given that term in sec-
11 tion 1030(e) of title 18, United States Code.

12 (c) CONGRESSIONAL NOTICE AND OPPORTUNITY FOR
13 DISAPPROVAL.—

14 (1) NOTIFICATION.—Not later than 10 days
15 after the date on which the Council identifies a cat-
16 egory of critical infrastructure as critical cyber infra-
17 structure under this section, the Council shall—

18 (A) notify Congress of the identification;

19 and

20 (B) submit to Congress a report explaining
21 the basis for the identification.

22 (2) OPPORTUNITY FOR CONGRESSIONAL RE-
23 VIEW.—The identification of a category of critical
24 infrastructure as critical cyber infrastructure shall
25 not take effect for purposes of this title until the

1 date that is 60 days after the date on which the
2 Council notifies Congress under paragraph (1).

3 **SEC. 103. VOLUNTARY CYBERSECURITY PRACTICES.**

4 (a) PRIVATE SECTOR DEVELOPMENT OF CYBERSE-
5 CURITY PRACTICES.—Not later than 180 days after the
6 date of enactment of this Act, each sector coordinating
7 council shall propose to the Council voluntary outcome-
8 based cybersecurity practices (referred to in this section
9 as “cybersecurity practices”) sufficient to effectively reme-
10 diate or mitigate cyber risks identified through an assess-
11 ment conducted under section 102(a) comprised of—

12 (1) industry best practices, standards, and
13 guidelines; or

14 (2) practices developed by the sector coordi-
15 nating council in coordination with owners and oper-
16 ators, voluntary consensus standards development
17 organizations, representatives of State and local gov-
18 ernments, the private sector, and appropriate infor-
19 mation sharing and analysis organizations.

20 (b) REVIEW OF CYBERSECURITY PRACTICES.—

21 (1) IN GENERAL.—The Council shall, in con-
22 sultation with owners and operators, the Critical In-
23 frastructure Partnership Advisory Council, and ap-
24 propriate information sharing and analysis organiza-

1 tions, and in coordination with appropriate rep-
2 resentatives from State and local governments—

3 (A) consult with relevant security experts
4 and institutions of higher education, including
5 university information security centers, appro-
6 priate nongovernmental cybersecurity experts,
7 and representatives from national laboratories;

8 (B) review relevant regulations or compul-
9 sory standards or guidelines;

10 (C) review cybersecurity practices proposed
11 under subsection (a); and

12 (D) consider any amendments to the cyber-
13 security practices and any additional cybersecu-
14 rity practices necessary to ensure adequate re-
15 mediation or mitigation of the cyber risks iden-
16 tified through an assessment conducted under
17 section 102(a).

18 (2) ADOPTION.—

19 (A) IN GENERAL.—Not later than 1 year
20 after the date of enactment of this Act, the
21 Council shall—

22 (i) adopt any cybersecurity practices
23 proposed under subsection (a) that ade-
24 quately remediate or mitigate identified
25 cyber risks and any associated con-

1 sequences identified through an assessment
2 conducted under section 102(a); and

3 (ii) adopt any amended or additional
4 cybersecurity practices necessary to ensure
5 the adequate remediation or mitigation of
6 the cyber risks identified through an as-
7 sessment conducted under section 102(a).

8 (B) NO SUBMISSION BY SECTOR COORDI-
9 NATING COUNCIL.—If a sector coordinating
10 council fails to propose to the Council cyberse-
11 curity practices under subsection (a) within 180
12 days of the date of enactment of this Act, not
13 later than 1 year after the date of enactment of
14 this Act the Council shall adopt cybersecurity
15 practices that adequately remediate or mitigate
16 identified cyber risks and associated con-
17 sequences identified through an assessment con-
18 ducted under section 102(a) for the sector.

19 (c) FLEXIBILITY OF CYBERSECURITY PRACTICES.—

20 Each sector coordinating council and the Council shall pe-
21 riodically assess cybersecurity practices, but not less fre-
22 quently than once every 3 years, and update or modify
23 cybersecurity practices as necessary to ensure adequate re-
24 mediation and mitigation of the cyber risks identified
25 through an assessment conducted under section 102(a).

1 (d) PRIORITIZATION.—Based on the risk assessments
2 performed under section 102(a), the Council shall
3 prioritize the development of cybersecurity practices to en-
4 sure the reduction or mitigation of the greatest cyber
5 risks.

6 (e) PRIVATE SECTOR RECOMMENDED MEASURES.—
7 Each sector coordinating council shall develop voluntary
8 recommended cybersecurity measures that provide owners
9 reasonable and cost-effective methods of meeting any cy-
10 bersecurity practice.

11 (f) TECHNOLOGY NEUTRALITY.—No cybersecurity
12 practice shall require—

13 (1) the use of a specific commercial information
14 technology product; or

15 (2) that a particular commercial information
16 technology product be designed, developed, or manu-
17 factured in a particular manner.

18 (g) RELATIONSHIP TO EXISTING REGULATIONS.—

19 (1) INCLUSION IN REGULATORY REGIMES.—

20 (A) IN GENERAL.—A Federal agency with
21 responsibilities for regulating the security of
22 critical infrastructure may adopt the cybersecu-
23 rity practices as mandatory requirements.

24 (B) REPORTS.—If, as of the date that is
25 1 year after the date of enactment of this Act,

1 a Federal agency with responsibilities for regu-
2 lating the security of critical infrastructure has
3 not adopted the cybersecurity practices as man-
4 datory requirements, the agency shall submit to
5 the appropriate congressional committees a re-
6 port on the reasons the agency did not do so,
7 including a description of whether the critical
8 cyber infrastructure for which the Federal
9 agency has responsibility is maintaining prac-
10 tices sufficient to effectively remediate or miti-
11 gate cyber risks identified through an assess-
12 ment conducted under section 102(a).

13 (C) RULE OF CONSTRUCTION.—Nothing in
14 this subsection shall be construed to provide a
15 Federal agency with authority for regulating
16 the security of critical cyber infrastructure in
17 addition or to a greater extent than the author-
18 ity the Federal agency has under other law.

19 (2) AVOIDANCE OF CONFLICT.—No cybersecu-
20 rity practice shall—

21 (A) prevent an owner (including a certified
22 owner) from complying with any law or regula-
23 tion; or

24 (B) require an owner (including a certified
25 owner) to implement cybersecurity measures

1 that prevent the owner from complying with
2 any law or regulation.

3 (3) AVOIDANCE OF DUPLICATION.—Where reg-
4 ulations or compulsory standards regulate the secu-
5 rity of critical cyber infrastructure, a cybersecurity
6 practice shall, to the greatest extent possible, com-
7 plement or otherwise improve the regulations or
8 compulsory standards.

9 (h) INDEPENDENT REVIEW.—

10 (1) IN GENERAL.—Each cybersecurity practice
11 shall be publicly reviewed by the relevant sector co-
12 ordinating council and the Critical Infrastructure
13 Partnership Advisory Council, which may include
14 input from relevant institutions of higher education,
15 including university information security centers, na-
16 tional laboratories, and appropriate non-govern-
17 mental cybersecurity experts.

18 (2) CONSIDERATION BY COUNCIL.—The Council
19 shall consider any review conducted under paragraph
20 (1).

21 (i) VOLUNTARY TECHNICAL ASSISTANCE.—At the re-
22 quest of an owner or operator of critical infrastructure,
23 the Council shall provide guidance on the application of
24 cybersecurity practices to the critical infrastructure.

1 **SEC. 104. VOLUNTARY CYBERSECURITY PROGRAM FOR**
2 **CRITICAL INFRASTRUCTURE.**

3 (a) VOLUNTARY CYBERSECURITY PROGRAM FOR
4 CRITICAL INFRASTRUCTURE.—

5 (1) IN GENERAL.—Not later than 1 year after
6 the date of enactment of this Act, the Council, in
7 consultation with owners and operators and the Crit-
8 ical Infrastructure Partnership Advisory Council,
9 shall establish the Voluntary Cybersecurity Program
10 for Critical Infrastructure in accordance with this
11 section.

12 (2) ELIGIBILITY.—

13 (A) IN GENERAL.—An owner of critical
14 cyber infrastructure may apply for certification
15 under the Voluntary Cybersecurity Program for
16 Critical Infrastructure.

17 (B) CRITERIA.—The Council shall estab-
18 lish criteria for owners of critical infrastructure
19 that is not critical cyber infrastructure to be eli-
20 gible to apply for certification in the Voluntary
21 Cybersecurity Program for Critical Infrastruc-
22 ture.

23 (3) APPLICATION FOR CERTIFICATION.—An
24 owner of critical cyber infrastructure or an owner of
25 critical infrastructure that meets the criteria estab-

lished under paragraph (2)(B) that applies for certification under this subsection shall—

(A) select and implement cybersecurity measures of their choosing that satisfy the outcome-based cybersecurity practices established under section 103; and

(B)(i) certify in writing and under penalty of perjury to the Council that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103; or

(ii) submit to the Council an assessment verifying that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.

(4) CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i) or an assessment under paragraph (3)(B)(ii) the Council shall certify an owner.

(5) NONPERFORMANCE.—If the Council determines that a certified owner is not in compliance with the cybersecurity practices established under section 103, the Council shall—

1 (A) notify the certified owner of such de-
 2 termination; and

3 (B) work with the certified owner to reme-
 4 diate promptly any deficiencies.

5 (6) REVOCATION.—If a certified owner fails to
 6 remediate promptly any deficiencies identified by the
 7 Council, the Council shall revoke the certification of
 8 the certified owner.

9 (7) REDRESS.—

10 (A) IN GENERAL.—If the Council revokes
 11 a certification under paragraph (6), the Council
 12 shall—

13 (i) notify the owner of such revoca-
 14 tion; and

15 (ii) provide the owner with specific cy-
 16 bersecurity measures that, if implemented,
 17 would remediate any deficiencies.

18 (B) RECERTIFICATION.—If the Council de-
 19 termines that an owner has remedied any defi-
 20 ciencies and is in compliance with the cyberse-
 21 curity practices, the Council may recertify the
 22 owner.

23 (b) ASSESSMENTS.—

24 (1) THIRD-PARTY ASSESSMENTS.—The Council,
 25 in consultation with owners and operators and the

1 Critical Infrastructure Protection Advisory Council,
2 shall enter into agreements with qualified third-
3 party private entities, to conduct assessments that
4 use reliable, repeatable, performance-based evalua-
5 tions and metrics to assess whether an owner cer-
6 tified under subsection (a)(3)(B)(ii) is in compliance
7 with all applicable cybersecurity practices.

8 (2) TRAINING.—The Council shall ensure that
9 third party assessors described in paragraph (1) un-
10 dergo regular training and accreditation.

11 (3) OTHER ASSESSMENTS.—Using the proce-
12 dures developed under this section, the Council may
13 perform cybersecurity assessments of a certified
14 owner based on actual knowledge or a reasonable
15 suspicion that the certified owner is not in compli-
16 ance with the cybersecurity practices or any other
17 risk-based factors as identified by the Council.

18 (4) NOTIFICATION.—The Council shall provide
19 copies of any assessments by the Federal Govern-
20 ment to the certified owner.

21 (5) ACCESS TO INFORMATION.—

22 (A) IN GENERAL.—For the purposes of an
23 assessment conducted under this subsection, a
24 certified owner shall provide the Council, or a

1 third party assessor, any reasonable access nec-
2 essary to complete an assessment.

3 (B) PROTECTION OF INFORMATION.—In-
4 formation provided to the Council, the Council's
5 designee, or any assessor during the course of
6 an assessment under this section shall be pro-
7 tected from disclosure in accordance with sec-
8 tion 106.

9 (c) BENEFITS OF CERTIFICATION.—

10 (1) LIMITATIONS ON CIVIL LIABILITY.—

11 (A) IN GENERAL.—In any civil action for
12 damages directly caused by an incident related
13 to a cyber risk identified through an assessment
14 conducted under section 102(a), a certified
15 owner shall not be liable for any punitive dam-
16 ages intended to punish or deter if the certified
17 owner is in substantial compliance with the ap-
18 propriate cybersecurity practices at the time of
19 the incident related to that cyber risk.

20 (B) LIMITATION.—Subaragraph (A) shall
21 only apply to harm directly caused by the inci-
22 dent related to the cyber risk and shall not
23 apply to damages caused by any additional or
24 intervening acts or omissions by the owner.

1 (2) EXPEDITED SECURITY CLEARANCE PROC-
2 ESS.—The Council, in coordination with the Office
3 of the Director of National Intelligence, shall estab-
4 lish a procedure to expedite the provision of security
5 clearances to appropriate personnel employed by a
6 certified owner.

7 (3) PRIORITIZED TECHNICAL ASSISTANCE.—
8 The Council shall ensure that certified owners are
9 eligible to receive prioritized technical assistance.

10 (4) PROVISION OF CYBER THREAT INFORMA-
11 TION.—The Council shall develop, in coordination
12 with certified owners, a procedure for ensuring that
13 certified owners are, to the maximum extent prac-
14 ticable and consistent with the protection of sources
15 and methods, informed of relevant real-time cyber
16 threat information.

17 (5) PUBLIC RECOGNITION.—With the approval
18 of a certified owner, the Council may publicly recog-
19 nize the certified owner if the Council determines
20 such recognition does not pose a risk to the security
21 of critical cyber infrastructure.

22 (6) STUDY TO EXAMINE BENEFITS OF PRO-
23 CUREMENT PREFERENCE.—

24 (A) IN GENERAL.—The Federal Acquisi-
25 tion Regulatory Council, in coordination with

1 the Council and with input from relevant pri-
2 vate sector individuals and entities, shall con-
3 duct a study examining the potential benefits of
4 establishing a procurement preference for the
5 Federal Government for certified owners.

6 (B) AREAS.—The study under subpara-
7 graph (A) shall include a review of—

8 (i) potential persons and related prop-
9 erty and services that could be eligible for
10 preferential consideration in the procure-
11 ment process;

12 (ii) development and management of
13 an approved list of categories of property
14 and services that could be eligible for pref-
15 erential consideration in the procurement
16 process;

17 (iii) appropriate mechanisms to imple-
18 ment preferential consideration in the pro-
19 curement process, including—

20 (I) establishing a policy encour-
21 aging Federal agencies to conduct
22 market research and industry out-
23 reach to identify property and services
24 that adhere to relevant cybersecurity
25 practices;

1 (II) authorizing the use of a
2 mark for the Voluntary Cybersecurity
3 Program for Critical Infrastructure to
4 be used for marketing property or
5 services to the Federal Government;

6 (III) establishing a policy of en-
7 couraging procurement of certain
8 property and services from an ap-
9 proved list;

10 (IV) authorizing the use of a
11 preference by Federal agencies in the
12 evaluation process; and

13 (V) authorizing a requirement in
14 certain solicitations that the person
15 providing the property or services be a
16 certified owner; and

17 (iv) benefits of and impact on the
18 economy and efficiency of the Federal pro-
19 curement system, if preferential consider-
20 ation were given in the procurement proc-
21 ess to encourage the procurement of prop-
22 erty and services that adhere to relevant
23 baseline performance goals establishing
24 under the Voluntary Cybersecurity Pro-
25 gram for Critical Infrastructure.

1 **SEC. 105. RULES OF CONSTRUCTION.**

2 Nothing in this title shall be construed to—

3 (1) limit the ability of a Federal agency with re-
 4 sponsibilities for regulating the security of critical
 5 infrastructure from requiring that the cybersecurity
 6 practices developed under section 103 be met;

7 (2) provide additional authority for any sector-
 8 specific agency or any Federal agency that is not a
 9 sector-specific agency with responsibilities for regu-
 10 lating the security of critical infrastructure to estab-
 11 lish standards or other cybersecurity measures that
 12 are applicable to the security of critical infrastruc-
 13 ture not otherwise authorized by law;

14 (3) limit or restrict the authority of the Depart-
 15 ment, or any other Federal agency, under any other
 16 provision of law; or

17 (4) permit any owner (including a certified
 18 owner) to fail to comply with any other law or regu-
 19 lation, unless specifically authorized.

20 **SEC. 106. PROTECTION OF INFORMATION.**

21 (a) DEFINITIONS.—In this section—

22 (1) the term “covered information” means any
 23 information—

24 (A) submitted as part of the process estab-
 25 lished under section 102(a)(3);

26 (B) submitted under section 102(b)(2)(C);

1 (C) required to be submitted by owners
2 under section 102(b)(4);

3 (D) provided to the Secretary, the Sec-
4 retary's designee, or any assessor during the
5 course of an assessment under section 104; or

6 (E) provided to the Secretary or the In-
7 spector General of the Department through the
8 tip line or another secure channel established
9 under subsection (c); and

10 (2) the term "Inspector General" means an In-
11 spector General described in subparagraph (A), (B),
12 or (I) of section 11(b)(1) of the Inspector General
13 Act of 1978 (5 U.S.C. App.), the Inspector General
14 of the United States Postal Service, the Inspector
15 General of the Central Intelligence Agency, and the
16 Inspector General of the Intelligence Community.

17 (b) CRITICAL INFRASTRUCTURE INFORMATION.—

18 (1) IN GENERAL.—Covered information shall be
19 treated as voluntarily shared critical infrastructure
20 information under section 214 of the Homeland Se-
21 curity Act of 2002 (6 U.S.C. 133), except that the
22 requirement of such section 214 that the informa-
23 tion be voluntarily submitted shall not be required
24 for protection of information under this section to
25 apply.

1 (2) SAVINGS CLAUSE FOR EXISTING WHISTLE-
 2 BLOWER PROTECTIONS.—With respect to covered in-
 3 formation, the rights and protections relating to dis-
 4 closure by individuals of voluntarily shared critical
 5 infrastructure information submitted under subtitle
 6 B of title II of the Homeland Security Act of 2002
 7 (6 U.S.C. 131 et seq.) shall apply with respect to
 8 disclosure of the covered information by individuals.

9 (c) CRITICAL INFRASTRUCTURE CYBER SECURITY
 10 TIP LINE.—

11 (1) IN GENERAL.—The Secretary shall establish
 12 and publicize the availability of a Critical Infrastruc-
 13 ture Cyber Security Tip Line (and any other secure
 14 means the Secretary determines would be desirable
 15 to establish), by which individuals may report—

16 (A) concerns involving the security of cov-
 17 ered critical infrastructure against cyber risks;
 18 and

19 (B) concerns (in addition to any concerns
 20 described under subparagraph (A)) with respect
 21 to programs and functions authorized or funded
 22 under this title involving—

23 (i) a possible violation of any law,
 24 rule, regulation or guideline;

25 (ii) mismanagement;

1 (iii) risk to public health, safety, secu-
2 rity, or privacy; or

3 (iv) other misfeasance or nonfeasance.

4 (2) DESIGNATION OF EMPLOYEES.—The Sec-
5 retary and the Inspector General of the Department
6 shall each designate employees authorized to receive
7 concerns reported under this subsection that in-
8 clude—

9 (A) disclosure of covered information; or

10 (B) any other disclosure of information
11 that is specifically prohibited by law or is spe-
12 cifically required by Executive order to be kept
13 secret in the interest of national defense or the
14 conduct of foreign affairs.

15 (3) HANDLING OF CERTAIN CONCERNS.—A
16 concern described in paragraph (1)(B)—

17 (A) shall be received initially to the Inspec-
18 tor General of the Department;

19 (B) shall not be provided initially to the
20 Secretary; and

21 (C) may be provided to the Secretary if de-
22 termined appropriate by the Inspector General
23 of the Department.

24 (d) RULES OF CONSTRUCTION.—Nothing in this sec-
25 tion shall be construed to—

1 (1) limit or otherwise affect the right, ability,
2 duty, or obligation of any entity to use or disclose
3 any information of that entity, including in the con-
4 duct of any judicial or other proceeding;

5 (2) prevent the classification of information
6 submitted under this section if that information
7 meets the standards for classification under Execu-
8 tive Order 12958, or any successor thereto, or affect
9 measures and controls relating to the protection of
10 classified information as prescribed by Federal stat-
11 ute or under Executive Order 12958, or any suc-
12 cessor thereto;

13 (3) limit or otherwise affect the ability of an en-
14 tity, agency, or authority of a State, a local govern-
15 ment, or the Federal Government or any other indi-
16 vidual or entity under applicable law to obtain infor-
17 mation that is not covered information (including
18 any information lawfully and properly disclosed gen-
19 erally or broadly to the public) and to use such in-
20 formation in any manner permitted by law, including
21 the disclosure of such information under—

22 (A) section 552 or 2302(b)(8) of title 5,
23 United States Code;

24 (B) section 2409 of title 10, United States
25 Code; or

1 (C) any other Federal, State, or local law,
2 ordinance, or regulation that protects against
3 retaliation an individual who discloses informa-
4 tion that the individual reasonably believes evi-
5 dences a violation of any law, rule, or regula-
6 tion, gross mismanagement, substantial and
7 specific danger to public health, safety, or secu-
8 rity, or other misfeasance or nonfeasance;

9 (4) prevent the Secretary from using informa-
10 tion required to be submitted under this Act for en-
11 forcement of this title, including enforcement pro-
12 ceedings subject to appropriate safeguards;

13 (5) authorize information to be withheld from
14 any committee of Congress, the Comptroller General,
15 or any Inspector General;

16 (6) affect protections afforded to trade secrets
17 under any other provision of law; or

18 (7) create a private right of action for enforce-
19 ment of any provision of this section.

20 (e) AUDIT.—

21 (1) IN GENERAL.—Not later than 1 year after
22 the date of enactment of this Act, the Inspector
23 General of the Department shall conduct an audit of
24 the management of covered information under this

1 title and report the findings to appropriate congres-
2 sional committees.

3 (2) CONTENTS.—The audit under paragraph
4 (1) shall include assessments of—

5 (A) whether the covered information is
6 adequately safeguarded against inappropriate
7 disclosure;

8 (B) the processes for marking and dissemi-
9 nating the covered information and resolving
10 any disputes;

11 (C) how the covered information is used
12 for the purposes of this title, and whether that
13 use is effective;

14 (D) whether sharing of covered informa-
15 tion has been effective to fulfill the purposes of
16 this title;

17 (E) whether the kinds of covered informa-
18 tion submitted have been appropriate and use-
19 ful, or overbroad or overnarrow;

20 (F) whether the protections of covered in-
21 formation allow for adequate accountability and
22 transparency of the regulatory, enforcement,
23 and other aspects of implementing this title;
24 and

1 (G) any other factors at the discretion of
2 the Inspector General of the Department.

3 **SEC. 107. ANNUAL ASSESSMENT OF CYBERSECURITY.**

4 (a) IN GENERAL.—Not later than 1 year after the
5 date of enactment of this Act, and every year thereafter,
6 the Council shall submit to the appropriate congressional
7 committees a report on the effectiveness of this title in
8 reducing the risk of cyber attack to critical infrastructure.

9 (b) CONTENTS.—Each report submitted under sub-
10 section (a) shall include—

11 (1) a discussion of cyber risks and associated
12 consequences and whether the cybersecurity prac-
13 tices developed under section 103 are sufficient to
14 effectively remediate and mitigate cyber risks and
15 associated consequences; and

16 (2) an analysis of—

17 (A) whether owners of critical cyber infra-
18 structure are successfully implementing the cy-
19 bersecurity practices adopted under section 103;

20 (B) whether the critical infrastructure of
21 the United States is effectively secured from cy-
22 bersecurity threats, vulnerabilities, and con-
23 sequences;

24 (C) whether Federal agencies with respon-
25 sibilities for regulating the security of critical

1 infrastructure are adequately adopting and en-
 2 forcing the cybersecurity practices adopted
 3 under section 103; and

4 (D) whether additional legislative authority
 5 or other actions are needed to effectively reme-
 6 diate or mitigate cyber risks and associated
 7 consequences.

8 (c) FORM OF REPORT.—A report submitted under
 9 this subsection shall be submitted in an unclassified form,
 10 but may include a classified annex, if necessary.

11 **SEC. 108. INTERNATIONAL COOPERATION.**

12 (a) IN GENERAL.—The Secretary, in coordination
 13 with the Secretary of State, the heads of appropriate sec-
 14 tor-specific agencies, and the heads of any appropriate
 15 Federal agency with responsibilities for regulating the se-
 16 curity of covered critical infrastructure, shall—

17 (1) consistent with the protection of intelligence
 18 sources and methods and other sensitive matters, in-
 19 form the owner or operator of information infra-
 20 structure located outside the United States the dis-
 21 ruption of which could result in national or regional
 22 catastrophic damage within the United States and
 23 the government of the country in which the informa-
 24 tion infrastructure is located of any cyber risks to
 25 such information infrastructure; and

1 (2) coordinate with the government of the coun-
 2 try in which such information infrastructure is lo-
 3 cated and, as appropriate, the owner or operator of
 4 the information infrastructure regarding the imple-
 5 mentation of cybersecurity measures or other meas-
 6 ures to the information infrastructure to mitigate or
 7 remediate cyber risks.

8 (b) INTERNATIONAL AGREEMENTS.—The Secretary,
 9 in coordination with the Secretary of State, including in
 10 particular with the interpretation of international agree-
 11 ments, shall perform the functions prescribed by this sec-
 12 tion consistent with applicable international agreements.

13 **SEC. 109. EFFECT ON OTHER LAWS.**

14 Except as expressly provided in section 104(c)(1) and
 15 section 106, nothing in this Act shall be construed to pre-
 16 empt the applicability of any State law or requirement.

17 **SEC. 110. DEFINITIONS.**

18 In this title:

19 (1) CERTIFIED OWNER.—The term “certified
 20 owner” means an owner of critical cyber infrastruc-
 21 ture or an owner of critical infrastructure that is
 22 certified by the Council under section 104(a)(4).

23 (2) CYBER RISK.—The term “cyber risk”
 24 means any risk to information infrastructure, includ-
 25 ing physical or personnel risks and security

1 vulnerabilities, that, if exploited or not mitigated,
2 could pose a significant risk of disruption to the op-
3 eration of information infrastructure essential to the
4 reliable operation of critical infrastructure.

5 (3) SECTOR COORDINATING COUNCIL.—The
6 term “sector coordinating council” means a private
7 sector coordinating council comprised of representa-
8 tives of owners and operators within a particular
9 sector of critical infrastructure established by the
10 National Infrastructure Protection Plan.

11 (4) SECTOR-SPECIFIC AGENCY.—The term “sec-
12 tor-specific agency” means the relevant Federal
13 agency responsible for infrastructure protection ac-
14 tivities in a designated critical infrastructure sector
15 or key resources category under the National Infra-
16 structure Protection Plan, or any other appropriate
17 Federal agency identified by the President after the
18 date of enactment of this Act.

1 **TITLE II—FEDERAL INFORMA-**
 2 **TION SECURITY MANAGE-**
 3 **MENT AND CONSOLIDATING**
 4 **RESOURCES**

5 **SEC. 201. FISMA REFORM.**

6 (a) IN GENERAL.—Chapter 35 of title 44, United
 7 States Code, is amended by striking subchapters II and
 8 III and inserting the following:

9 “SUBCHAPTER II—INFORMATION SECURITY

10 **“§ 3551. Purposes**

11 “The purposes of this subchapter are to—

12 “(1) provide a comprehensive framework for en-
 13 suring the effectiveness of information security con-
 14 trols over information resources that support Fed-
 15 eral operations and assets;

16 “(2) recognize the highly networked nature of
 17 the Federal computing environment and provide ef-
 18 fective governmentwide management of policies, di-
 19 rectives, standards, and guidelines, as well as effec-
 20 tive and nimble oversight of and response to infor-
 21 mation security risks, including coordination of in-
 22 formation security efforts throughout the Federal ci-
 23 vilian, national security, and law enforcement com-
 24 munities;

1 “(3) provide for development and maintenance
 2 of controls required to protect agency information
 3 and information systems and contribute to the over-
 4 all improvement of agency information security pos-
 5 ture; and

6 “(4) provide a mechanism to improve and con-
 7 tinuously monitor the security of agency information
 8 security programs and systems through a focus on
 9 continuous monitoring of agency information sys-
 10 tems and streamlined reporting requirements rather
 11 than overly prescriptive manual reporting.

12 **“§ 3552. Definitions**

13 “(a) IN GENERAL.—Except as provided under sub-
 14 section (b), the definitions under section 3502 (including
 15 the definitions of the terms ‘agency’ and ‘information sys-
 16 tem’) shall apply to this subchapter.

17 “(b) OTHER TERMS.—In this subchapter:

18 “(1) ADEQUATE SECURITY.—The term ‘ade-
 19 quate security’ means security commensurate with
 20 the risk and impact resulting from the unauthorized
 21 access to or loss, misuse, destruction, or modifica-
 22 tion of information.

23 “(2) CONTINUOUS MONITORING.—The term
 24 ‘continuous monitoring’ means the ongoing real time
 25 or near real-time process used to determine if the

1 complete set of planned, required, and deployed se-
2 curity controls within an information system con-
3 tinue to be effective over time in light of rapidly
4 changing information technology and threat develop-
5 ment. To the maximum extent possible, this also re-
6 quires automation of that process to enable cost ef-
7 fective, efficient, and consistent monitoring and pro-
8 vide a more dynamic view of the security state of
9 those deployed controls.

10 “(3) COUNTERMEASURE.—The term ‘counter-
11 measure’ means automated or manual actions with
12 defensive intent to modify or block data packets as-
13 sociated with electronic or wire communications,
14 Internet traffic, program code, or other system traf-
15 fic transiting to or from or stored on an information
16 system for the purpose of protecting the information
17 system from cybersecurity threats, conducted on an
18 information system owned or operated by or on be-
19 half of the party to be protected or operated by a
20 private entity acting as a provider of electronic com-
21 munication services, remote computing services, or
22 cybersecurity services to the party to be protected.

23 “(4) INCIDENT.—The term ‘incident’ means an
24 occurrence that—

1 “(A) actually or imminently jeopardizes,
2 without lawful authority, the integrity, con-
3 fidentiality, or availability of information or an
4 information system; or

5 “(B) constitutes a violation or imminent
6 threat of violation of law, security policies, secu-
7 rity procedures, or acceptable use policies.

8 “(5) INFORMATION SECURITY.—The term ‘in-
9 formation security’ means protecting information
10 and information systems from unauthorized access,
11 use, disclosure, disruption, modification, or destruc-
12 tion in order to provide—

13 “(A) integrity, which means guarding
14 against improper information modification or
15 destruction, and includes ensuring nonrepudi-
16 ation and authenticity;

17 “(B) confidentiality, which means pre-
18 serving authorized restrictions on access and
19 disclosure, including means for protecting per-
20 sonal privacy and proprietary information; and

21 “(C) availability, which means ensuring
22 timely and reliable access to and use of infor-
23 mation.

1 “(6) INFORMATION TECHNOLOGY.—The term
 2 ‘information technology’ has the meaning given that
 3 term in section 11101 of title 40.

4 “(7) NATIONAL SECURITY SYSTEM.—

5 “(A) IN GENERAL.—The term ‘national se-
 6 curity system’ means any information system
 7 (including any telecommunications system) used
 8 or operated by an agency or by a contractor of
 9 an agency, or other organization on behalf of an
 10 agency—

11 “(i) the function, operation, or use of
 12 which—

13 “(I) involves intelligence activi-
 14 ties;

15 “(II) involves cryptologic activi-
 16 ties related to national security;

17 “(III) involves command and
 18 control of military forces;

19 “(IV) involves equipment that is
 20 an integral part of a weapon or weap-
 21 ons system; or

22 “(V) subject to subparagraph
 23 (B), is critical to the direct fulfillment
 24 of military or intelligence missions; or

1 “(ii) that is protected at all times by
 2 procedures established for information that
 3 have been specifically authorized under cri-
 4 teria established by an Executive order or
 5 an Act of Congress to be kept classified in
 6 the interest of national defense or foreign
 7 policy.

8 “(B) EXCLUSION.—Subparagraph
 9 (A)(i)(V) does not include a system that is to
 10 be used for routine administrative and business
 11 applications (including payroll, finance, logis-
 12 tics, and personnel management applications).

13 “(8) SECRETARY.—The term ‘Secretary’ means
 14 the Secretary of Homeland Security.

15 **“§ 3553. Federal information security authority and**
 16 **coordination**

17 “(a) IN GENERAL.—Except as provided in sub-
 18 sections (f) and (g), the Secretary shall oversee agency in-
 19 formation security policies and practices, including the de-
 20 velopment and oversight of information security policies
 21 and directives and compliance with this subchapter.

22 “(b) DUTIES.—The Secretary shall—

23 “(1) develop, issue, and oversee the implemen-
 24 tation of information security policies and directives,
 25 which shall be compulsory and binding on agencies

1 to the extent determined appropriate by the Sec-
2 retary, including—

3 “(A) policies and directives consistent with
4 the standards promulgated under section 11331
5 of title 40 to identify and provide information
6 security protections that are commensurate
7 with the risk and impact resulting from the un-
8 authorized access, use, disclosure, disruption,
9 modification, or destruction of—

10 “(i) information collected, created,
11 processed, stored, disseminated, or other-
12 wise used or maintained by or on behalf of
13 an agency; or

14 “(ii) information systems used or op-
15 erated by an agency or by a contractor of
16 an agency or other organization, such as a
17 State government entity, on behalf of an
18 agency;

19 “(B) minimum operational requirements
20 for network operations centers and security op-
21 erations centers of agencies to facilitate the
22 protection of and provide common situational
23 awareness for all agency information and infor-
24 mation systems;

1 “(C) reporting requirements, consistent
2 with relevant law, regarding information secu-
3 rity incidents;

4 “(D) requirements for agencywide informa-
5 tion security programs, including continuous
6 monitoring of information security;

7 “(E) performance requirements and
8 metrics for the security of agency information
9 systems;

10 “(F) training requirements to ensure that
11 agencies are able to fully and timely comply
12 with directions issued by the Secretary under
13 this subchapter;

14 “(G) training requirements regarding pri-
15 vacy, civil rights, civil liberties, and information
16 oversight for agency information security em-
17 ployees;

18 “(H) requirements for the annual reports
19 to the Secretary under section 3554(c); and

20 “(I) any other information security re-
21 quirements as determined by the Secretary;

22 “(2) review agency information security pro-
23 grams required to be developed under section
24 3554(b);

1 “(3) develop and conduct targeted risk assess-
2 ments and operational evaluations for agency infor-
3 mation and information systems in consultation with
4 the heads of other agencies or governmental and pri-
5 vate entities that own and operate such systems,
6 that may include threat, vulnerability, and impact
7 assessments and penetration testing;

8 “(4) operate consolidated intrusion detection,
9 prevention, or other protective capabilities and use
10 associated countermeasures for the purpose of pro-
11 tecting agency information and information systems
12 from information security threats;

13 “(5) in conjunction with other agencies and the
14 private sector, assess and foster the development of
15 information security technologies and capabilities for
16 use across multiple agencies;

17 “(6) designate an entity to receive reports and
18 information about information security incidents,
19 threats, and vulnerabilities affecting agency informa-
20 tion systems;

21 “(7) provide incident detection, analysis, miti-
22 gation, and response information and remote or on-
23 site technical assistance to the heads of agencies;

24 “(8) coordinate with appropriate agencies and
25 officials to ensure, to the maximum extent feasible,

1 that policies and directives issued under paragraph
2 (1) are complementary with—

3 “(A) standards and guidelines developed
4 for national security systems; and

5 “(B) policies and directives issues by the
6 Secretary of Defense, Director of the Central
7 Intelligence Agency, and Director of National
8 Intelligence under subsection (g)(1); and

9 “(9) not later than March 1 of each year, sub-
10 mit to Congress a report on agency compliance with
11 the requirements of this subchapter, which shall in-
12 clude—

13 “(A) a summary of the incidents described
14 by the reports required in section 3554(c);

15 “(B) a summary of the results of assess-
16 ments required by section 3555;

17 “(C) a summary of the results of evalua-
18 tions required by section 3556;

19 “(D) significant deficiencies in agency in-
20 formation security practices as identified in the
21 reports, assessments, and evaluations referred
22 to in subparagraphs (A), (B), and (C), or other-
23 wise; and

1 “(E) planned remedial action to address
2 any deficiencies identified under subparagraph
3 (D).

4 “(c) ISSUING POLICIES AND DIRECTIVES.—When
5 issuing policies and directives under subsection (b), the
6 Secretary shall consider any applicable standards or guide-
7 lines developed by the National Institute of Standards and
8 Technology and issued by the Secretary of Commerce
9 under section 11331 of title 40. The Secretary shall con-
10 sult with the Director of the National Institute of Stand-
11 ards and Technology when such policies and directives im-
12 plement standards or guidelines developed by National In-
13 stitute of Standards and Technology. To the maximum ex-
14 tent feasible, such standards and guidelines shall be com-
15 plementary with standards and guidelines developed for
16 national security systems.

17 “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

18 “(1) IN GENERAL.—Notwithstanding any other
19 provision of law, in carrying out the responsibilities
20 under paragraphs (3) and (4) of subsection (b), if
21 the Secretary makes a certification described in
22 paragraph (2), the Secretary may acquire, intercept,
23 retain, use, and disclose communications and other
24 system traffic that are transiting to or from or
25 stored on agency information systems and deploy

1 countermeasures with regard to the communications
2 and system traffic.

3 “(2) CERTIFICATION.—A certification described
4 in this paragraph is a certification by the Secretary
5 that—

6 “(A) the acquisitions, interceptions, and
7 countermeasures are reasonably necessary for
8 the purpose of protecting agency information
9 systems from information security threats;

10 “(B) the content of communications will be
11 collected and retained only when the commu-
12 nication is associated with a known or reason-
13 ably suspected information security threat, and
14 communications and system traffic will not be
15 subject to the operation of a countermeasure
16 unless associated with the threats;

17 “(C) information obtained under activities
18 authorized under this subsection will only be re-
19 tained, used, or disclosed to protect agency in-
20 formation systems from information security
21 threats, mitigate against such threats, or, with
22 the approval of the Attorney General, for law
23 enforcement purposes when—

1 “(i) the information is evidence of a
2 crime that has been, is being, or is about
3 to be committed; and

4 “(ii) disclosure of the information to a
5 law enforcement agency is not otherwise
6 prohibited by law;

7 “(D) notice has been provided to users of
8 agency information systems concerning the po-
9 tential for acquisition, interception, retention,
10 use, and disclosure of communications and
11 other system traffic; and

12 “(E) the activities are implemented pursu-
13 ant to policies and procedures governing the ac-
14 quisition, interception, retention, use, and dis-
15 closure of communications and other system
16 traffic that have been reviewed and approved by
17 the Attorney General.

18 “(3) PRIVATE ENTITIES.—The Secretary may
19 enter into contracts or other agreements, or other-
20 wise request and obtain the assistance of, private en-
21 tities that provide electronic communication or infor-
22 mation security services to acquire, intercept, retain,
23 use, and disclose communications and other system
24 traffic or to deploy countermeasures in accordance
25 with this subsection.

1 “(e) DIRECTIONS TO AGENCIES.—

2 “(1) AUTHORITY.—

3 “(A) IN GENERAL.—Notwithstanding sec-
4 tion 3554, and subject to subparagraph (B), in
5 response to a known or reasonably suspected in-
6 formation security threat, vulnerability, or inci-
7 dent that represents a substantial threat to the
8 information security of an agency, the Secretary
9 may direct other agency heads to take any law-
10 ful action with respect to the operation of the
11 information systems, including those owned or
12 operated by another entity on behalf of an
13 agency, that collect, process, store, transmit,
14 disseminate, or otherwise maintain agency in-
15 formation, for the purpose of protecting the in-
16 formation system from or mitigating an infor-
17 mation security threat.

18 “(B) EXCEPTION.—The authorities of the
19 Secretary under this subsection shall not apply
20 to a system described in paragraph (2), (3), or
21 (4) of subsection (g).

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

23 The Secretary shall—

24 “(A) in coordination with the Director of
25 the Office of Management and Budget and, as

appropriate, in consultation with operators of information systems, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

“(i) thresholds and other criteria;

“(ii) privacy and civil liberties protections; and

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

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

“(C) minimize the impact of directives under this subsection by—

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

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

“(D) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of a directive under this subsection.

“(3) IMMINENT THREATS.—

1 “(A) IN GENERAL.—If the Secretary deter-
2 mines that there is an imminent threat to agen-
3 cy information systems and a directive under
4 this subsection is not reasonably likely to result
5 in a timely response to the threat, the Secretary
6 may authorize the use of protective capabilities
7 under the control of the Secretary for commu-
8 nications or other system traffic transiting to or
9 from or stored on an agency information system
10 without prior consultation with the affected
11 agency for the purpose of ensuring the security
12 of the information or information system or
13 other agency information systems.

14 “(B) LIMITATION ON DELEGATION.—The
15 authority under this paragraph may not be del-
16 egated to an official in a position lower than
17 Assistant Secretary or Director of the National
18 Cybersecurity and Communications Integration
19 Center.

20 “(C) NOTICE.—The Secretary or designee
21 of the Secretary shall immediately notify the
22 Director of the Office of Management and
23 Budget and the head and chief information offi-
24 cer (or equivalent official) of each affected
25 agency of—

1 “(i) any action taken under this sub-
2 section; and

3 “(ii) the reasons for and duration and
4 nature of the action.

5 “(D) OTHER LAW.—The actions of the
6 Secretary under this paragraph shall be con-
7 sistent with applicable law.

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

11 “(A) protect agency information from un-
12 authorized access, use, disclosure, disruption,
13 modification, or destruction; or

14 “(B) require the remediation of or protect
15 against identified information security risks
16 with respect to—

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

19 “(ii) that portion of an information
20 system used or operated by an agency or
21 by a contractor of an agency or other orga-
22 nization on behalf of an agency.

23 “(f) NATIONAL SECURITY SYSTEMS.—

24 “(1) IN GENERAL.—This section shall not apply
25 to a national security system.

1 “(2) INFORMATION SECURITY.—Information se-
2 curity policies, directives, standards, and guidelines
3 for national security systems shall be overseen as di-
4 rected by the President and, in accordance with that
5 direction, carried out under the authority of the
6 heads of agencies that operate or exercise authority
7 over national security systems.

8 “(g) DELEGATION OF AUTHORITIES.—

9 “(1) IN GENERAL.—The authorities of the Sec-
10 retary described in paragraphs (1), (2), (3), and (4)
11 of subsection (b) shall be delegated to—

12 “(A) the Secretary of Defense in the case
13 of systems described in paragraph (2);

14 “(B) the Director of the Central Intel-
15 ligence Agency in the case of systems described
16 in paragraph (3); and

17 “(C) the Director of National Intelligence
18 in the case of systems described in paragraph
19 (4).

20 “(2) DEPARTMENT OF DEFENSE.—The systems
21 described in this paragraph are systems that are op-
22 erated by the Department of Defense, a contractor
23 of the Department of Defense, or another entity on
24 behalf of the Department of Defense that process
25 any information the unauthorized access, use, disclo-

1 sure, disruption, modification, or destruction of
2 which would have a debilitating impact on the mis-
3 sion of the Department of Defense.

4 “(3) CENTRAL INTELLIGENCE AGENCY.—The
5 systems described in this paragraph are systems
6 that are operated by the Central Intelligence Agen-
7 cy, a contractor of the Central Intelligence Agency,
8 or another entity on behalf of the Central Intel-
9 ligence Agency that process any information the un-
10 authorized access, use, disclosure, disruption, modi-
11 fication, or destruction of which would have a debili-
12 tating impact on the mission of the Central Intel-
13 ligence Agency.

14 “(4) OFFICE OF THE DIRECTOR OF NATIONAL
15 INTELLIGENCE.—The systems described in this
16 paragraph are systems that are operated by the Of-
17 fice of the Director of National Intelligence, a con-
18 tractor of the Office of the Director of National In-
19 telligence, or another entity on behalf of the Office
20 of the Director of National Intelligence that process
21 any information the unauthorized access, use, disclo-
22 sure, disruption, modification, or destruction of
23 which would have a debilitating impact on the mis-
24 sion of the Office of the Director of National Intel-
25 ligence.

1 “(5) INTEGRATION OF INFORMATION.—The
 2 Secretary of Defense, the Director of the Central In-
 3 telligence Agency, and the Director of National In-
 4 telligence shall carry out their responsibilities under
 5 this subsection in coordination with the Secretary
 6 and share relevant information in a timely manner
 7 with the Secretary relating to the security of agency
 8 information and information systems, including sys-
 9 tems described in paragraphs (2), (3), and (4), to
 10 enable the Secretary to carry out the responsibilities
 11 set forth in this section and to maintain comprehen-
 12 sive situational awareness regarding information se-
 13 curity incidents, threats, and vulnerabilities affecting
 14 agency information systems, consistent with stand-
 15 ards and guidelines for national security systems,
 16 issued in accordance with law and as directed by the
 17 President.

18 **“§ 3554. Agency responsibilities**

19 “(a) IN GENERAL.—The head of each agency shall—
 20 “(1) be responsible for—
 21 “(A) providing information security protec-
 22 tions commensurate with the risk resulting
 23 from unauthorized access, use, disclosure, dis-
 24 ruption, modification, or destruction of—

1 “(i) information collected, created,
2 processed, stored, disseminated, or other-
3 wise used or maintained by or on behalf of
4 the agency; or

5 “(ii) information systems used or op-
6 erated by the agency or by a contractor of
7 the agency or other organization, such as
8 a State government entity, on behalf of the
9 agency;

10 “(B) complying with this subchapter, in-
11 cluding—

12 “(i) the policies and directives issued
13 under section 3553, including any direc-
14 tions under section 3553(e); and

15 “(ii) information security policies, di-
16 rectives, standards, and guidelines for na-
17 tional security systems issued in accord-
18 ance with law and as directed by the Presi-
19 dent;

20 “(C) complying with the requirements of
21 the information security standards prescribed
22 under section 11331 of title 40, including any
23 required security configuration checklists; and

24 “(D) ensuring that information security
25 management processes are integrated with

1 agency strategic and operational planning proc-
2 esses;

3 “(2) ensure that senior agency officials provide
4 information security for the information and infor-
5 mation systems that support the operations and as-
6 sets under the control of the officials, including
7 through—

8 “(A) assessing, with a frequency commen-
9 surate with risk, the risk and impact that could
10 result from the unauthorized access, use, disclo-
11 sure, disruption, modification, or destruction of
12 the information or information systems;

13 “(B) determining the levels of information
14 security appropriate to protect the information
15 and information systems in accordance with the
16 policies and directives issued under section
17 3553(b) and standards prescribed under section
18 11331 of title 40;

19 “(C) implementing policies, procedures,
20 and capabilities to reduce risks to an acceptable
21 level in a cost-effective manner;

22 “(D) security testing and evaluation, in-
23 cluding continuously monitoring the effective
24 implementation of information security controls
25 and techniques, threats, vulnerabilities, assets,

1 and other aspects of information security as ap-
2 propriate; and

3 “(E) reporting information about informa-
4 tion security incidents, threats, and
5 vulnerabilities in a timely manner as required
6 under policies and procedures established under
7 subsection (b)(7);

8 “(3) assess and maintain the resiliency of infor-
9 mation systems critical to the mission and oper-
10 ations of the agency;

11 “(4) delegate to the chief information officer or
12 equivalent official (or to a senior agency official who
13 reports to the chief information officer or equivalent
14 official) the authority to ensure and primary respon-
15 sibility for ensuring compliance with this subchapter,
16 including—

17 “(A) overseeing the establishment and
18 maintenance of an agencywide security oper-
19 ations capability that on a continuous basis
20 can—

21 “(i) detect, report, respond to, con-
22 tain, and mitigate information security in-
23 cidents that impair adequate security of
24 the agency information and information
25 systems in a timely manner and in accord-

1 ance with the policies and directives issued
2 under section 3553(b); and

3 “(ii) report any information security
4 incident described under clause (i) to the
5 entity designated under section 3553(b)(6);

6 “(B) developing, maintaining, and over-
7 seeing an agencywide information security pro-
8 gram as required under subsection (b);

9 “(C) developing, maintaining, and over-
10 seeing information security policies, procedures,
11 and control techniques to address all applicable
12 requirements, including those issued under sec-
13 tion 3553 and section 11331 of title 40;

14 “(D) training and overseeing employees
15 and contractors of the agency with significant
16 responsibilities for information security with re-
17 spect to such responsibilities; and

18 “(E) assisting senior agency officials con-
19 cerning their responsibilities under paragraph
20 (2);

21 “(5) the agency has trained and obtained secu-
22 rity clearances for an adequate number of employees
23 to assist the agency in complying with this sub-
24 chapter, including the policies and directives issued
25 under section 3553(b);

1 “(6) ensure that the chief information officer
2 (or other senior agency official designated under
3 paragraph (4)), in coordination with other senior
4 agency officials, reports to the head of the agency on
5 the effectiveness of the agency information security
6 program, including the progress of remedial actions;

7 “(7) ensure that the chief information officer
8 (or other senior agency official designated under
9 paragraph (4))—

10 “(A) possesses the necessary qualifications
11 to administer the duties of the official under
12 this subchapter; and

13 “(B) has information security duties as a
14 primary duty of the official; and

15 “(8) ensure that senior agency officials (includ-
16 ing component chief information officers or equiva-
17 lent officials) carry out responsibilities under this
18 subchapter as directed by the official delegated au-
19 thority under paragraph (4).

20 “(b) AGENCY PROGRAM.—The head of each agency
21 shall develop, document, and implement an agencywide in-
22 formation security program, which shall be reviewed under
23 section 3553(b)(2), to provide information security for the
24 information and information systems that support the op-
25 erations and assets of the agency, including those provided

1 or managed by another agency, contractor, or other
2 source, which shall include—

3 “(1) the development, execution, and mainte-
4 nance of a risk management strategy for information
5 security that—

6 “(A) considers information security
7 threats, vulnerabilities, and consequences;

8 “(B) includes periodic assessments and re-
9 porting of risk, with a frequency commensurate
10 with risk and impact;

11 “(2) policies and procedures that—

12 “(A) are based on the risk management
13 strategy and assessment results required under
14 paragraph (1);

15 “(B) reduce information security risks to
16 an acceptable level in a cost-effective manner;

17 “(C) ensure that cost-effective and ade-
18 quate information security is addressed
19 throughout the life cycle of each agency infor-
20 mation system; and

21 “(D) ensure compliance with—

22 “(i) this subchapter;

23 “(ii) the information security policies
24 and directives issued under section
25 3553(b); and

1 “(iii) any other applicable require-
2 ments;

3 “(3) subordinate plans for providing adequate
4 information security for networks, facilities, and sys-
5 tems or groups of information systems;

6 “(4) security awareness training developed in
7 accordance with the requirements issued under sec-
8 tion 3553(b) to inform individuals with access to
9 agency information systems, including information
10 security employees, contractors, and other users of
11 information systems that support the operations and
12 assets of the agency, of—

13 “(A) information security risks associated
14 with their activities;

15 “(B) their responsibilities in complying
16 with agency policies and procedures designed to
17 reduce those risks;

18 “(C) requirements for fulfilling privacy,
19 civil rights, civil liberties, and other information
20 oversight responsibilities; and

21 “(D) methods for individuals to report
22 risks and incidents to relevant Offices of In-
23 spectors General and the Secretary under sec-
24 tion 106 of the Cybersecurity Act of 2012;

1 “(5) security testing and evaluation commensu-
2 rate with risk and impact that includes—

3 “(A) risk-based continuous monitoring of
4 the operational status and security of agency
5 information systems to enable evaluation of the
6 effectiveness of and compliance with informa-
7 tion security policies, procedures, and practices,
8 including a relevant and appropriate selection of
9 management, operational, and technical controls
10 of information systems identified in the inven-
11 tory required under section 3505(c);

12 “(B) penetration testing exercises and
13 operational evaluations in accordance with the
14 requirements issued under section 3553(b) to
15 evaluate whether the agency adequately protects
16 against, detects, and responds to incidents;

17 “(C) vulnerability scanning, intrusion de-
18 tection and prevention, and penetration testing,
19 in accordance with the requirements issued
20 under section 3553(b); and

21 “(D) any other periodic testing and evalua-
22 tion, in accordance with the requirements
23 issued under section 3553(b);

24 “(6) a process for ensuring that remedial ac-
25 tions are taken to mitigate information security

1 vulnerabilities commensurate with risk and impact,
2 and otherwise address any deficiencies in the infor-
3 mation security policies, procedures, and practices of
4 the agency;

5 “(7) policies and procedures to ensure detec-
6 tion, mitigation, reporting, and responses to infor-
7 mation security incidents, in accordance with the
8 policies and directives issued under section 3553(b),
9 including—

10 “(A) ensuring timely internal reporting of
11 information security incidents;

12 “(B) establishing and maintaining appro-
13 priate technical capabilities to detect and miti-
14 gate risks associated with information security
15 incidents;

16 “(C) notifying and consulting with the en-
17 tity designated by the Secretary under section
18 3553(b)(6); and

19 “(D) notifying and consulting with—

20 “(i) law enforcement agencies and rel-
21 evant Offices of Inspectors General;

22 “(ii) relevant committees of Congress,
23 as appropriate; and

1 “(iii) any other entity, in accordance
2 with law and as directed by the President;
3 and

4 “(8) plans and procedures to ensure continuity
5 of operations for information systems that support
6 the operations and assets of the agency.

7 “(c) ANNUAL AGENCY REPORTING.—The head of
8 each agency shall—

9 “(1) report annually to the Committee on Gov-
10 ernment Reform and the Committee on Science,
11 Space, and Technology of the House of Representa-
12 tives, the Committee on Homeland Security and
13 Governmental Affairs and the Committee on Com-
14 merce, Science, and Transportation of the Senate,
15 any other appropriate committees of Congress, and
16 the Secretary on the adequacy and effectiveness of
17 information security policies, procedures, and prac-
18 tices, including—

19 “(A) a description of each major informa-
20 tion security incident, or set of related inci-
21 dents, resulting in significant compromise of in-
22 formation security, including a summary of—

23 “(i) the threats, vulnerabilities, and
24 impact of the incident;

1 “(ii) the system risk assessment con-
2 ducted before the incident and required
3 under section 3554(a)(2); and

4 “(iii) the detection and response ac-
5 tions taken;

6 “(B) the number of information security
7 incidents within the agency resulting in signifi-
8 cant compromise of information security, pre-
9 sented by system impact level, type of incident,
10 and location;

11 “(C) the total number of information secu-
12 rity incidents within the agency, presented by
13 system impact level, type of incident, and loca-
14 tion;

15 “(D) an identification and analysis of, in-
16 cluding actions and plans to address, any sig-
17 nificant deficiencies identified in such policies,
18 procedures and practices;

19 “(E) any information or evaluation re-
20 quired under the reporting requirements issued
21 under section 3553(b); and

22 “(2) address the adequacy and effectiveness of
23 the information security policies, procedures, and
24 practices of the agency as required for management
25 and budget plans and reports, as appropriate.

1 “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—
 2 Notwithstanding any other provision of law, the head of
 3 each agency is authorized to allow the Secretary, or a pri-
 4 vate entity providing assistance to the Secretary under
 5 section 3553, to acquire, intercept, retain, use, and dis-
 6 close communications, system traffic, records, or other in-
 7 formation transiting to or from or stored on an agency
 8 information system for the purpose of protecting agency
 9 information and information systems from information se-
 10 curity threats or mitigating the threats in connection with
 11 the implementation of the information security capabilities
 12 authorized by paragraph (3) or (4) of section 3553(b).

13 **“§ 3555. Annual assessments**

14 “(a) IN GENERAL.—Except as provided in subsection
 15 (c), the Secretary shall conduct periodic assessments of
 16 the information security programs and practices of agen-
 17 cies based on the annual agency reports required under
 18 section 3554(c), the annual independent evaluations re-
 19 quired under section 3556, the results of any continuous
 20 monitoring, and other available information.

21 “(b) CONTENTS.—Each assessment conducted under
 22 subsection (a) shall—

23 “(1) assess the effectiveness of agency informa-
 24 tion security policies, procedures, and practices;

1 “(2) provide an assessment of the status of
2 agency information system security for the Federal
3 Government as a whole; and

4 “(3) include recommendations for improving in-
5 formation system security for an agency or the Fed-
6 eral Government as a whole.

7 “(c) CERTAIN INFORMATION SYSTEMS.—

8 “(1) NATIONAL SECURITY SYSTEMS.—A peri-
9 odic assessment conducted under subsection (a) re-
10 lating to a national security system shall be pre-
11 pared as directed by the President.

12 “(2) SPECIFIC AGENCIES.—Periodic assess-
13 ments conducted under subsection (a) shall be pre-
14 pared in accordance with governmentwide reporting
15 requirements by—

16 “(A) the Secretary of Defense for informa-
17 tion systems under the control of the Depart-
18 ment of Defense;

19 “(B) the Director of the Central Intel-
20 ligence Agency for information systems under
21 the control of the Central Intelligence Agency;
22 and

23 “(C) the Director of National Intelligence
24 for information systems under the control of

1 the Office of the Director of National Intel-
2 ligence.

3 “(d) AGENCY-SPECIFIC ASSESSMENTS.—Each as-
4 sessment conducted under subsection (a) that relates, in
5 whole or in part, to the information systems of an agency
6 shall be made available to the head of the agency.

7 “(e) PROTECTION OF INFORMATION.—In conducting
8 assessments under subsection (a), the Secretary shall take
9 appropriate actions to ensure the protection of information
10 which, if disclosed, may adversely affect information secu-
11 rity. Such protections shall be commensurate with the risk
12 and comply with all applicable laws and policies.

13 “(f) REPORT TO CONGRESS.—The Secretary, in co-
14 ordination with the Secretary of Defense, the Director of
15 the Central Intelligence Agency, and the Director of Na-
16 tional Intelligence, shall evaluate and submit to Congress
17 an annual report on the adequacy and effectiveness of the
18 information security programs and practices assessed
19 under this section.

20 **“§ 3556. Independent evaluations**

21 “(a) IN GENERAL.—Not less than annually, an inde-
22 pendent evaluation of the information security program
23 and practices of each agency shall be performed to assess
24 the effectiveness of the programs and practices.

1 “(b) CONTENTS.—Each evaluation performed under
2 subsection (a) shall include—

3 “(1) testing of the effectiveness of information
4 security policies, procedures, and practices of a rep-
5 resentative subset of the information systems of the
6 agency; and

7 “(2) an assessment of the effectiveness of the
8 information security policies, procedures, and prac-
9 tices of the agency.

10 “(c) CONDUCT OF INDEPENDENT EVALUATIONS.—
11 Except as provided in subsection (f), an evaluation of an
12 agency under subsection (a) shall be performed by—

13 “(1) the Inspector General of the agency;

14 “(2) at the discretion of the Inspector General
15 of the agency, an independent entity entering a con-
16 tract with the Inspector General to perform the eval-
17 uation; or

18 “(3) if the agency does not have an Inspector
19 General, an independent entity selected by the head
20 of the agency, in consultation with the Secretary.

21 “(d) PREVIOUSLY CONDUCTED EVALUATIONS.—The
22 evaluation required by this section may be based in whole
23 or in part on a previously conducted audit, evaluation, or
24 report relating to programs or practices of the applicable
25 agency.

1 “(e) REPORTS.—The official or entity performing an
 2 evaluation of an agency under subsection (a) shall submit
 3 to Congress, the agency, and the Comptroller General of
 4 the United States a report regarding the evaluation. The
 5 head of the agency shall provide to the Secretary a report
 6 received under this subsection.

7 “(f) NATIONAL SECURITY SYSTEMS.—An evaluation
 8 under subsection (a) of a national security system shall
 9 be performed as directed by the President.

10 “(g) COMPTROLLER GENERAL.—The Comptroller
 11 General of the United States shall periodically evaluate
 12 and submit to Congress reports on—

13 “(1) the adequacy and effectiveness of the in-
 14 formation security policies and practices of agencies;
 15 and

16 “(2) implementation of this subchapter.

17 **“§ 3557. National security systems**

18 “The head of each agency operating or exercising
 19 control of a national security system shall be responsible
 20 for ensuring that the agency—

21 “(1) provides information security protections
 22 commensurate with the risk and magnitude of the
 23 harm resulting from the unauthorized use, disclo-
 24 sure, disruption, modification, or destruction of the

1 information contained in the national security sys-
 2 tem;

3 “(2) implements information security policies
 4 and practices as required by standards and guide-
 5 lines for national security systems issued in accord-
 6 ance with law and as directed by the President; and

7 “(3) complies with this subchapter.

8 **“§ 3558. Effect on existing law**

9 “Nothing in this subchapter shall be construed to
 10 alter or amend any law regarding the authority of any
 11 head of an agency over the agency.”.

12 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 13 The table of sections for chapter 35 of title 44 is amended
 14 by striking the matter relating to subchapters II and III
 15 and inserting the following:

“SUBCHAPTER II—INFORMATION SECURITY

“Sec. 3551. Purposes.

“Sec. 3552. Definitions.

“Sec. 3553. Federal information security authority and coordination.

“Sec. 3554. Agency responsibilities.

“Sec. 3555. Annual assessments.

“Sec. 3556. Independent evaluations.

“Sec. 3557. National security systems.

“Sec. 3558. Effect on existing law.”.

16 **SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.**

17 (a) IN GENERAL.—Section 11331 of title 40, United
 18 States Code, is amended to read as follows:

19 **“§ 11331. Responsibilities for Federal information sys-**
 20 **tems standards**

21 “(a) DEFINITIONS.—In this section:

1 “(1) FEDERAL INFORMATION SYSTEM.—The
2 term ‘Federal information system’ means an infor-
3 mation system used or operated by an executive
4 agency, by a contractor of an executive agency, or by
5 another entity on behalf of an executive agency.

6 “(2) INFORMATION SECURITY.—The term ‘in-
7 formation security’ has the meaning given that term
8 in section 3552 of title 44.

9 “(3) NATIONAL SECURITY SYSTEM.—The term
10 ‘national security system’ has the meaning given
11 that term in section 3552 of title 44.

12 “(b) STANDARDS AND GUIDELINES.—

13 “(1) AUTHORITY TO PRESCRIBE.—Except as
14 provided under paragraph (2), and based on the
15 standards and guidelines developed by the National
16 Institute of Standards and Technology under para-
17 graphs (2) and (3) of section 20(a) of the National
18 Institute of Standards and Technology Act (15
19 U.S.C. 278g–3(a)), the Secretary of Commerce, in
20 consultation with the Secretary of Homeland Secu-
21 rity, shall prescribe standards and guidelines relat-
22 ing to Federal information systems.

23 “(2) NATIONAL SECURITY SYSTEMS.—Stand-
24 ards and guidelines for national security systems
25 shall be developed, prescribed, enforced, and over-

1 seen as otherwise authorized by law and as directed
2 by the President.

3 “(c) MANDATORY REQUIREMENTS.—

4 “(1) AUTHORITY TO MAKE MANDATORY.—The
5 Secretary of Commerce may require executive agen-
6 cies to comply with the standards prescribed under
7 subsection (b)(1) to the extent determined necessary
8 by the Secretary of Commerce to improve the effi-
9 ciency of operation or security of Federal informa-
10 tion systems.

11 “(2) REQUIRED MANDATORY STANDARDS.—

12 “(A) IN GENERAL.—The Secretary of
13 Commerce shall require executive agencies to
14 comply with the standards described in sub-
15 paragraph (B).

16 “(B) CONTENTS.—The standards de-
17 scribed in this subparagraph are information
18 security standards that—

19 “(i) provide minimum information se-
20 curity requirements as determined under
21 section 20(b) of the National Institute of
22 Standards and Technology Act (15 U.S.C.
23 278g–3(b)); and

1 “(ii) are otherwise necessary to im-
2 prove the security of Federal information
3 and Federal information systems.

4 “(d) **AUTHORITY TO DISAPPROVE OR MODIFY.**—The
5 President may disapprove or modify the standards and
6 guidelines prescribed under subsection (b)(1) if the Presi-
7 dent determines such action to be in the public interest.
8 The authority of the President to disapprove or modify
9 the standards and guidelines may be delegated to the Di-
10 rector of the Office of Management and Budget. Notice
11 of a disapproval or modification under this subsection
12 shall be published promptly in the Federal Register. Upon
13 receiving notice of a disapproval or modification, the Sec-
14 retary of Commerce shall immediately rescind or modify
15 the standards or guidelines as directed by the President
16 or the Director of the Office of Management and Budget.

17 “(e) **EXERCISE OF AUTHORITY.**—To ensure fiscal
18 and policy consistency, the Secretary of Commerce shall
19 exercise the authority under this section subject to direc-
20 tion by the President and in coordination with the Direc-
21 tor of the Office of Management and Budget.

22 “(f) **APPLICATION OF MORE STRINGENT STAND-**
23 **ARDS.**—The head of an executive agency may employ
24 standards for the cost-effective information security for
25 Federal information systems of that agency that are more

1 stringent than the standards prescribed by the Secretary
 2 of Commerce under subsection (b)(1) if the more stringent
 3 standards—

4 “(1) contain any standards with which the Sec-
 5 retary of Commerce has required the agency to com-
 6 ply; and

7 “(2) are otherwise consistent with the policies
 8 and directives issued under section 3553(b) of title
 9 44.

10 “(g) DECISIONS ON PROMULGATION OF STAND-
 11 ARDS.—The decision by the Secretary of Commerce re-
 12 garding the promulgation of any standard under this sec-
 13 tion shall occur not later than 6 months after the submis-
 14 sion of the proposed standard to the Secretary of Com-
 15 merce by the National Institute of Standards and Tech-
 16 nology, as provided under section 20 of the National Insti-
 17 tute of Standards and Technology Act (15 U.S.C. 278g–
 18 3).”.

19 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

20 (1) Section 3502(8)) of title 44, United States
 21 Code, is amended by inserting “hosting,” after “col-
 22 lection,”.

23 (2) The National Institute of Standards and
 24 Technology Act (15 U.S.C. 271 et seq.) is amend-
 25 ed—

1 (A) in section 20(a)(2) (15 U.S.C. 278g–
 2 3(a)(2)), by striking “section 3532(b)(2)” and
 3 inserting “section 3552(b)”; and

4 (B) in section 21(b) (15 U.S.C. 278g–
 5 4(b))—

6 (i) in paragraph (2), by inserting “,
 7 the Secretary of Homeland Security,” after
 8 “the Institute”; and

9 (ii) in paragraph (3), by inserting
 10 “the Secretary of Homeland Security,”
 11 after “the Secretary of Commerce,”.

12 (3) Section 1001(c)(1)(A) of the Homeland Se-
 13 curity Act of 2002 (6 U.S.C. 511(c)(1)(A)) is
 14 amended by striking “section 3532(3)” and insert-
 15 ing “section 3552(b)”.

16 (4) Part IV of title 10, United States Code, is
 17 amended—

18 (A) in section 2222(j)(5), by striking “sec-
 19 tion 3542(b)(2)” and inserting “section
 20 3552(b)”;

21 (B) in section 2223(c)(3), by striking “sec-
 22 tion 3542(b)(2)” and inserting “section
 23 3552(b)”; and

24 (C) in section 2315, by striking “section
 25 3542(b)(2)” and inserting “section 3552(b)”.

1 (5) Section 8(d)(1) of the Cyber Security Re-
2 search and Development Act (15 U.S.C. 7406(d)(1))
3 is amended by striking “section 3534(b)” and in-
4 serting “section 3554(b)”.

5 **SEC. 203. SAVINGS PROVISIONS.**

6 (a) IN GENERAL.—Policies and compliance guidance
7 issued by the Director of the Office of Management and
8 Budget before the date of enactment of this Act under
9 section 3543(a)(1) of title 44 (as in effect on the day be-
10 fore the date of enactment of this Act) shall continue in
11 effect, according to their terms, until modified, termi-
12 nated, superseded, or repealed under section 3553(b)(1)
13 of title 44, as added by this Act.

14 (b) OTHER STANDARDS AND GUIDELINES.—Stand-
15 ards and guidelines issued by the Secretary of Commerce
16 or by the Director of the Office of Management and Budg-
17 et before the date of enactment of this Act under section
18 11331(b)(1) of title 40 (as in effect on the day before the
19 date of enactment of this Act) shall continue in effect, ac-
20 cording to their terms, until modified, terminated, super-
21 seded, or repealed under section 11331(b)(1), as added by
22 this Act.

1 **SEC. 204. CONSOLIDATION OF EXISTING DEPARTMENTAL**
 2 **CYBER RESOURCES AND AUTHORITIES.**

3 (a) IN GENERAL.—Title II of the Homeland Security
 4 Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding
 5 at the end the following:

6 **“Subtitle E—Cybersecurity**

7 **“SEC. 241. DEFINITIONS.**

8 “In this subtitle:

9 “(1) AGENCY INFORMATION INFRASTRUC-
 10 TURE.—The term ‘agency information infrastruc-
 11 ture’ means the Federal information infrastructure
 12 of a particular Federal agency.

13 “(2) CENTER.—The term ‘Center’ means the
 14 National Center for Cybersecurity and Communica-
 15 tions established under section 242.

16 “(3) DAMAGE.—The term ‘damage’ has the
 17 meaning given that term in section 1030(e) of title
 18 18, United States Code.

19 “(4) FEDERAL AGENCY.—The term ‘Federal
 20 agency’ has the meaning given the term ‘agency’ in
 21 section 3502 of title 44, United States Code.

22 “(5) FEDERAL CYBERSECURITY CENTER.—The
 23 term ‘Federal cybersecurity center’ has the meaning
 24 given that term in section 708 of the Cybersecurity
 25 Act of 2012.

1 “(6) FEDERAL ENTITY.—The term ‘Federal en-
2 tity’ has the meaning given that term in section 708
3 of the Cybersecurity Act of 2012.

4 “(7) FEDERAL INFORMATION INFRASTRUC-
5 TURE.—The term ‘Federal information infrastruc-
6 ture’—

7 “(A) means information and information
8 systems that are owned, operated, controlled, or
9 licensed solely for use by, or on behalf of, any
10 Federal agency, including information systems
11 used or operated by another entity on behalf of
12 a Federal agency; and

13 “(B) does not include—

14 “(i) a national security system; or

15 “(ii) information and information sys-
16 tems that are owned, operated, controlled,
17 or licensed for use solely by, or on behalf
18 of, the Department of Defense, a military
19 department, or another element of the in-
20 telligence community.

21 “(8) INCIDENT.—The term ‘incident’ has the
22 meaning given that term in section 3552 of title 44,
23 United States Code.

1 “(9) INFORMATION SECURITY.—The term ‘in-
2 formation security’ has the meaning given that term
3 in section 3552 of title 44, United States Code.

4 “(10) INFORMATION SYSTEM.—The term ‘infor-
5 mation system’ has the meaning given that term in
6 section 3502 of title 44, United States Code.

7 “(11) INTELLIGENCE COMMUNITY.—The term
8 ‘intelligence community’ has the meaning given that
9 term in section 3(4) of the National Security Act of
10 1947 (50 U.S.C. 401a(4)).

11 “(12) NATIONAL SECURITY AND EMERGENCY
12 PREPAREDNESS COMMUNICATIONS INFRASTRUC-
13 TURE.—The term ‘national security and emergency
14 preparedness communications infrastructure’ means
15 the systems supported or covered by the Office of
16 Emergency Communications and the National Com-
17 munications System on the date of enactment of the
18 Cybersecurity Act of 2012 or otherwise described in
19 Executive Order 12472, or any successor thereto, re-
20 lating to national security and emergency prepared-
21 ness communications functions.

22 “(13) NATIONAL INFORMATION INFRASTRUC-
23 TURE.—The term ‘national information infrastruc-
24 ture’ means information and information systems—

1 “(A) that are owned, operated, or con-
 2 trolled, in whole or in part, within or from the
 3 United States; and

4 “(B) that are not owned, operated, con-
 5 trolled, or licensed for use by a Federal agency.

6 “(14) NATIONAL SECURITY SYSTEM.—The term
 7 ‘national security system’ has the meaning given
 8 that term in section 3552 of title 44, United States
 9 Code.

10 “(15) NON-FEDERAL ENTITY.—The term ‘non-
 11 Federal entity’ has the meaning given that term in
 12 section 708 of the Cybersecurity Act of 2012.

13 **“SEC. 242. CONSOLIDATION OF EXISTING RESOURCES.**

14 “(a) ESTABLISHMENT.—There is established within
 15 the Department a National Center for Cybersecurity and
 16 Communications.

17 “(b) TRANSFER OF FUNCTIONS.—There are trans-
 18 ferred to the Center the National Cyber Security Division,
 19 the Office of Emergency Communications, and the Na-
 20 tional Communications System, including all the func-
 21 tions, personnel, assets, authorities, and liabilities of the
 22 National Cyber Security Division, the Office of Emergency
 23 Communications, and the National Communications Sys-
 24 tem.

1 “(c) DIRECTOR.—The Center shall be headed by a
2 Director, who shall be appointed by the President, by and
3 with the advice and consent of the Senate, and who shall
4 report directly to the Secretary.

5 “(d) DUTIES.—The Director of the Center shall—

6 “(1) manage Federal efforts to secure, protect,
7 and ensure the resiliency of the Federal information
8 infrastructure, national information infrastructure,
9 and national security and emergency preparedness
10 communications infrastructure of the United States,
11 working cooperatively with appropriate government
12 agencies and the private sector;

13 “(2) support private sector efforts to secure,
14 protect, and ensure the resiliency of the national in-
15 formation infrastructure;

16 “(3) prioritize the efforts of the Center to ad-
17 dress the most significant risks and incidents that
18 have caused or are likely to cause damage to the
19 Federal information infrastructure, the national in-
20 formation infrastructure, and national security and
21 emergency preparedness communications infrastruc-
22 ture of the United States;

23 “(4) ensure, in coordination with the privacy of-
24 ficer designated under subsection (j), the privacy of-
25 ficer appointed under section 222, and the Director

1 of the Office of Civil Rights and Civil Liberties ap-
2 pointed under section 705, that the activities of the
3 Center comply with all policies, regulations, and laws
4 protecting the privacy and civil liberties of United
5 States persons; and

6 “(5) perform such other duties as the Secretary
7 may require relating to the security and resiliency of
8 the Federal information infrastructure, national in-
9 formation infrastructure, and the national security
10 and emergency preparedness communications infra-
11 structure of the United States.

12 “(e) AUTHORITIES AND RESPONSIBILITIES OF CEN-
13 TER.—The Center shall—

14 “(1) engage in activities and otherwise coordi-
15 nate Federal efforts to identify, protect against, re-
16 mediate, and mitigate, respond to, and recover from
17 cybersecurity threats, consequences, vulnerabilities
18 and incidents impacting the Federal information in-
19 frastructure and the national information infrastruc-
20 ture, including by providing support to entities that
21 own or operate national information infrastructure,
22 at their request;

23 “(2) conduct risk-based assessments of the Fed-
24 eral information infrastructure, and risk assessments
25 of critical infrastructure;

1 “(3) develop, oversee the implementation of,
2 and enforce policies, principles, and guidelines on in-
3 formation security for the Federal information infra-
4 structure, including exercise of the authorities under
5 the Federal Information Security Management Act
6 of 2002 (title III of Public Law 107–347; 116 Stat.
7 2946);

8 “(4) evaluate and facilitate the adoption of
9 technologies designed to enhance the protection of
10 information infrastructure, including making such
11 technologies available to entities that own or operate
12 national information infrastructure, with or without
13 reimbursement, as necessary to accomplish the pur-
14 poses of this section;

15 “(5) oversee the responsibilities related to na-
16 tional security and emergency preparedness commu-
17 nications infrastructure, including the functions of
18 the Office of Emergency Communications and the
19 National Communications System;

20 “(6)(A) maintain comprehensive situational
21 awareness of the security of the Federal information
22 infrastructure and the national information infra-
23 structure for the purpose of enabling and supporting
24 activities under subparagraph (e)(1); and

1 “(B) receive and distribute classified and un-
2 classified information from and to entities that own
3 or operate national information infrastructure to
4 support efforts by such entities to secure such infra-
5 structure and for enhancing overall situational
6 awareness;

7 “(7) serve as the focal point for, and foster col-
8 laboration between, the Federal Government, State
9 and local governments, and private entities on mat-
10 ters relating to the security of the national informa-
11 tion infrastructure;

12 “(8) develop, in coordination with the Assistant
13 Secretary for Infrastructure Protection, other Fed-
14 eral agencies, the private sector, and State and local
15 governments a national incident response plan that
16 details the roles of Federal agencies, State and local
17 governments, and the private sector, and coordinate
18 national cyber incident response efforts;

19 “(9) consult, in coordination with the Secretary
20 of State, with appropriate international partners to
21 enhance the security of the Federal information in-
22 frastructure, national information infrastructure,
23 and information infrastructure located outside the
24 United States the disruption of which could result in

1 national or regional catastrophic damage in the
2 United States;

3 “(10) coordinate the activities undertaken by
4 Federal agencies to—

5 “(A) protect Federal information infra-
6 structure and national information infrastruc-
7 ture; and

8 “(B) prepare the Nation to respond to, re-
9 cover from, and mitigate against risks of inci-
10 dents involving such infrastructure; and

11 “(11) perform such other duties as the Sec-
12 retary may require relating to the security and resil-
13 iency of the Federal information infrastructure, na-
14 tional information infrastructure, and national secu-
15 rity and emergency preparedness communications in-
16 frastructure of the United States.

17 “(f) USE OF EXISTING MECHANISMS FOR COLLABO-
18 RATION.—To avoid unnecessary duplication or waste, in
19 carrying out the authorities and responsibilities of the
20 Center under this subtitle, to the maximum extent prac-
21 ticable, the Director of the Center shall make use of exist-
22 ing mechanisms for collaboration and information sharing,
23 including mechanisms relating to the identification and
24 communication of cybersecurity threats, vulnerabilities,
25 and associated consequences, established by other compo-

1 nents of the Department or other Federal agencies and
2 the information sharing mechanisms established under
3 title VII of the Cybersecurity Act of 2012.

4 “(g) DEPUTY DIRECTORS.—

5 “(1) IN GENERAL.—There shall be a Deputy
6 Director appointed by the Secretary, who shall—

7 “(A) have expertise in infrastructure pro-
8 tection; and

9 “(B) ensure that the operations of the
10 Center and the Office of Infrastructure Protec-
11 tion avoid duplication and use, to the maximum
12 extent practicable, joint mechanisms for infor-
13 mation sharing and coordination with the pri-
14 vate sector.

15 “(2) INTELLIGENCE COMMUNITY.—The Direc-
16 tor of National Intelligence, with the concurrence of
17 the Secretary, shall identify an employee of an ele-
18 ment of the intelligence community to serve as a
19 Deputy Director of the Center. The employee shall
20 be detailed to the Center on a reimbursable basis for
21 such period as is agreed to by the Director of the
22 Center and the Director of National Intelligence,
23 and, while serving as Deputy Director, shall report
24 directly to the Director of the Center.

1 “(h) CYBERSECURITY EXERCISE PROGRAM.—The
 2 Director of the Center shall develop and implement a na-
 3 tional cybersecurity exercise program with the participa-
 4 tion of State and local governments, international partners
 5 of the United States, and the private sector.

6 “(i) LIAISON OFFICERS.—

7 “(1) REQUIRED DETAIL OF LIAISON OFFI-
 8 CERS.—The Secretary of Defense, the Attorney Gen-
 9 eral, the Secretary of Commerce, and the Director of
 10 National Intelligence shall assign personnel to the
 11 Center to act as full-time liaisons.

12 “(2) OPTIONAL DETAIL OF LIAISON OFFI-
 13 CERS.—The head of any Federal agency not de-
 14 scribed in paragraph (1), with the concurrence of
 15 the Director of the Center, may assign personnel to
 16 the Center to act as liaisons.

17 “(3) PRIVATE SECTOR LIAISON.—The Director
 18 of the Center shall designate not less than 1 em-
 19 ployee of the Center to serve as a liaison with the
 20 private sector.

21 “(j) PRIVACY OFFICER.—The Director of the Center,
 22 in consultation with the Secretary, shall designate a full-
 23 time privacy officer.

24 “(k) SUFFICIENCY OF RESOURCES PLAN.—

1 “(1) REPORT.—Not later than 120 days after
2 the date of enactment of the Cybersecurity Act of
3 2012, the Director of the Office of Management and
4 Budget shall submit to the appropriate committees
5 of Congress and the Comptroller General of the
6 United States a report on the resources and staff
7 necessary to carry out fully the responsibilities under
8 this subtitle, including the availability of existing re-
9 sources and staff.

10 “(2) COMPTROLLER GENERAL REVIEW.—The
11 Comptroller General of the United States shall
12 evaluate the reasonableness and adequacy of the re-
13 port submitted by the Director of the Office of Man-
14 agement and Budget under paragraph (1) and sub-
15 mit to the appropriate committees of Congress a re-
16 port regarding the same.

17 “(1) NO RIGHT OR BENEFIT.—The provision of as-
18 sistance or information under this section to governmental
19 or private entities that own or operate critical infrastruc-
20 ture shall be at the discretion of the Secretary. The provi-
21 sion of certain assistance or information to a governmental
22 or private entity pursuant to this section shall not create
23 a right or benefit, substantive or procedural, to similar
24 assistance or information for any other governmental or
25 private entity.

1 **“SEC. 243. DEPARTMENT OF HOMELAND SECURITY INFOR-**
2 **MATION SHARING.**

3 “(a) INFORMATION SHARING.—The Director of the
4 Center shall establish procedures to—

5 “(1) ensure the appropriate, regular, and timely
6 sharing of classified and unclassified cybersecurity
7 information, including information relating to
8 threats, vulnerabilities, traffic, trends, incidents, and
9 other anomalous activities that affect the Federal in-
10 formation infrastructure, national information infra-
11 structure, or information systems between and
12 among appropriate Federal and non-Federal entities,
13 including Federal cybersecurity centers, Federal and
14 non-Federal network and security operations cen-
15 ters, cybersecurity exchanges, and non-Federal enti-
16 ties responsible for such information systems;

17 “(2) expand and enhance the sharing of timely
18 and actionable cybersecurity threat and vulnerability
19 information by the Federal Government with owners
20 and operators of the national information infrastruc-
21 ture;

22 “(3) establish a method of accessing classified
23 or unclassified information, as appropriate and in
24 accordance with applicable laws protecting trade se-
25 crets, that will provide situational awareness of the
26 security of the Federal information infrastructure

1 and the national information infrastructure relating
2 to cybersecurity threats, and vulnerabilities, includ-
3 ing traffic, trends, incidents, damage, and other
4 anomalous activities affecting the Federal informa-
5 tion infrastructure or the national information infra-
6 structure;

7 “(4) develop, in consultation with the Attorney
8 General, the Director of National Intelligence, and
9 the privacy officer established under section 242(j),
10 guidelines to protect the privacy and civil liberties of
11 United States persons and intelligence sources and
12 methods, while carrying out this subsection; and

13 “(5) ensure, to the extent necessary, that any
14 information sharing under this section is consistent
15 with title VII of the Cybersecurity Act of 2012.

16 “(b) VOLUNTARILY SHARED INFORMATION.—

17 “(1) IN GENERAL.—The Director of the Center
18 shall ensure that information submitted in accord-
19 ance with this section by States and units of local
20 governments, private entities, and international part-
21 ners of the United States regarding threats,
22 vulnerabilities, incidents, and anomalous activities
23 affecting the national information infrastructure,
24 Federal information infrastructure, or information
25 infrastructure that is owned, operated, controlled, or

1 licensed solely for use by, or on behalf of, the De-
 2 partment of Defense, a military department, or an-
 3 other element of the intelligence community is treat-
 4 ed as voluntarily shared critical infrastructure infor-
 5 mation under section 214 as requested by submit-
 6 ting entities.

7 “(2) LIMITATION.—Paragraph (1) shall not
 8 apply to information that is submitted to—

9 “(A) conceal violations of law, inefficiency,
 10 or administrative error;

11 “(B) prevent embarrassment to a person,
 12 organization, or agency; or

13 “(C) interfere with competition in the pri-
 14 vate sector.

15 “(c) LIMITATION ON USE OF VOLUNTARILY SUB-
 16 MITTED INFORMATION FOR REGULATORY ENFORCEMENT
 17 ACTIONS.—A Federal entity may not use information sub-
 18 mitted under this subtitle as evidence in a regulatory en-
 19 forcement action against the individual or entity that law-
 20 fully submitted the information.

21 “(d) FEDERAL AGENCIES.—

22 “(1) INFORMATION SHARING PROGRAM.—The
 23 Director of the Center, in consultation with the
 24 members of the Chief Information Officers Council
 25 established under section 3603 of title 44, United

1 States Code, shall establish a program for sharing
2 information with and between the Center and other
3 Federal agencies that includes processes and proce-
4 dures—

5 “(A) under which the Director of the Cen-
6 ter regularly shares with each Federal agency
7 analyses and reports regarding the security of
8 such agency information infrastructure and on
9 the overall security of the Federal information
10 infrastructure and information infrastructure
11 that is owned, operated, controlled, or licensed
12 for use by, or on behalf of, the Department of
13 Defense, a military department, or another ele-
14 ment of the intelligence community, which shall
15 include means and methods of preventing, re-
16 sponding to, mitigating, and remediating cyber-
17 security threats and vulnerabilities; and

18 “(B) under which Federal agencies provide
19 the Director of the Center, upon request, with
20 information concerning the security of the Fed-
21 eral information infrastructure, information in-
22 frastructure that is owned, operated, controlled,
23 or licensed for use by, or on behalf of, the De-
24 partment of Defense, a military department, or
25 another element of the intelligence community,

1 or the national information infrastructure nec-
2 essary to carry out the duties of the Director of
3 the Center under this subtitle or any other pro-
4 vision of law.

5 “(2) ACCESS TO INFORMATION.—

6 “(A) IN GENERAL.—The Director of the
7 Center shall ensure—

8 “(i) that the head of each Federal
9 agency has timely access to data, including
10 appropriate raw and processed data, re-
11 garding the information infrastructure of
12 the Federal agency; and

13 “(ii) to the greatest extent possible,
14 that the head of each Federal agency is
15 kept apprised of common trends in security
16 compliance as well as the likelihood that a
17 significant cybersecurity risk or incident
18 could cause damage to the agency informa-
19 tion infrastructure.

20 “(B) COMPLIANCE.—The head of a Fed-
21 eral agency shall comply with all processes and
22 procedures established under this subsection re-
23 garding notification to the Director of the Cen-
24 ter relating to incidents.

1 “(C) IMMEDIATE NOTIFICATION RE-
2 QUIRED.—Unless otherwise directed by the
3 President, any Federal agency with a national
4 security system shall, consistent with the level
5 of the risk, immediately notify the Director of
6 the Center regarding any incident affecting the
7 security of a national security system.

8 **“SEC. 244. PROHIBITED CONDUCT.**

9 “None of the authorities provided under this subtitle
10 shall authorize the Director of the Center, the Center, the
11 Department, or any other Federal entity to—

12 “(1) compel the disclosure of information from
13 a private entity relating to an incident unless other-
14 wise authorized by law; or

15 “(2) intercept a wire, oral, or electronic commu-
16 nication (as those terms are defined in section 2510
17 of title 18, United States Code), access a stored
18 electronic or wire communication, install or use a
19 pen register or trap and trace device, or conduct
20 electronic surveillance (as defined in section 101 of
21 the Foreign Intelligence Surveillance Act of 1978
22 (50 U.S.C.1801)) relating to an incident unless oth-
23 erwise authorized under chapter 119, chapter 121,
24 or chapter 206 of title 18, United States Code, or

1 the Foreign Intelligence Surveillance Act of 1978
 2 (50 U.S.C. 1801 et seq.).”.

3 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 4 The table of contents in section 1(b) of the Homeland Se-
 5 curity Act of 2002 (6 U.S.C. 101 et seq.) is amended by
 6 inserting after the item relating to section 237 the fol-
 7 lowing:

“Subtitle E—Cybersecurity

“Sec. 241. Definitions.

“Sec. 242. Consolidation of existing resources.

“Sec. 243. Department of Homeland Security information sharing.

“Sec. 244. Prohibited conduct.”.

8 **TITLE III—RESEARCH AND** 9 **DEVELOPMENT**

10 **SEC. 301. FEDERAL CYBERSECURITY RESEARCH AND DE-** 11 **VELOPMENT.**

12 (a) FUNDAMENTAL CYBERSECURITY RESEARCH.—
 13 The Director of the Office of Science and Technology Pol-
 14 icy (referred to in this section as the “Director”), in co-
 15 ordination with the Secretary and the head of any relevant
 16 Federal agency, shall build upon programs and plans in
 17 effect as of the date of enactment of this Act to develop
 18 a national cybersecurity research and development plan,
 19 which shall be updated biennially.

20 (b) REQUIREMENTS.—The plan required to be devel-
 21 oped under subsection (a) shall encourage computer and

1 information science and engineering research to meet chal-
2 lenges in cybersecurity, including—

3 (1) how to design and build complex software-
4 intensive systems that are secure and reliable when
5 first deployed;

6 (2) how to test and verify that software, wheth-
7 er developed locally or obtained from a third party,
8 is free of significant known security flaws;

9 (3) how to test and verify that software ob-
10 tained from a third party correctly implements stat-
11 ed functionality, and only that functionality;

12 (4) how to guarantee the privacy of the iden-
13 tity, information, or lawful transactions of an indi-
14 vidual when stored in distributed systems or trans-
15 mitted over networks;

16 (5) how to build new protocols to enable the
17 Internet to have robust security as one of the key
18 capabilities of the Internet;

19 (6) how to determine the origin of a message
20 transmitted over the Internet;

21 (7) how to support privacy in conjunction with
22 improved security;

23 (8) how to address the growing problem of in-
24 sider threat;

1 (9) how improved consumer education and dig-
2 ital literacy initiatives can address human factors
3 that contribute to cybersecurity;

4 (10) how to protect information stored through
5 cloud computing or transmitted through wireless
6 services;

7 (11) conducting research in the areas described
8 in section 4(a)(1) of the Cyber Security Research
9 and Development Act (15 U.S.C. 7403(a)(1)), as
10 amended by subsection (f); and

11 (12) any additional objectives the Director or
12 Secretary determines appropriate.

13 (c) CYBERSECURITY PRACTICES RESEARCH.—The
14 Director of the National Science Foundation shall support
15 research—

16 (1) that develops, evaluates, disseminates, and
17 integrates new cybersecurity practices and concepts
18 into the core curriculum of computer science pro-
19 grams and of other programs where graduates of
20 such programs have a substantial probability of de-
21 veloping software after graduation, including new
22 practices and concepts relating to secure coding edu-
23 cation and improvement programs; and

1 (2) that develops new models for professional
2 development of faculty in cybersecurity education,
3 including secure coding development.

4 (d) CYBERSECURITY MODELING AND TEST BEDS.—

5 (1) REVIEW.—Not later than 1 year after the
6 date of enactment of this Act, the Director shall
7 conduct a review of cybersecurity test beds in exist-
8 ence on the date of enactment of this Act to inform
9 the program established under paragraph (2).

10 (2) ESTABLISHMENT OF PROGRAM.—

11 (A) IN GENERAL.—The Director of the
12 National Science Foundation, the Secretary,
13 and the Secretary of Commerce shall establish
14 a program for the appropriate Federal agencies
15 to award grants to institutions of higher edu-
16 cation or research and development non-profit
17 institutions to establish cybersecurity test beds
18 capable of realistic modeling of real-time cyber
19 attacks and defenses.

20 (B) REQUIREMENT.—The test beds estab-
21 lished under subparagraph (A) shall be suffi-
22 ciently large in order to model the scale and
23 complexity of real world networks and environ-
24 ments.

1 (3) PURPOSE.—The purpose of the program es-
2 tablished under paragraph (2) shall be to support
3 the rapid development of new cybersecurity defenses,
4 techniques, and processes by improving under-
5 standing and assessing the latest technologies in a
6 real-world environment.

7 (e) COORDINATION WITH OTHER RESEARCH INITIA-
8 TIVES.—The Director shall to the extent practicable, co-
9 ordinate research and development activities under this
10 section with other ongoing research and development secu-
11 rity-related initiatives, including research being conducted
12 by—

13 (1) the National Institute of Standards and
14 Technology;

15 (2) the Department;

16 (3) other Federal agencies;

17 (4) other Federal and private research labora-
18 tories, research entities, and universities and institu-
19 tions of higher education, and relevant nonprofit or-
20 ganizations; and

21 (5) international partners of the United States.

22 (f) NSF COMPUTER AND NETWORK SECURITY RE-
23 SEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Se-
24 curity Research and Development Act (15 U.S.C.
25 7403(a)(1)) is amended—

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

3 (2) in subparagraph (I), by striking the period
4 at the end and inserting a semicolon; and

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

6 “(J) secure fundamental protocols that are
7 at the heart of inter-network communications
8 and data exchange;

9 “(K) secure software engineering and soft-
10 ware assurance, including—

11 “(i) programming languages and sys-
12 tems that include fundamental security
13 features;

14 “(ii) portable or reusable code that re-
15 mains secure when deployed in various en-
16 vironments;

17 “(iii) verification and validation tech-
18 nologies to ensure that requirements and
19 specifications have been implemented; and

20 “(iv) models for comparison and
21 metrics to assure that required standards
22 have been met;

23 “(L) holistic system security that—

1 “(i) addresses the building of secure
 2 systems from trusted and untrusted com-
 3 ponents;

4 “(ii) proactively reduces
 5 vulnerabilities;

6 “(iii) addresses insider threats; and

7 “(iv) supports privacy in conjunction
 8 with improved security;

9 “(M) monitoring and detection;

10 “(N) mitigation and rapid recovery meth-
 11 ods;

12 “(O) security of wireless networks and mo-
 13 bile devices; and

14 “(P) security of cloud infrastructure and
 15 services.”.

16 (g) CYBERSECURITY FACULTY DEVELOPMENT
 17 TRAINEESHIP PROGRAM.—Section 5(e)(9) of the Cyber
 18 Security Research and Development Act (15 U.S.C.
 19 7404(e)(9)) is amended by striking “2003 through 2007”
 20 and inserting “2012 through 2014”.

21 (h) NETWORKING AND INFORMATION TECHNOLOGY
 22 RESEARCH AND DEVELOPMENT PROGRAM.—Section
 23 204(a)(1) of the High-Performance Computing Act of
 24 1991 (15 U.S.C. 5524(a)(1)) is amended—

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

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

4 “(D) develop and propose standards and
 5 guidelines, and develop measurement techniques
 6 and test methods, for enhanced cybersecurity
 7 for computer networks and common user inter-
 8 faces to systems; and”.

9 **SEC. 302. HOMELAND SECURITY CYBERSECURITY RE-**
 10 **SEARCH AND DEVELOPMENT.**

11 (a) IN GENERAL.—Subtitle D of title II of the Home-
 12 land Security Act of 2002 (6 U.S.C. 161 et seq.) is amend-
 13 ed by adding at the end the following:

14 **“SEC. 238. CYBERSECURITY RESEARCH AND DEVELOP-**
 15 **MENT.**

16 “(a) ESTABLISHMENT OF RESEARCH AND DEVELOP-
 17 MENT PROGRAM.—The Under Secretary for Science and
 18 Technology, in coordination with the Director of the Na-
 19 tional Center for Cybersecurity and Communications, shall
 20 carry out a research and development program for the
 21 purpose of improving the security of information infra-
 22 structure.

23 “(b) ELIGIBLE PROJECTS.—The research and devel-
 24 opment program carried out under subsection (a) may in-
 25 clude projects to—

1 “(1) advance the development and accelerate
2 the deployment of more secure versions of funda-
3 mental Internet protocols and architectures, includ-
4 ing for the secure domain name addressing system
5 and routing security;

6 “(2) improve and create technologies for detect-
7 ing and analyzing attacks or intrusions, including
8 analysis of malicious software;

9 “(3) improve and create mitigation and recov-
10 ery methodologies, including techniques for contain-
11 ment of attacks and development of resilient net-
12 works and systems;

13 “(4) develop and support infrastructure and
14 tools to support cybersecurity research and develop-
15 ment efforts, including modeling, test beds, and data
16 sets for assessment of new cybersecurity tech-
17 nologies;

18 “(5) assist the development and support of
19 technologies to reduce vulnerabilities in process con-
20 trol systems;

21 “(6) understand human behavioral factors that
22 can affect cybersecurity technology and practices;

23 “(7) test, evaluate, and facilitate, with appro-
24 priate protections for any proprietary information
25 concerning the technologies, the transfer of tech-

1 nologies associated with the engineering of less vul-
2 nerable software and securing the information tech-
3 nology software development lifecycle;

4 “(8) assist the development of identity manage-
5 ment and attribution technologies;

6 “(9) assist the development of technologies de-
7 signed to increase the security and resiliency of tele-
8 communications networks;

9 “(10) advance the protection of privacy and
10 civil liberties in cybersecurity technology and prac-
11 tices; and

12 “(11) address other risks identified by the Di-
13 rector of the National Center for Cybersecurity and
14 Communications.

15 “(c) COORDINATION WITH OTHER RESEARCH INI-
16 TIATIVES.—The Under Secretary for Science and Tech-
17 nology—

18 “(1) shall ensure that the research and develop-
19 ment program carried out under subsection (a) is
20 consistent with any strategy to increase the security
21 and resilience of cyberspace;

22 “(2) shall, to the extent practicable, coordinate
23 the research and development activities of the De-
24 partment with other ongoing research and develop-

1 ment security-related initiatives, including research
2 being conducted by—

3 “(A) the National Institute of Standards
4 and Technology;

5 “(B) the National Science Foundation;

6 “(C) the National Academy of Sciences;

7 “(D) other Federal agencies;

8 “(E) other Federal and private research
9 laboratories, research entities, and universities
10 and institutions of higher education, and rel-
11 evant nonprofit organizations; and

12 “(F) international partners of the United
13 States;

14 “(3) shall carry out any research and develop-
15 ment project under subsection (a) through a reim-
16 bursable agreement with an appropriate Federal
17 agency, if the Federal agency—

18 “(A) is sponsoring a research and develop-
19 ment project in a similar area; or

20 “(B) has a unique facility or capability
21 that would be useful in carrying out the project;

22 “(4) may make grants to, or enter into coopera-
23 tive agreements, contracts, other transactions, or re-
24 imbursable agreements with, the entities described in
25 paragraph (2); and

1 “(5) shall submit a report to the appropriate
 2 committees of Congress on a review of the cyberse-
 3 curity activities, and the capacity, of the national
 4 laboratories and other research entities available to
 5 the Department to determine if the establishment of
 6 a national laboratory dedicated to cybersecurity re-
 7 search and development is necessary.”.

8 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 9 The table of contents in section 1(b) of the Homeland Se-
 10 curity Act of 2002 (6 U.S.C. 101 et seq.), as amended
 11 by section 204, is amended by inserting after the item re-
 12 lating to section 237 the following:

 “Sec. 238. Cybersecurity research and development.”.

13 **SEC. 303. RESEARCH CENTERS FOR CYBERSECURITY.**

14 (a) ESTABLISHMENT.—Not later than 1 year after
 15 the date of enactment of this Act, the Director of the Na-
 16 tional Science Foundation, in coordination with the Sec-
 17 retary, shall establish cybersecurity research centers based
 18 at institutions of higher education and other entities that
 19 meet the criteria described in subsection (b) to develop so-
 20 lutions and strategies that support the efforts of the Fed-
 21 eral government under this Act in—

- 22 (1) improving the security and resilience of in-
- 23 formation infrastructure;
- 24 (2) reducing cyber vulnerabilities; and

1 (3) mitigating the consequences of cyber at-
2 tacks on critical infrastructure.

3 (b) CRITERIA FOR SELECTION.—In selecting an insti-
4 tution of higher education or other entity to serve as a
5 Research Center for Cybersecurity, the Director of the
6 National Science Foundation shall consider—

7 (1) demonstrated expertise in systems security,
8 wireless security, networking and protocols, formal
9 methods and high-performance computing, nanotech-
10 nology, and industrial control systems;

11 (2) demonstrated capability to conduct high
12 performance computation integral to complex cyber-
13 security research, whether through on-site or off-site
14 computing;

15 (3) demonstrated expertise in interdisciplinary
16 cybersecurity research;

17 (4) affiliation with private sector entities in-
18 volved with industrial research described in para-
19 graph (1) and ready access to testable commercial
20 data;

21 (5) prior formal research collaboration arrange-
22 ments with institutions of higher education and Fed-
23 eral research laboratories;

24 (6) capability to conduct research in a secure
25 environment; and

1 (7) affiliation with existing research programs
 2 of the Federal Government.

3 **SEC. 304. CENTERS OF EXCELLENCE.**

4 The Secretary and the Secretary of Defense may
 5 jointly establish academic and professional Centers of Ex-
 6 cellence in cybersecurity for the protection of critical infra-
 7 structure in conjunction with international academic and
 8 professional partners from countries that may include al-
 9 lies of the United States, as determined to be appropriate
 10 under title XIX of the Implementing Recommendations of
 11 the 9/11 Commission Act of 2007 (Public Law 110–53;
 12 121 Stat. 505) in order to research and develop tech-
 13 nologies, best practices, and other means to defend critical
 14 infrastructure.

15 **TITLE IV—EDUCATION,**
 16 **WORKFORCE, AND AWARENESS**

17 **SEC. 401. DEFINITIONS.**

18 In this title:

19 (1) CYBERSECURITY MISSION.—The term “cy-
 20 bersecurity mission” means activities that encom-
 21 pass the full range of threat reduction, vulnerability
 22 reduction, deterrence, international engagement, in-
 23 cident response, resiliency, and recovery policies and
 24 activities, including computer network operations, in-
 25 formation assurance, law enforcement, diplomacy,

1 military, and intelligence missions as such activities
2 relate to the security and stability of cyberspace.

3 (2) CYBERSECURITY MISSION OF A FEDERAL
4 AGENCY.—The term “cybersecurity mission of a
5 Federal agency” means the portion of a cybersecu-
6 rity mission that is the responsibility of a Federal
7 agency.

8 **SEC. 402. EDUCATION AND AWARENESS.**

9 (a) ASSESSMENT OF CYBERSECURITY EDUCATION IN
10 COLLEGES AND UNIVERSITIES.—

11 (1) REPORT.—Not later than 1 year after the
12 date of enactment of this Act, the Director of the
13 National Science Foundation shall submit to the
14 Committee on Commerce, Science, and Transpor-
15 tation of the Senate and the Committee on Science,
16 Space, and Technology of the House of Representa-
17 tives a report on the state of cybersecurity education
18 in institutions of higher education in the United
19 States.

20 (2) CONTENTS OF REPORT.—The report re-
21 quired under paragraph (1) shall include baseline
22 data on—

23 (A) the state of cybersecurity education in
24 the United States;

1 (B) the extent of professional development
2 opportunities for faculty in cybersecurity prin-
3 ciples and practices;

4 (C) descriptions of the content of cyberse-
5 curity courses in undergraduate computer
6 science curriculum;

7 (D) the extent of the partnerships and col-
8 laborative cybersecurity curriculum development
9 activities that leverage industry and government
10 needs, resources, and tools; and

11 (E) proposed metrics to assess progress to-
12 ward improving cybersecurity education.

13 (b) ENRICHMENT PROGRAMS.—The Director of the
14 National Science Foundation shall—

15 (1) encourage and support programming, in-
16 cluding summer enrichment programs, to be pro-
17 vided by nonprofit organizations, in math, computer
18 programming, science, technology, and engineering,
19 with a goal of increasing cybersecurity skills in stu-
20 dents enrolled in kindergarten through grade 12;
21 and

22 (2) when appropriate, provide opportunities for
23 top-achieving students to participate in the pro-
24 grams described in paragraph (1) at no cost.

1 (c) NATIONAL EDUCATION AND AWARENESS CAM-
2 PAIGN.—The Secretary, in consultation with appropriate
3 Federal agencies shall develop and implement outreach
4 and awareness programs on cybersecurity, including—

5 (1) in consultation with the Director of the Na-
6 tional Institute of Standards and Technology—

7 (A) a public education campaign to in-
8 crease the awareness of cybersecurity, cyber
9 safety, and cyber ethics, which shall include the
10 use of the Internet, social media, entertainment,
11 and other media to reach the public; and

12 (B) an education campaign to increase the
13 understanding of State and local governments
14 and private sector entities of the benefits of en-
15 suring effective risk management of the infor-
16 mation infrastructure versus the costs of failure
17 to do so and methods to mitigate and remediate
18 vulnerabilities;

19 (2) in coordination with the Secretary of Com-
20 merce, development of a program to publicly recog-
21 nize or identify products, services, and companies,
22 including owners and operators, that meet the high-
23 est standards of cybersecurity; and

24 (3) in accordance with subsection (d), a pro-
25 gram for carrying out collaborative education and

1 training activities for cybersecurity through a con-
2 sortium or other appropriate entity.

3 (d) COLLABORATIVE EDUCATION AND TRAINING.—

4 (1) IN GENERAL.—The consortium or other en-
5 tity established under subsection (c)(3) shall—

6 (A) provide training to State and local first
7 responders and officials specifically for pre-
8 paring and responding to cyber attacks;

9 (B) develop and update a curriculum and
10 training models for State and local first re-
11 sponders and officials;

12 (C) provide technical assistance services to
13 build and sustain capabilities in support of cy-
14 bersecurity preparedness and response; and

15 (D) conduct cybersecurity training and
16 simulation exercises to defend from and respond
17 to cyber attacks.

18 (2) MEMBERS.—The Consortium or other enti-
19 ty established under subsection (c)(3) shall consist
20 of academic, nonprofit, Federal Government, and
21 State and local government partners that develop,
22 update, and deliver cybersecurity training in support
23 of homeland security.

24 (e) CONSIDERATIONS.—In carrying out the authority
25 described in subsection (c), the Secretary of Commerce,

1 the Secretary, and the Director of the National Institute
 2 of Standards and Technology shall leverage existing pro-
 3 grams designed to inform the public of safety and security
 4 of products or services, including self-certifications and
 5 independently-verified assessments regarding the quan-
 6 tification and valuation of information security risk.

7 **SEC. 403. NATIONAL CYBERSECURITY COMPETITION AND**
 8 **CHALLENGE.**

9 (a) TALENT COMPETITION AND CHALLENGE.—

10 (1) IN GENERAL.—The Secretary and the Sec-
 11 retary of Commerce shall establish a program to
 12 conduct competitions and challenges and ensure the
 13 effective operation of national and statewide com-
 14 petitions and challenges that seek to identify, de-
 15 velop, and recruit talented individuals to work in
 16 Federal agencies, State and local government agen-
 17 cies, and the private sector to perform duties relat-
 18 ing to the security of the Federal information infra-
 19 structure or the national information infrastructure.

20 (2) PARTICIPATION.—Participants in the com-
 21 petitions and challenges of the program established
 22 under paragraph (1) shall include—

23 (A) students enrolled in grades 9 through
 24 12;

1 (B) students enrolled in a postsecondary
2 program of study leading to a baccalaureate de-
3 gree at an institution of higher education;

4 (C) students enrolled in a
5 postbaccalaureate program of study at an insti-
6 tution of higher education;

7 (D) institutions of higher education and
8 research institutions;

9 (E) veterans; and

10 (F) other groups or individuals as the Sec-
11 retary and the Secretary of Commerce deter-
12 mine appropriate.

13 (3) SUPPORT OF OTHER COMPETITIONS AND
14 CHALLENGES.—The program established under
15 paragraph (1) may support other competitions and
16 challenges not established under this subsection
17 through affiliation and cooperative agreements
18 with—

19 (A) Federal agencies;

20 (B) regional, State, or school programs
21 supporting the development of cyber profes-
22 sionals;

23 (C) State, local, and tribal governments; or

24 (D) other private sector organizations.

(4) AREAS OF TALENT.—The program established under paragraph (1) shall seek to identify, develop, and recruit exceptional talent relating to—

(A) ethical hacking;

(B) penetration testing;

(C) vulnerability assessment;

(D) continuity of system operations;

(E) cyber forensics;

(F) offensive and defensive cyber operations; and

(G) other areas to fulfill the cybersecurity mission as the Secretary determines appropriate.

(5) INTERNSHIPS.—The Director of the Office of Personnel Management shall establish, in coordination with the Director of the National Center for Cybersecurity and Communications, a program to provide, where appropriate, internships or other work experience in the Federal government to the winners of the competitions and challenges.

(b) NATIONAL RESEARCH AND DEVELOPMENT COMPETITION AND CHALLENGE.—

(1) IN GENERAL.—The Director of the National Science Foundation, in consultation with appropriate Federal agencies, shall establish a program of cyber-

1 security competitions and challenges to stimulate in-
2 novation in basic and applied cybersecurity research,
3 technology development, and prototype demonstra-
4 tion that has the potential for application to the in-
5 formation technology activities of the Federal Gov-
6 ernment.

7 (2) PARTICIPATION.—Participants in the com-
8 petitions and challenges of the program established
9 under paragraph (1) shall include—

10 (A) students enrolled in grades 9 through
11 12;

12 (B) students enrolled in a postsecondary
13 program of study leading to a baccalaureate de-
14 gree at an institution of higher education;

15 (C) students enrolled in a
16 postbaccalaureate program of study at an insti-
17 tution of higher education;

18 (D) institutions of higher education and
19 research institutions;

20 (E) veterans; and

21 (F) other groups or individuals as the Di-
22 rector of the National Science Foundation de-
23 termines appropriate.

1 (3) TOPICS.—In selecting topics for competi-
2 tions and challenges held as part of the program es-
3 tablished under paragraph (1), the Director—

4 (A) shall consult widely both within and
5 outside the Federal Government; and

6 (B) may empanel advisory committees.

7 (4) INTERNSHIPS.—The Director of the Office
8 of Personnel Management shall establish, in coordi-
9 nation with the Director of the National Science
10 Foundation, a program to provide, where appro-
11 priate, internships or other work experience in the
12 Federal government to the winners of the competi-
13 tions and challenges held as part of the program es-
14 tablished under paragraph (1).

15 **SEC. 404. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
16 **PROGRAM.**

17 (a) IN GENERAL.—The Director of the National
18 Science Foundation, in coordination with the Secretary,
19 shall establish a Federal Cyber Scholarship-for-Service
20 program to recruit and train the next generation of infor-
21 mation technology professionals, industrial control system
22 security professionals, and security managers to meet the
23 needs of the cybersecurity mission for the Federal Govern-
24 ment and State, local, and tribal governments.

1 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

2 The program established under subsection (a) shall—

3 (1) incorporate findings from the assessment
4 and development of the strategy under section 405;

5 (2) provide not more than 1,000 scholarships
6 per year, to students who are enrolled in a program
7 of study at an institution of higher education leading
8 to a degree or specialized program certification in
9 the cybersecurity field, in an amount that covers
10 each student's tuition and fees at the institution and
11 provides the student with an additional stipend;

12 (3) require each scholarship recipient, as a con-
13 dition of receiving a scholarship under the program,
14 to enter into an agreement under which the recipient
15 agrees to work in the cybersecurity mission of a
16 Federal, State, local, or tribal agency for a period
17 equal to the length of the scholarship following re-
18 ceipt of the student's degree if offered employment
19 in that field by a Federal, State, local, or tribal
20 agency;

21 (4) provide a procedure by which the National
22 Science Foundation or a Federal agency may, con-
23 sistent with regulations of the Office of Personnel
24 Management, request and fund security clearances
25 for scholarship recipients, including providing for

1 clearances during summer internships and after the
 2 recipient receives the degree; and

3 (5) provide opportunities for students to receive
 4 temporary appointments for meaningful employment
 5 in the cybersecurity mission of a Federal agency
 6 during school vacation periods and for internships.

7 (c) HIRING AUTHORITY.—

8 (1) IN GENERAL.—For purposes of any law or
 9 regulation governing the appointment of individuals
 10 in the Federal civil service, upon receiving a degree
 11 for which an individual received a scholarship under
 12 this section, the individual shall be—

13 (A) hired under the authority provided for
 14 in section 213.3102(r) of title 5, Code of Fed-
 15 eral Regulations; and

16 (B) exempt from competitive service.

17 (2) COMPETITIVE SERVICE POSITION.—Upon
 18 satisfactory fulfillment of the service term of an in-
 19 dividual hired under paragraph (1), the individual
 20 may be converted to a competitive service position
 21 without competition if the individual meets the re-
 22 quirements for that position.

23 (d) ELIGIBILITY.—To be eligible to receive a scholar-
 24 ship under this section, an individual shall—

1 (1) be a citizen or lawful permanent resident of
2 the United States;

3 (2) demonstrate a commitment to a career in
4 improving the security of information infrastructure;
5 and

6 (3) have demonstrated a high level of pro-
7 ficiency in mathematics, engineering, or computer
8 sciences.

9 (e) REPAYMENT.—If a recipient of a scholarship
10 under this section does not meet the terms of the scholar-
11 ship program, the recipient shall refund the scholarship
12 payments in accordance with rules established by the Di-
13 rector of the National Science Foundation, in coordination
14 with the Secretary.

15 (f) EVALUATION AND REPORT.—The Director of the
16 National Science Foundation shall evaluate and report pe-
17 riodically to Congress on the success of recruiting individ-
18 uals for the scholarships and on hiring and retaining those
19 individuals in the public sector workforce.

20 **SEC. 405. ASSESSMENT OF CYBERSECURITY FEDERAL**
21 **WORKFORCE.**

22 (a) IN GENERAL.—The Director of the Office of Per-
23 sonnel Management and the Secretary, in coordination
24 with the Director of National Intelligence, the Secretary
25 of Defense, and the Chief Information Officers Council es-

1 tablished under section 3603 of title 44, United States
2 Code, shall assess the readiness and capacity of the Fed-
3 eral workforce to meet the needs of the cybersecurity mis-
4 sion of the Federal Government.

5 (b) STRATEGY.—

6 (1) IN GENERAL.—Not later than 180 days
7 after the date of enactment of this Act, the Director
8 of the Office of Personnel Management, in consulta-
9 tion with the Director of the National Center for Cy-
10 bersecurity and Communications and the Director of
11 the Office of Management and Budget, shall develop
12 a comprehensive workforce strategy that enhances
13 the readiness, capacity, training, and recruitment
14 and retention of cybersecurity personnel of the Fed-
15 eral Government.

16 (2) CONTENTS.—The strategy developed under
17 paragraph (1) shall include—

18 (A) a 5-year plan on recruitment of per-
19 sonnel for the Federal workforce; and

20 (B) a 10-year projections of Federal work-
21 force needs.

22 (c) UPDATES.—The Director of the Office of Per-
23 sonnel Management, in consultation with the Director of
24 the National Center for Cybersecurity and Communica-
25 tions and the Director of the Office of Management and

1 Budget, shall update the strategy developed under sub-
 2 section (b) as needed.

3 **SEC. 406. FEDERAL CYBERSECURITY OCCUPATION CLASSI-**
 4 **FICATIONS.**

5 (a) IN GENERAL.—Not later than 1 year after the
 6 date of enactment of this Act, the Director of the Office
 7 of Personnel Management, in coordination with the Direc-
 8 tor of the National Center for Cybersecurity and Commu-
 9 nications, shall develop and issue comprehensive occupa-
 10 tion classifications for Federal employees engaged in cy-
 11 bersecurity missions.

12 (b) APPLICABILITY OF CLASSIFICATIONS.—The Di-
 13 rector of the Office of Personnel Management shall ensure
 14 that the comprehensive occupation classifications issued
 15 under subsection (a) may be used throughout the Federal
 16 Government.

17 **SEC. 407. TRAINING AND EDUCATION OF FEDERAL EM-**
 18 **PLOYEES.**

19 (a) DEFINITION.—In this section, the term “agency
 20 information infrastructure” means the Federal informa-
 21 tion infrastructure of a Federal agency.

22 (b) TRAINING.—

23 (1) FEDERAL GOVERNMENT EMPLOYEES AND
 24 FEDERAL CONTRACTORS.—The Director of the Of-
 25 fice of Personnel Management, in coordination with

1 the Secretary, the Director of National Intelligence,
2 the Secretary of Defense, and the Chief Information
3 Officers Council established under section 3603 of
4 title 44, United States Code, shall establish a cyber-
5 security awareness and education curriculum that
6 shall be required for all Federal employees and con-
7 tractors engaged in the design, development, or op-
8 eration of an agency information infrastructure or
9 the Federal information infrastructure.

10 (2) CONTENTS.—The curriculum established
11 under paragraph (1) shall include, at a minimum—

12 (A) role-based security awareness training;

13 (B) recommended cybersecurity practices;

14 (C) cybersecurity recommendations for
15 traveling abroad;

16 (D) unclassified counterintelligence infor-
17 mation;

18 (E) information regarding industrial espio-
19 nage;

20 (F) information regarding malicious activ-
21 ity online;

22 (G) information regarding cybersecurity
23 and law enforcement;

24 (H) identity management information;

1 (I) information regarding supply chain se-
2 curity;

3 (J) information security risks associated
4 with the activities of Federal employees and
5 contractors; and

6 (K) the responsibilities of Federal employ-
7 ees and contractors in complying with policies
8 and procedures designed to reduce information
9 security risks identified under subparagraph
10 (J).

11 (3) FEDERAL CYBERSECURITY PROFES-
12 SIONALS.—The Director of the Office of Personnel
13 Management in conjunction with the Secretary, the
14 Director of National Intelligence, the Secretary of
15 Defense, the Director of the Office of Management
16 and Budget, and, as appropriate, colleges, univer-
17 sities, and nonprofit organizations with cybersecurity
18 training expertise, shall develop a program to pro-
19 vide training to improve and enhance the skills and
20 capabilities of Federal employees engaged in the cy-
21 bersecurity mission, including training specific to the
22 acquisition workforce.

23 (4) HEADS OF FEDERAL AGENCIES.—Not later
24 than 30 days after the date on which an individual
25 is appointed to a position at level I or II of the Ex-

1 executive Schedule, the Secretary and the Director of
2 National Intelligence shall provide that individual
3 with a cybersecurity threat briefing.

4 (5) CERTIFICATION.—The head of each Federal
5 agency shall include in the annual report required
6 under section 3554(c) of title 44, United States
7 Code, as amended by this Act, a certification regard-
8 ing whether all employees and contractors of the
9 Federal agency have completed the training required
10 under this subsection.

11 (c) RECRUITMENT.—The Director of the Office of
12 Personnel Management, in coordination with the Director
13 of the National Center for Cybersecurity and Communica-
14 tions, shall develop strategies and programs to recruit stu-
15 dents enrolled in institutions of higher education and stu-
16 dents enrolled in career and technical institutions in the
17 United States to serve as Federal employees engaged in
18 cybersecurity missions.

19 (d) LEADERSHIP IN CYBERSECURITY.—The head of
20 each Federal agency shall adopt best practices, developed
21 by the Office of Personnel Management, regarding effec-
22 tive ways to educate and motivate employees of the Fed-
23 eral Government to demonstrate leadership in cybersecu-
24 rity, including—

1 (1) promotions and other nonmonetary awards;
2 and

3 (2) publicizing information sharing accomplish-
4 ments by individual employees and, if appropriate,
5 the tangible benefits that resulted.

6 **SEC. 408. NATIONAL CENTER FOR CYBERSECURITY AND**
7 **COMMUNICATIONS ACQUISITION AUTHORI-**
8 **TIES.**

9 (a) IN GENERAL.—Subtitle E of title II of the Home-
10 land Security Act of 2002, as added by section 204, is
11 amended by adding at the end the following:

12 **“SEC. 245. NATIONAL CENTER FOR CYBERSECURITY AND**
13 **COMMUNICATIONS ACQUISITION AUTHORI-**
14 **TIES.**

15 “(a) IN GENERAL.—The National Center for Cyber-
16 security and Communications is authorized to use the au-
17 thorities under subsections (c)(1) and (d)(1)(B) of section
18 2304 of title 10, United States Code, instead of the au-
19 thorities under subsections (a)(1) and (b)(2) of section
20 3304 of title 41, United States Code, subject to all other
21 requirements of sections 3301 and 3304 of title 41, United
22 States Code.

23 “(b) GUIDELINES.—Not later than 90 days after the
24 date of enactment of the Cybersecurity Act of 2012, the

1 chief procurement officer of the Department shall issue
2 guidelines for use of the authority under subsection (a).

3 “(c) TERMINATION.—The National Center for Cyber-
4 security and Communications may not use the authority
5 under subsection (a) on and after the date that is 3 years
6 after the date of enactment of this Act.

7 “(d) REPORTING.—

8 “(1) IN GENERAL.—On a semiannual basis, the
9 Director of the Center shall submit a report on use
10 of the authority granted by subsection (a) to—

11 “(A) the Committee on Homeland Security
12 and Governmental Affairs of the Senate; and

13 “(B) the Committee on Homeland Security
14 of the House of Representatives.

15 “(2) CONTENTS.—Each report submitted under
16 paragraph (1) shall include, at a minimum—

17 “(A) the number of contract actions taken
18 under the authority under subsection (a) during
19 the period covered by the report; and

20 “(B) for each contract action described in
21 subparagraph (A)—

22 “(i) the total dollar value of the con-
23 tract action;

24 “(ii) a summary of the market re-
25 search conducted by the National Center

for Cybersecurity and Communications, including a list of all offerors who were considered and those who actually submitted bids, in order to determine that use of the authority was appropriate; and

“(iii) a copy of the justification and approval documents required by section 3304(e) of title 41, United States Code.

“(3) CLASSIFIED ANNEX.—A report submitted under this subsection shall be submitted in an unclassified form, but may include a classified annex, if necessary.

**“SEC. 246. RECRUITMENT AND RETENTION PROGRAM FOR
THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.**

“(a) DEFINITIONS.—In this section:

“(1) COLLECTIVE BARGAINING AGREEMENT.—The term ‘collective bargaining agreement’ has the meaning given that term in section 7103(a)(8) of title 5, United States Code.

“(2) QUALIFIED EMPLOYEE.—The term ‘qualified employee’ means an employee who performs functions relating to the security of Federal systems and critical information infrastructure.

“(b) GENERAL AUTHORITY.—

1 “(1) ESTABLISH POSITIONS, APPOINT PER-
2 SONNEL, AND FIX RATES OF PAY.—The Secretary
3 may exercise with respect to qualified employees of
4 the Department the same authority of that the Sec-
5 retary of Defense has with respect to civilian intel-
6 ligence personnel under sections 1601, 1602, and
7 1603 of title 10, United States Code, to establish as
8 positions in the excepted service, to appoint individ-
9 uals to those positions, and fix pay. Such authority
10 shall be exercised subject to the same conditions and
11 limitations applicable to the Secretary of Defense
12 with respect to civilian intelligence personnel of the
13 Department of Defense.

14 “(2) SCHOLARSHIP PROGRAM.—The Secretary
15 may exercise with respect to qualified employees of
16 the Department the same authority of the Secretary
17 of Defense has with respect to civilian personnel
18 under section 2200a of title 10, United States Code,
19 to the same extent, and subject to the same condi-
20 tions and limitations, that the Secretary of Defense
21 may exercise such authority with respect to civilian
22 personnel of the Department of Defense.

23 “(3) PLAN FOR EXECUTION OF AUTHORI-
24 TIES.—Not later than 120 days after the date of en-
25 actment of this subtitle, the Secretary shall submit

1 a report to the appropriate committees of Congress
2 with a plan for the use of the authorities provided
3 under this subsection.

4 “(4) COLLECTIVE BARGAINING AGREEMENTS.—
5 Nothing in paragraph (1) may be construed to im-
6 pair the continued effectiveness of a collective bar-
7 gaining agreement with respect to an office, compo-
8 nent, subcomponent, or equivalent of the Depart-
9 ment that is a successor to an office, component,
10 subcomponent, or equivalent of the Department cov-
11 ered by the agreement before the succession.

12 “(5) REQUIRED REGULATIONS.—The Secretary,
13 in coordination with the Director of the Center and
14 the Director of the Office of Personnel Management,
15 shall prescribe regulations for the administration of
16 this section.

17 “(c) MERIT SYSTEM PRINCIPLES AND CIVIL SERVICE
18 PROTECTIONS: APPLICABILITY.—

19 “(1) APPLICABILITY OF MERIT SYSTEM PRIN-
20 CIPLES.—The Secretary shall exercise the authority
21 under subsection (b) in a manner consistent with the
22 merit system principles set forth in section 2301 of
23 title 5, United States Code.

24 “(2) CIVIL SERVICE PROTECTIONS.—Section
25 1221, section 2302, and chapter 75 of title 5,

1 United States Code, shall apply to the positions es-
2 tablished under subsection (b)(1).

3 “(d) REQUIREMENTS.—Before the initial exercise of
4 any authority authorized under subsection (b)(1) the Sec-
5 retary shall—

6 “(1) seek input from affected employees, and
7 the union representatives of affected employees as
8 applicable, and Federal manager and professional
9 associations into the design and implementation of a
10 fair, credible, and transparent system for exercising
11 any authority under subsection (b)(1);

12 “(2) make a good faith attempt to resolve any
13 employee concerns regarding proposed changes in
14 conditions of employment through discussions with
15 the groups described in paragraph (1);

16 “(3) develop a program to provide training to
17 supervisors of cybersecurity employees at the De-
18 partment on the use of the new authorities, includ-
19 ing actions, options, and strategies a supervisor may
20 use in—

21 “(A) developing and discussing relevant
22 goals and objectives with the employee, commu-
23 nicating and discussing progress relative to per-
24 formance goals and objectives, and conducting
25 performance appraisals;

1 “(B) mentoring and motivating employees,
2 and improving employee performance and pro-
3 ductivity;

4 “(C) fostering a work environment charac-
5 terized by fairness, respect, equal opportunity,
6 and attention to the quality of work of the em-
7 ployees;

8 “(D) effectively managing employees with
9 unacceptable performance;

10 “(E) addressing reports of a hostile work
11 environment, reprisal, or harassment of or by
12 another supervisor or employee; and

13 “(F) otherwise carrying out the duties and
14 responsibilities of a supervisor;

15 “(4) develop a program to provide training to
16 supervisors of cybersecurity employees at the De-
17 partment on the prohibited personnel practices
18 under section 2302 of title 5, United States Code,
19 (particularly with respect to the practices described
20 in paragraphs (1) and (8) of section 2302(b) of title
21 5, United States Code), employee collective bar-
22 gaining and union participation rights, and the pro-
23 cedures and processes used to enforce employee
24 rights; and

1 “(5) develop a program under which experi-
2 enced supervisors mentor new supervisors by—

3 “(A) sharing knowledge and advice in
4 areas such as communication, critical thinking,
5 responsibility, flexibility, motivating employees,
6 teamwork, leadership, and professional develop-
7 ment; and

8 “(B) pointing out strengths and areas for
9 development.

10 “(e) SUPERVISOR REQUIREMENT.—

11 “(1) IN GENERAL.—Except as provided in para-
12 graph (2), not later than 1 year after the date of en-
13 actment of the Cybersecurity Act of 2012 and every
14 3 years thereafter, every supervisor of cybersecurity
15 employees at the Department shall complete the pro-
16 grams established under paragraphs (3) and (4) of
17 subsection (d).

18 “(2) EXCEPTION.—A supervisor of cybersecu-
19 rity employees at the Department who is appointed
20 after the date of enactment of the Cybersecurity Act
21 of 2012 shall complete the programs established
22 under paragraphs (3) and (4) of subsection (d) not
23 later than 1 year after the date on which the super-
24 visor is appointed to the position, and every 3 years
25 thereafter.

1 “(3) ONGOING PARTICIPATION.—Participation
2 by supervisors of cybersecurity employees at the De-
3 partment in the program established under sub-
4 section (d)(5) shall be ongoing.

5 “(f) CONVERSION TO COMPETITIVE SERVICE.—In
6 consultation with the Director of the Center, the Secretary
7 may grant competitive civil service status to a qualified
8 employee appointed to the excepted service under sub-
9 section (b) if that employee is employed in the Center or
10 is transferring to the Center.

11 “(g) ANNUAL REPORT.—Not later than 1 year after
12 the date of enactment of this subtitle, and every year
13 thereafter for 4 years, the Secretary shall submit to the
14 appropriate committees of Congress a detailed report
15 that—

16 “(1) discusses the process used by the Sec-
17 retary in accepting applications, assessing can-
18 didates, ensuring adherence to veterans’ preference,
19 and selecting applicants for vacancies to be filled by
20 a qualified employee;

21 “(2) describes—

22 “(A) how the Secretary plans to fulfill the
23 critical need of the Department to recruit and
24 retain qualified employees;

1 “(B) the measures that will be used to
2 measure progress; and

3 “(C) any actions taken during the report-
4 ing period to fulfill such critical need;

5 “(3) discusses how the planning and actions
6 taken under paragraph (2) are integrated into the
7 strategic workforce planning of the Department;

8 “(4) provides metrics on actions occurring dur-
9 ing the reporting period, including—

10 “(A) the number of qualified employees
11 hired by occupation and grade and level or pay
12 band;

13 “(B) the total number of veterans hired;

14 “(C) the number of separations of qualified
15 employees by occupation and grade and level or
16 pay band;

17 “(D) the number of retirements of quali-
18 fied employees by occupation and grade and
19 level or pay band; and

20 “(E) the number and amounts of recruit-
21 ment, relocation, and retention incentives paid
22 to qualified employees by occupation and grade
23 and level or pay band.”.

24 (b) TECHNICAL AND CONFORMING AMENDMENT.—

25 The table of contents in section 1(b) of the Homeland Se-

1 curity Act of 2002 (6 U.S.C. 101 et seq.), as amended
 2 by section 204, is amended by inserting after the item re-
 3 lating to section 244 the following:

“Sec. 245. National Center for Cybersecurity and Communications acquisition
 authorities.

“Sec. 246. Recruitment and retention program for the national center for cy-
 bersecurity and communications.”.

4 **SEC. 409. REPORTS ON CYBER INCIDENTS AGAINST GOV-**
 5 **ERNMENT NETWORKS.**

6 (a) DEPARTMENT OF HOMELAND SECURITY.—Not
 7 later than 180 days after the date of enactment of this
 8 Act, and annually thereafter, the Secretary shall submit
 9 to Congress a report that—

10 (1) summarizes major cyber incidents involving
 11 networks of Executive agencies (as defined in section
 12 105 of title 5, United States Code), except for the
 13 Department of Defense;

14 (2) provides aggregate statistics on the number
 15 of breaches of networks of Executive agencies, the
 16 volume of data exfiltrated, and the estimated cost of
 17 remedying the breaches; and

18 (3) discusses the risk of cyber sabotage.

19 (b) DEPARTMENT OF DEFENSE.—Not later than 180
 20 days after the date of enactment of this Act, and annually
 21 thereafter, the Secretary of Defense shall submit to Con-
 22 gress a report that—

1 (1) summarizes major cyber incidents against
2 networks of the Department of Defense and the
3 military departments;

4 (2) provides aggregate statistics on the number
5 of breaches against networks of the Department of
6 Defense and the military departments, the volume of
7 data exfiltrated, and the estimated cost of remedying
8 the breaches; and

9 (3) discusses the risk of cyber sabotage.

10 (c) FORM OF REPORTS.—Each report submitted
11 under this section shall be in unclassified form, but may
12 include a classified annex as necessary to protect sources,
13 methods, and national security.

14 (d) CONTENTS OF REPORTS.—Each report submitted
15 under this section may be based in whole or in part on
16 the reporting requirements under section 3553 of chapter
17 35 of title 44, United States Code, as amended by this
18 Act.

19 **SEC. 410. REPORTS ON PROSECUTION FOR CYBERCRIME.**

20 (a) IN GENERAL.—Not later than 180 days after the
21 date of enactment of this Act, the Attorney General and
22 the Directors of the Federal Bureau of Investigation and
23 the United States Secret Service shall submit to Congress
24 reports—

1 (1) describing investigations and prosecutions
2 relating to cyber intrusions or other cybercrimes the
3 preceding year, including—

4 (A) the number of investigations initiated
5 relating to such crimes;

6 (B) the number of arrests relating to such
7 crimes;

8 (C) the number and description of in-
9 stances in which investigations or prosecutions
10 relating to such crimes have been delayed or
11 prevented because of an inability to extradite a
12 criminal defendant in a timely manner; and

13 (D) the number of prosecutions for such
14 crimes, including—

15 (i) the number of defendants pros-
16 ecuted;

17 (ii) whether the prosecutions resulted
18 in a conviction;

19 (iii) the sentence imposed and the
20 statutory maximum for each such crime
21 for which a defendant was convicted; and

22 (iv) the average sentence imposed for
23 a conviction of such crimes;

24 (2) identifying the number of employees, finan-
25 cial resources, and other resources (such as tech-

1 nology and training) devoted to the enforcement, in-
2 vestigation, and prosecution of cyber intrusions or
3 other cybercrimes, including the number of inves-
4 tigators, prosecutors, and forensic specialists dedi-
5 cated to investigating and prosecuting cyber intru-
6 sions or other cybercrimes; and

7 (3) discussing any impediments under the laws
8 of the United States or international law to prosecu-
9 tions for cyber intrusions or other cybercrimes.

10 (b) UPDATES.—The Attorney General and the Direc-
11 tors of the Federal Bureau of Investigation and the
12 United States Secret Service shall annually submit to Con-
13 gress reports updating the reports submitted under sub-
14 section (a) at the same time the Attorney General and
15 the Directors submit annual reports under section 404 of
16 the Prioritizing Resources and Organization for Intellec-
17 tual Property Act of 2008 (42 U.S.C. 3713d).

18 **SEC. 411. REPORT ON RESEARCH RELATING TO SECURE**
19 **DOMAIN.**

20 (a) IN GENERAL.—The Secretary shall enter into a
21 contract with the National Research Council, or another
22 federally funded research and development corporation,
23 under which the Council or corporation shall submit to
24 Congress reports on available technical options, consistent
25 with constitutional and statutory privacy rights, for en-

1 hancing the security of the information networks of enti-
 2 ties that own or manage critical infrastructure through—

3 (1) technical improvements, including devel-
 4 oping a secure domain; or

5 (2) increased notice of and consent to the use
 6 of technologies to scan for, detect, and defeat cyber
 7 security threats, such as technologies used in a se-
 8 cure domain.

9 (b) **TIMING.**—The contract entered into under sub-
 10 section (a) shall require that the report described in sub-
 11 section (a) be submitted—

12 (1) not later than 180 days after the date of
 13 enactment of this Act;

14 (2) annually, after the first report submitted
 15 under subsection (a), for 3 years; and

16 (3) more frequently, as determined appropriate
 17 by the Secretary in response to new risks or tech-
 18 nologies that emerge.

19 **SEC. 412. REPORT ON PREPAREDNESS OF FEDERAL**
 20 **COURTS TO PROMOTE CYBERSECURITY.**

21 Not later than 180 days after the date of enactment
 22 of this Act, the Attorney General, in coordination with the
 23 Administrative Office of the United States Courts, shall
 24 submit to Congress a report—

1 (1) on whether Federal courts have granted
2 timely relief in matters relating to botnets and other
3 cybercrime and cyber security threats; and

4 (2) that includes, as appropriate, recommenda-
5 tions on changes or improvements to—

6 (A) the Federal Rules of Civil Procedure
7 or the Federal Rules of Criminal Procedure;

8 (B) the training and other resources avail-
9 able to support the Federal judiciary;

10 (C) the capabilities and specialization of
11 courts to which such cases may be assigned;
12 and

13 (D) Federal civil and criminal laws.

14 **SEC. 413. REPORT ON IMPEDIMENTS TO PUBLIC AWARE-**
15 **NESS.**

16 Not later than 180 days after the date of enactment
17 of this Act, and annually thereafter for 3 years (or more
18 frequently if determined appropriate by the Secretary) the
19 Secretary shall submit to Congress a report on—

20 (1) legal or other impediments to appropriate
21 public awareness of—

22 (A) the nature of, methods of propagation
23 of, and damage caused by common cyber secu-
24 rity threats such as computer viruses, phishing
25 techniques, and malware;

1 (B) the minimal standards of computer se-
2 curity necessary for responsible Internet use;
3 and

4 (C) the availability of commercial off the
5 shelf technology that allows consumers to meet
6 such levels of computer security;

7 (2) a summary of the plans of the Secretary to
8 enhance public awareness of common cyber security
9 threats, including a description of the metrics used
10 by the Department for evaluating the efficacy of
11 public awareness campaigns; and

12 (3) recommendations for congressional actions
13 to address these impediments to appropriate public
14 awareness of common cyber security threats.

15 **SEC. 414. REPORT ON PROTECTING THE ELECTRICAL GRID**
16 **OF THE UNITED STATES.**

17 Not later than 180 days after the date of enactment
18 of this Act, the Secretary, in consultation with the Sec-
19 retary of Defense and the Director of National Intel-
20 ligence, shall submit to Congress a report on—

21 (1) the threat of a cyber attack disrupting the
22 electrical grid of the United States;

23 (2) the implications for the national security of
24 the United States if the electrical grid is disrupted;

1 (3) the options available to the United States
 2 and private sector entities to quickly reconstitute
 3 electrical service to provide for the national security
 4 of the United States, and, within a reasonable time
 5 frame, the reconstitution of all electrical service
 6 within the United States; and

7 (4) a plan to prevent disruption of the electric
 8 grid of the United States caused by a cyber attack.

9 **SEC. 415. MARKETPLACE INFORMATION.**

10 (a) SENSE OF CONGRESS.—It is the sense of Con-
 11 gress that—

12 (1) registrants that file reports with the Securi-
 13 ties and Exchange Commission have an obligation to
 14 disclose material risks to investors; and

15 (2) as with longstanding rules regarding other
 16 material risks, information security risks and related
 17 events that are material to investors should be dis-
 18 closed on a regular basis to provide quality informa-
 19 tion to the marketplace and enable informed investor
 20 decisions.

21 (b) DEFINITION OF INFORMATION SECURITY RISK.—
 22 In this section, the term “information security risk and
 23 related events” means the risk to a registrant’s business
 24 operations, assets, financial condition, strategy, competi-
 25 tive positioning, and reputation, due to the potential for

1 unauthorized access, use, disclosure, disruption, modifica-
2 tion, or destruction of registrant information, information
3 of third parties collected by the registrant, or information
4 systems of the registrant.

5 (c) GUIDANCE.—Not later than 1 year after the date
6 of enactment of this Act, the Securities and Exchange
7 Commission (referred to in this section as the “Commis-
8 sion”) shall evaluate existing guidance to registrants re-
9 lated to disclosures by registrants of information security
10 risks and related events (including Securities and Ex-
11 change Commission Division of Corporation Finance, CF
12 Disclosure Guidance: Topic No. 2, Cybersecurity) to deter-
13 mine whether such guidance, in light of the evaluation,
14 should be—

15 (1) updated by the Division of Corporation Fi-
16 nance; or

17 (2) issued as Commission interpretive guidance.

18 (d) ANNUAL REPORTS.—For 5 years following the
19 evaluation under subsection (b), the Commission shall sub-
20 mit to Congress, on an annual basis, a report that re-
21 views—

22 (1) the types of information security risks and
23 related events that registrants disclosed in the pre-
24 vious year;

1 (2) whether the staff of the Commission has re-
 2 requested registrants to provide additional information
 3 on the disclosures under paragraph (1);

4 (3) any awareness or education activities for
 5 registrants or investors, on the subject of informa-
 6 tion security risks and related events disclosure re-
 7 quirements, sponsored by the Commission or at-
 8 tended by a Commissioner or staff of the Commis-
 9 sion; and

10 (4) any public actions commenced by the Com-
 11 mission relating to the enforcement of disclosure re-
 12 quirements pertaining to the information security
 13 risks and related events.

14 **TITLE V—FEDERAL ACQUI-**
 15 **TION RISK MANAGEMENT**
 16 **STRATEGY**

17 **SEC. 501. FEDERAL ACQUISITION RISK MANAGEMENT**
 18 **STRATEGY.**

19 (a) IN GENERAL.—The Secretary, in coordination
 20 with relevant private sector and academic experts and each
 21 Federal entity described in paragraphs (1) through (9) of
 22 subsection (b), shall develop and periodically update an ac-
 23 quisition risk management strategy designed to ensure,
 24 based on mission criticality and cost effectiveness, the se-
 25 curity of the Federal information infrastructure.

1 (b) COORDINATION.—In developing the acquisition
2 risk management strategy required under subsection (a),
3 the Secretary shall coordinate with—

4 (1) the Secretary of Defense;

5 (2) the Secretary of Commerce;

6 (3) the Secretary of State;

7 (4) the Director of National Intelligence;

8 (5) the Administrator of General Services;

9 (6) the Administrator for Federal Procurement
10 Policy;

11 (7) the members of the Chief Information Offi-
12 cers Council established under section 3603 of title
13 44, United States Code;

14 (8) the Chief Acquisition Officers Council estab-
15 lished under section 1311 of title 41, United States
16 Code; and

17 (9) the Chief Financial Officers Council estab-
18 lished under section 302 of the Chief Financial Offi-
19 cers Act of 1990 (31 U.S.C. 901 note).

20 (c) ELEMENTS.—The risk management strategy de-
21 veloped under subsection (a) shall—

22 (1) address risks in the acquisition of any part
23 of the Federal information infrastructure; and

24 (2) include developing processes that—

1 (A) incorporate all-source intelligence anal-
2 ysis into assessments of the integrity of the
3 supply chain for the Federal information infra-
4 structure;

5 (B) incorporate internationally recognized
6 standards, guidelines, and best practices, in-
7 cluding those developed by the private sector,
8 for supply chain integrity;

9 (C) enhance capabilities to test and evalu-
10 ate software and hardware within or for use in
11 the Federal information infrastructure, and,
12 where appropriate, make the capabilities avail-
13 able for use by the private sector;

14 (D) protect the intellectual property and
15 trade secrets of suppliers of information and
16 communications technology products and serv-
17 ices;

18 (E) share with the private sector, to the
19 fullest extent possible, the risks identified in the
20 supply chain and working with the private sec-
21 tor to mitigate those threats as identified;

22 (F) identify specific acquisition practices of
23 Federal agencies that increase risks to the sup-
24 ply chain and develop a process to provide rec-

ommendations for revisions to those processes;
and

(G) to the maximum extent practicable,
promote the ability of Federal agencies to pro-
cure authentic commercial off-the-shelf informa-
tion and communications technology products
and services from a diverse pool of suppliers,
consistent with the preferences for the acquisi-
tion of commercial items under section 2377 of
title 10, United States Code, and section 3307
of title 41, United States Code.

**SEC. 502. AMENDMENTS TO CLINGER-COHEN PROVISIONS
TO ENHANCE AGENCY PLANNING FOR INFOR-
MATION SECURITY NEEDS.**

Chapter 113 of title 40, United States Code, is
amended—

(1) in section 11302—

(A) in subsection (f), by striking “tech-
nology.” and inserting “technology, including
information technology or network information
security requirements.”;

(B) in subsection (i)—

(i) by inserting “, including informa-
tion security requirements,” after “infor-
mation resources management”; and

1 (ii) by adding at the end the fol-
2 lowing: “The Administrator for Federal
3 Procurement Policy, in coordination with
4 the Chief Information Officers Council and
5 the Federal Acquisition Institute, shall en-
6 sure that contracting officers and the indi-
7 viduals preparing descriptions of the Gov-
8 ernment requirements and statements of
9 work have adequate training in informa-
10 tion security requirements, including in in-
11 formation technology security contracts.”;

12 (C) in subsection (j), by adding at the end
13 the following: “The Director shall review and
14 report on possible impediments in the acquisi-
15 tion process or elsewhere that are acting to slow
16 agency uptake of the newest, most secure tech-
17 nologies.”; and

18 (D) by adding at the end the following:

19 “(l) MULTIPLE AWARD SCHEDULE FOR INFORMA-
20 TION SECURITY.—The Administrator of General Services
21 shall develop a special item number under Schedule 70
22 for information security products and services and consoli-
23 date those products and services under that special item
24 number to promote acquisition.

1 “(m) REDUCING THE USE OF COUNTERFEIT PROD-
 2 UCTS.—Not later than 180 days after the date of enact-
 3 ment of the Cybersecurity Act of 2012, the Director shall
 4 issue guidance requiring, to the extent practicable, Federal
 5 agencies to purchase information technology products only
 6 through the authorized channels or distributors of a sup-
 7 plier.”; and

8 (2) in section 11312(b)(3), by inserting “, in-
 9 formation security improvement,” after “risk-ad-
 10 justed return on investment”.

11 **TITLE VI—INTERNATIONAL** 12 **COOPERATION**

13 **SEC. 601. DEFINITIONS.**

14 In this title:

15 (1) COMPUTER SYSTEM; COMPUTER DATA.—
 16 The terms “computer system” and “computer data”
 17 have the meanings given those terms in chapter I of
 18 the Convention on Cybercrime.

19 (2) CONVENTION ON CYBERCRIME.—The term
 20 “Convention on Cybercrime” means the Council of
 21 Europe’s Convention on Cybercrime, done at Buda-
 22 pest November 23, 2001 as ratified by the United
 23 States Senate on August 3, 2006 (Treaty 108–11)
 24 with any relevant reservations or declarations.

1 (3) CYBER ISSUES.—The term “cyber issues”
2 means the full range of international policies de-
3 signed to ensure an open, interoperable, secure, and
4 reliable global information and communications in-
5 frastructure.

6 (4) CYBERCRIME.—The term “cybercrime” re-
7 fers to criminal offenses relating to computer sys-
8 tems of computer data described in the Convention
9 of Cybercrime.

10 (5) RELEVANT FEDERAL AGENCIES.—The term
11 “relevant Federal agencies” means any Federal
12 agency that has responsibility for combating
13 cybercrime globally, including the Department of
14 Commerce, the Department of Homeland Security,
15 the Department of Justice, the Department of State,
16 the Department of the Treasury, and the Office of
17 the United States Trade Representative.

18 **SEC. 602. FINDINGS.**

19 Congress finds the following:

20 (1) On February 2, 2010, Admiral Dennis C.
21 Blair, the Director of National Intelligence, testified
22 before the Select Committee on Intelligence of the
23 Senate regarding the Annual Threat Assessment of
24 the U.S. Intelligence Community, stating “The na-
25 tional security of the United States, our economic

1 prosperity, and the daily functioning of our govern-
2 ment are dependent on a dynamic public and private
3 information infrastructure, which includes tele-com-
4 munications, computer networks and systems, and
5 the information residing within. This critical infra-
6 structure is severely threatened. . . . We cannot pro-
7 tect cyberspace without a coordinated and collabo-
8 rative effort that incorporates both the US private
9 sector and our international partners.”

10 (2) In a January 2010 speech on Internet free-
11 dom, Secretary of State Hillary Clinton stated:
12 “Those who disrupt the free flow of information in
13 our society, or any other, pose a threat to our econ-
14 omy, our government, and our civil society. Coun-
15 tries or individuals that engage in cyber attacks
16 should face consequences and international con-
17 demnation. In an Internet-connected world, an at-
18 tack on one nation’s networks can be an attack on
19 all. And by reinforcing that message, we can create
20 norms of behavior among states and encourage re-
21 spect for the global networked commons.”

22 (3) November 2011 marked the tenth anniver-
23 sary of the Convention on Cybercrime, the only mul-
24 tilateral agreement on cybercrime, to which the Sen-

1 ate provided advice and consent on August 3, 2006,
 2 and is currently ratified by over 30 countries.

3 (4) The May 2009 White House Cyberspace
 4 Policy Review asserts “[t]he Nation also needs a
 5 strategy for cybersecurity designed to shape the
 6 international environment and bring like-minded na-
 7 tions together on a host of issues, such as technical
 8 standards and acceptable legal norms regarding ter-
 9 ritorial jurisdiction, sovereign responsibility, and use
 10 of force. International norms are critical to estab-
 11 lishing a secure and thriving digital infrastructure.”

12 **SEC. 603. SENSE OF CONGRESS.**

13 It is the sense of Congress that—

14 (1) engagement with other countries to advance
 15 the cyberspace objectives of the United States should
 16 be an integral part of the conduct of United States
 17 foreign relations and diplomacy;

18 (2) the cyberspace objectives of the United
 19 States include the full range of cyber issues, includ-
 20 ing issues related to governance, standards, cyberse-
 21 curity, cybercrime, international security, human
 22 rights, and the free flow of information;

23 (3) it is in the interest of the United States to
 24 work with other countries to build consensus on
 25 principles and standards of conduct that protect

1 computer systems and users that rely on them, pre-
2 vent and punish acts of cybercrime, and promote the
3 free flow of information;

4 (4) a comprehensive national cyberspace strat-
5 egy must include tools for addressing threats to
6 computer systems and acts of cybercrime from
7 sources and by persons outside the United States;

8 (5) developing effective solutions to inter-
9 national cyberspace threats requires engagement
10 with foreign countries on a bilateral basis and
11 through relevant regional and multilateral fora;

12 (6) it is in the interest of the United States to
13 encourage the development of effective frameworks
14 for international cooperation to combat cyberthreats,
15 and the development of foreign government capabili-
16 ties to combat cyberthreats; and

17 (7) the Secretary of State, in consultation with
18 other relevant Federal agencies, should develop and
19 lead Federal Government efforts to engage with
20 other countries to advance the cyberspace objectives
21 of the United States, including efforts to bolster an
22 international framework of cyber norms, governance
23 and deterrence.

1 **SEC. 604. COORDINATION OF INTERNATIONAL CYBER**
2 **ISSUES WITHIN THE UNITED STATES GOV-**
3 **ERNMENT.**

4 The Secretary of State is authorized to designate a
5 senior level official at the Department of State, to carry
6 out the Secretary's responsibilities to—

7 (1) coordinate the United States global diplo-
8 matic engagement on the full range of international
9 cyber issues, including building multilateral coopera-
10 tion and developing international norms, common
11 policies, and responses to secure the integrity of
12 cyberspace;

13 (2) provide strategic direction and coordination
14 for United States Government policy and programs
15 aimed at addressing and responding to cyber issues
16 overseas, especially in relation to issues that affect
17 United States foreign policy and related national se-
18 curity concerns;

19 (3) coordinate with relevant Federal agencies,
20 including the Department, the Department of De-
21 fense, the Department of the Treasury, the Depart-
22 ment of Justice, the Department of Commerce, and
23 the intelligence community to develop interagency
24 plans regarding international cyberspace, cybersecu-
25 rity, and cybercrime issues; and

(4) ensure that cyber issues, including cybersecurity and cybercrime, are included in the responsibilities of overseas Embassies and consulates of the United States, as appropriate.

**SEC. 605. CONSIDERATION OF CYBERCRIME IN FOREIGN
POLICY AND FOREIGN ASSISTANCE PRO-
GRAMS.**

(a) BRIEFING.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary of State, after consultation with the heads of the relevant Federal agencies, shall provide a comprehensive briefing to relevant congressional committees—

(A) assessing global issues, trends, and actors considered to be significant with respect to cybercrime;

(B) assessing, after consultation with private industry groups, civil society organizations, and other relevant domestic or multilateral organizations, which shall be selected by the President based on an interest in combating cybercrime, means of enhancing multilateral or bilateral efforts in areas of significance—

(i) to prevent and investigate cybercrime;

(ii) to develop and share best practices with respect to directly or indirectly combating cybercrime; and

(iii) to cooperate and take action with respect to the prevention, investigation, and prosecution of cybercrime; and

(C) describing the steps taken by the United States to promote the multilateral or bilateral efforts described in subparagraph (B).

(2) CONTRIBUTIONS FROM RELEVANT FEDERAL AGENCIES.—Not later than 30 days before the date on which the briefing is to be provided under paragraph (1), the head of each relevant Federal agency shall consult with and provide to the Secretary of State relevant information appropriate for the briefing.

(b) PERIODIC UPDATES.—The Secretary of State shall provide updated information highlighting significant developments relating to the issues described in subsection (a), through periodic briefings to Congress.

(c) USE OF FOREIGN ASSISTANCE PROGRAMS.—

(1) FOREIGN ASSISTANCE PROGRAMS TO COMBAT CYBERCRIME.—The Secretary of State is authorized to accord priority in foreign assistance to programs designed to combat cybercrime in a region

1 or program of significance in order to better combat
 2 cybercrime by, among other things, improving the
 3 effectiveness and capacity of the legal and judicial
 4 systems and the capabilities of law enforcement
 5 agencies with respect to cybercrime.

6 (2) SENSE OF THE CONGRESS WITH RESPECT
 7 TO BILATERAL AND MULTILATERAL ASSISTANCE.—

8 It is the sense of Congress that the Secretary of
 9 State should include programs designed to combat
 10 cybercrime in relevant bilateral or multilateral as-
 11 sistance programs administered or supported by the
 12 United States Government.

13 **TITLE VII—INFORMATION** 14 **SHARING**

15 **SEC. 701. AFFIRMATIVE AUTHORITY TO MONITOR AND DE-** 16 **FEND AGAINST CYBERSECURITY THREATS.**

17 (a) IN GENERAL.—Notwithstanding chapter 119,
 18 121, or 206 of title 18, United States Code, the Foreign
 19 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et
 20 seq.), and sections 222 and 705 of the Communications
 21 Act of 1934 (47 U.S.C. 222 and 605), any private entity
 22 may—

23 (1) monitor its information systems and infor-
 24 mation that is stored on, processed by, or transiting
 25 such information systems for—

1 (A) malicious reconnaissance;

2 (B) efforts to defeat a technical control or
3 an operational control;

4 (C) technical vulnerabilities;

5 (D) efforts to cause a user with legitimate
6 access to an information system or information
7 that is stored on, processed by, or transiting an
8 information system to unwittingly enable the
9 defeat of a technical control or an operational
10 control;

11 (E) malicious cyber command and control;

12 (F) information exfiltrated as a result of
13 defeating a technical control or an operational
14 control;

15 (G) any other attribute of a cybersecurity
16 threat, if monitoring for such attribute is not
17 otherwise prohibited by law; or

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

20 (2) operate countermeasures on its information
21 systems to protect its rights or property from cyber-
22 security threats;

23 (3) consent to another private entity monitoring
24 or operating countermeasures on its information sys-
25 tems and information that is stored on, processed

1 by, or transiting such information systems in accord-
2 ance with this section;

3 (4) monitor a third party's information systems
4 and information that is stored on, processed by, or
5 transiting such information systems for the informa-
6 tion listed in subparagraphs (A) through (H) of
7 paragraph (1), if—

8 (A) the third party provides express prior
9 consent to such monitoring; and

10 (B) such monitoring would be lawful under
11 paragraph (1) or under any other provision of
12 law if the third party were to perform such
13 monitoring of its own networks; and

14 (5) operate countermeasures on a third party's
15 information systems to protect the third party's
16 rights or property from cybersecurity threats, if—

17 (A) the third party provides express prior
18 consent to such countermeasures; and

19 (B) operating such countermeasures would
20 be lawful under paragraph (2) or under any
21 other provision of law if the third party were to
22 operate such countermeasures on its own infor-
23 mation systems to protect its own rights or
24 property.

1 (b) USE AND PROTECTION OF INFORMATION.—A pri-
2 vate entity performing monitoring or operating counter-
3 measures under subsection (a)—

4 (1) may use cybersecurity threat indicators ac-
5 quired under this title, provided such use is solely
6 for the purpose of protecting an information system
7 or information that is stored on, processed by, or
8 transiting an information system from cybersecurity
9 threats or mitigating such threats;

10 (2) shall make reasonable efforts to safeguard
11 communications, records, system traffic, or other in-
12 formation that may be used to identify specific per-
13 sons acquired in the course of such monitoring from
14 unauthorized access or acquisition;

15 (3) shall comply with any lawful restrictions
16 placed on the use of cybersecurity threat indicators,
17 including, if requested, the removal or destruction of
18 information that can be used to identify specific per-
19 sons from such indicators;

20 (4) may not use cybersecurity threat indicators
21 to gain an unfair competitive advantage to the det-
22 riment of the entity that authorized such monitoring
23 or operation of countermeasures; and

24 (5) may use information obtained under any
25 other provision of law.

1 **SEC. 702. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
2 **THREAT INDICATORS AMONG PRIVATE ENTI-**
3 **TIES.**

4 (a) **AUTHORITY TO DISCLOSE.**—Notwithstanding any
5 other provision of law, any private entity may disclose law-
6 fully obtained cybersecurity threat indicators to any other
7 private entity in accordance with this section.

8 (b) **USE AND PROTECTION OF INFORMATION.**—A pri-
9 vate entity disclosing or receiving cybersecurity threat in-
10 dicators pursuant to subsection (a)—

11 (1) may use, retain, or further disclose such cy-
12 bersecurity threat indicators solely for the purpose
13 of protecting an information system or information
14 that is stored on, processed by, or transiting an in-
15 formation system from cybersecurity threats or miti-
16 gating such threats;

17 (2) shall make reasonable efforts to safeguard
18 communications, records, system traffic, or other in-
19 formation that can be used to identify specific per-
20 sons from unauthorized access or acquisition;

21 (3) shall comply with any lawful restrictions
22 placed on the disclosure or use of cybersecurity
23 threat indicators, including, if requested, the re-
24 moval of information that may be used to identify
25 specific persons from such indicators; and

1 (4) may not use the cybersecurity threat indica-
 2 tors to gain an unfair competitive advantage to the
 3 detriment of the entity that authorized such sharing.

4 (c) TRANSFERS TO UNRELIABLE PRIVATE ENTITIES
 5 PROHIBITED.—A private entity may not disclose cyberse-
 6 curity threat indicators to another private entity that the
 7 disclosing entity knows—

8 (1) has intentionally or willfully violated the re-
 9 quirements of subsection (b); and

10 (2) is reasonably likely to violate such require-
 11 ments.

12 **SEC. 703. CYBERSECURITY EXCHANGES.**

13 (a) DESIGNATION OF CYBERSECURITY EX-
 14 CHANGES.—The Secretary of Homeland Security, in con-
 15 sultation with the Director of National Intelligence, the
 16 Attorney General, and the Secretary of Defense, shall es-
 17 tablish—

18 (1) a process for designating one or more ap-
 19 propriate civilian Federal entities or non-Federal en-
 20 tities to serve as cybersecurity exchanges to receive
 21 and distribute cybersecurity threat indicators;

22 (2) procedures to facilitate and ensure the shar-
 23 ing of classified and unclassified cybersecurity threat
 24 indicators in as close to real time as possible with

1 appropriate Federal entities and non-Federal entities
2 in accordance with this title; and

3 (3) a process for identifying certified entities to
4 receive classified cybersecurity threat indicators in
5 accordance with paragraph (2).

6 (b) PURPOSE.—The purpose of a cybersecurity ex-
7 change is to receive and distribute, in as close to real time
8 as possible, cybersecurity threat indicators, and to thereby
9 avoid unnecessary and duplicative Federal bureaucracy for
10 information sharing as provided in this title.

11 (c) REQUIREMENT FOR A LEAD FEDERAL CIVILIAN
12 CYBERSECURITY EXCHANGE.—

13 (1) IN GENERAL.—The Secretary, in consulta-
14 tion with the Director of National Intelligence, the
15 Attorney General, and the Secretary of Defense,
16 shall designate a civilian Federal entity as the lead
17 cybersecurity exchange to serve as a focal point
18 within the Federal Government for cybersecurity in-
19 formation sharing among Federal entities and with
20 non-Federal entities.

21 (2) RESPONSIBILITIES.—The lead Federal civil-
22 ian cybersecurity exchange designated under para-
23 graph (1) shall—

1 (A) receive and distribute, in as close to
2 real time as possible, cybersecurity threat indi-
3 cators in accordance with this title;

4 (B) facilitate information sharing, inter-
5 action, and collaboration among and between—

6 (i) Federal entities;

7 (ii) State, local, tribal, and territorial
8 governments;

9 (iii) private entities;

10 (iv) academia;

11 (v) international partners, in consulta-
12 tion with the Secretary of State; and

13 (vi) other cybersecurity exchanges;

14 (C) disseminate timely and actionable cy-
15 bersecurity threat, vulnerability, mitigation, and
16 warning information lawfully obtained from any
17 source, including alerts, advisories, indicators,
18 signatures, and mitigation and response meas-
19 ures, to appropriate Federal and non-Federal
20 entities in as close to real time as possible, to
21 improve the security and protection of informa-
22 tion systems;

23 (D) coordinate with other Federal and
24 non-Federal entities, as appropriate, to inte-
25 grate information from Federal and non-Fed-

1 eral entities, including Federal cybersecurity
2 centers, non-Federal network or security oper-
3 ation centers, other cybersecurity exchanges,
4 and non-Federal entities that disclose cyberse-
5 curity threat indicators under section 704(a), in
6 as close to real time as possible, to provide situ-
7 ational awareness of the United States informa-
8 tion security posture and foster information se-
9 curity collaboration among information system
10 owners and operators;

11 (E) conduct, in consultation with private
12 entities and relevant Federal and other govern-
13 mental entities, regular assessments of existing
14 and proposed information sharing models to
15 eliminate bureaucratic obstacles to information
16 sharing and identify best practices for such
17 sharing; and

18 (F) coordinate with other Federal entities,
19 as appropriate, to compile and analyze informa-
20 tion about risks and incidents that threaten in-
21 formation systems, including information volun-
22 tarily submitted in accordance with section
23 704(a) or otherwise in accordance with applica-
24 ble laws.

1 (3) SCHEDULE FOR DESIGNATION.—The des-
2 ignation of a lead Federal civilian cybersecurity ex-
3 change under paragraph (1) shall be made concu-
4 rently with the issuance of the interim policies and
5 procedures under section 704(g)(3)(D).

6 (d) ADDITIONAL CIVILIAN FEDERAL CYBERSECU-
7 RITY EXCHANGES.—In accordance with the process and
8 procedures established in subsection (a), the Secretary, in
9 consultation with the Director of National Intelligence, the
10 Attorney General, and the Secretary of Defense, may des-
11 ignate additional civilian Federal entities to receive and
12 distribute cybersecurity threat indicators, if such entities
13 are subject to the requirements for use, retention, and dis-
14 closure of information by a cybersecurity exchange under
15 section 704(b) and the special requirements for Federal
16 entities under section 704(g).

17 (e) REQUIREMENTS FOR NON-FEDERAL CYBERSECU-
18 RITY EXCHANGES.—

19 (1) IN GENERAL.—In considering whether to
20 designate a private entity or any other non-Federal
21 entity as a cybersecurity exchange to receive and dis-
22 tribute cybersecurity threat indicators under section
23 704, and what entity to designate, the Secretary
24 shall consider the following factors:

1 (A) The net effect that such designation
2 would have on the overall cybersecurity of the
3 United States.

4 (B) Whether such designation could sub-
5 stantially improve such overall cybersecurity by
6 serving as a hub for receiving and sharing cy-
7 bersecurity threat indicators in as close to real
8 time as possible, including the capacity of the
9 non-Federal entity for performing those func-
10 tions.

11 (C) The capacity of such non-Federal enti-
12 ty to safeguard cybersecurity threat indicators
13 from unauthorized disclosure and use.

14 (D) The adequacy of the policies and pro-
15 cedures of such non-Federal entity to protect
16 personally identifiable information from unau-
17 thorized disclosure and use.

18 (E) The ability of the non-Federal entity
19 to sustain operations using entirely non-Federal
20 sources of funding.

21 (2) REGULATIONS.—The Secretary may pro-
22 mulgate regulations as may be necessary to carry
23 out this subsection.

24 (f) CONSTRUCTION WITH OTHER AUTHORITIES.—
25 Nothing in this section may be construed to alter the au-

1 thorities of a Federal cybersecurity center, unless such cy-
 2 bersecurity center is acting in its capacity as a designated
 3 cybersecurity exchange.

4 (g) CONGRESSIONAL NOTIFICATION OF DESIGNA-
 5 TION OF CYBERSECURITY EXCHANGES.—

6 (1) IN GENERAL.—The Secretary, in coordina-
 7 tion with the Director of National Intelligence, the
 8 Attorney General, and the Secretary of Defense,
 9 shall promptly notify Congress, in writing, of any
 10 designation of a cybersecurity exchange under this
 11 title.

12 (2) REQUIREMENT.—Written notification under
 13 paragraph (1) shall include a description of the cri-
 14 teria and processes used to make the designation.

15 **SEC. 704. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
 16 **THREAT INDICATORS TO A CYBERSECURITY**
 17 **EXCHANGE.**

18 (a) AUTHORITY TO DISCLOSE.—Notwithstanding any
 19 other provision of law, a non-Federal entity may disclose
 20 lawfully obtained cybersecurity threat indicators to a cy-
 21 bersecurity exchange in accordance with this section.

22 (b) USE, RETENTION, AND DISCLOSURE OF INFOR-
 23 MATION BY A CYBERSECURITY EXCHANGE.—A cybersecu-
 24 rity exchange may only use, retain, or further disclose in-
 25 formation provided pursuant to subsection (a)—

1 (1) in order to protect information systems
2 from cybersecurity threats and to mitigate cyberse-
3 curity threats; or

4 (2) to law enforcement pursuant to subsection
5 (g)(2).

6 (c) USE AND PROTECTION OF INFORMATION RE-
7 CEIVED FROM A CYBERSECURITY EXCHANGE.—A non-
8 Federal entity receiving cybersecurity threat indicators
9 from a cybersecurity exchange—

10 (1) may use, retain, or further disclose such cy-
11 bersecurity threat indicators solely for the purpose
12 of protecting an information system or information
13 that is stored on, processed by, or transiting an in-
14 formation system from cybersecurity threats or miti-
15 gating such threats;

16 (2) shall make reasonable efforts to safeguard
17 communications, records, system traffic, or other in-
18 formation that can be used to identify specific per-
19 sons from unauthorized access or acquisition;

20 (3) shall comply with any lawful restrictions
21 placed on the disclosure or use of cybersecurity
22 threat indicators by the cybersecurity exchange or a
23 third party, if the cybersecurity exchange received
24 such information from the third party, including, if
25 requested, the removal of information that can be

1 used to identify specific persons from such indica-
2 tors; and

3 (4) may not use the cybersecurity threat indica-
4 tors to gain an unfair competitive advantage to the
5 detriment of the third party that authorized such
6 sharing.

7 (d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any
8 cybersecurity threat indicator disclosed by a non-Federal
9 entity to a cybersecurity exchange pursuant to subsection
10 (a) shall be—

11 (1) exempt from disclosure under section
12 552(b)(3) of title 5, United States Code, or any
13 comparable State law; and

14 (2) treated as voluntarily shared information
15 under section 552 of title 5, United States Code, or
16 any comparable State law.

17 (e) EXEMPTION FROM EX PARTE LIMITATIONS.—
18 Any cybersecurity threat indicator disclosed by a non-Fed-
19 eral entity to a cybersecurity exchange pursuant to sub-
20 section (a) shall not be subject to the rules of any govern-
21 mental entity or judicial doctrine regarding ex parte com-
22 munications with a decision making official.

23 (f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any
24 cybersecurity threat indicator disclosed by a non-Federal
25 entity to a cybersecurity exchange pursuant to subsection

1 (a) may not be construed to be a waiver of any applicable
 2 privilege or protection provided under Federal, State, trib-
 3 al, or territorial law, including any trade secret protection.

4 (g) SPECIAL REQUIREMENTS FOR FEDERAL AND
 5 LAW ENFORCEMENT ENTITIES.—

6 (1) RECEIPT, DISCLOSURE AND USE OF CYBER-
 7 SECURITY THREAT INDICATORS BY A FEDERAL EN-
 8 TITY.—

9 (A) AUTHORITY TO RECEIVE AND USE CY-
 10 BERSECURITY THREAT INDICATORS.—A Fed-
 11 eral entity that is not a cybersecurity exchange
 12 may receive, retain, and use cybersecurity
 13 threat indicators from a cybersecurity exchange
 14 in order—

15 (i) to protect information systems
 16 from cybersecurity threats and to mitigate
 17 cybersecurity threats; and

18 (ii) to disclose such cybersecurity
 19 threat indicators to law enforcement in ac-
 20 cordance with paragraph (2).

21 (B) AUTHORITY TO DISCLOSE CYBERSECU-
 22 RITY THREAT INDICATORS.—A Federal entity
 23 that is not a cybersecurity exchange shall en-
 24 sure that if disclosing cybersecurity threat indi-
 25 cators to a non-Federal entity under this sec-

tion, such non-Federal entity shall use or retain such cybersecurity threat indicators in a manner that is consistent with the requirements in—

(i) subsection (b) on the use and protection of information; and

(ii) paragraph (2).

(2) LAW ENFORCEMENT ACCESS AND USE OF CYBERSECURITY THREAT INDICATORS.—

(A) DISCLOSURE TO LAW ENFORCEMENT.—A Federal entity may disclose cybersecurity threat indicators received under this title to a law enforcement entity if—

(i) the disclosure is permitted under the procedures developed by the Secretary and approved by the Attorney General under paragraph (3); and

(ii) the information appears to pertain—

(I) to a cybersecurity crime which has been, is being, or is about to be committed;

(II) to an imminent threat of death or serious bodily harm; or

1 (III) to a serious threat to mi-
2 nors, including sexual exploitation and
3 threats to physical safety.

4 (B) USE BY LAW ENFORCEMENT.—A law
5 enforcement entity may only use cybersecurity
6 threat indicators received by a Federal entity
7 under paragraph (A) in order—

8 (i) to protect information systems
9 from a cybersecurity threat or investigate,
10 prosecute, or disrupt a cybersecurity crime;

11 (ii) to protect individuals from an im-
12 minent threat of death or serious bodily
13 harm; or

14 (iii) to protect minors from any seri-
15 ous threat, including sexual exploitation
16 and threats to physical safety.

17 (3) PRIVACY AND CIVIL LIBERTIES.—

18 (A) REQUIREMENT FOR POLICIES AND
19 PROCEDURES.—The Secretary, in consultation
20 with privacy and civil liberties experts, the Di-
21 rector of National Intelligence, and the Sec-
22 retary of Defense, shall develop and periodically
23 review policies and procedures governing the re-
24 ceipt, retention, use, and disclosure of cyberse-
25 curity threat indicators by a Federal entity ob-

1 tained in connection with activities authorized
2 in this title. Such policies and procedures
3 shall—

4 (i) minimize the impact on privacy
5 and civil liberties, consistent with the need
6 to protect information systems from cyber-
7 security threats and mitigate cybersecurity
8 threats;

9 (ii) reasonably limit the receipt, reten-
10 tion, use and disclosure of cybersecurity
11 threat indicators associated with specific
12 persons consistent with the need to carry
13 out the responsibilities of this title, includ-
14 ing establishing a process for the timely
15 destruction of cybersecurity threat indica-
16 tors that are received pursuant to this sec-
17 tion that do not reasonably appear to be
18 related to the purposes identified in para-
19 graph (1)(A);

20 (iii) include requirements to safeguard
21 cybersecurity threat indicators that may be
22 used to identify specific persons from un-
23 authorized access or acquisition;

24 (iv) include procedures for notifying
25 entities, as appropriate, if information re-

1 ceived pursuant to this section is not a cy-
2 bersecurity threat indicator; and

3 (v) protect the confidentiality of cy-
4 bersecurity threat indicators associated
5 with specific persons to the greatest extent
6 practicable and require recipients to be in-
7 formed that such indicators may only be
8 used for the purposes identified in para-
9 graph (1)(A).

10 (B) ADOPTION OF POLICIES AND PROCE-
11 DURES.—The head of an agency responsible for
12 a Federal entity designated as a cybersecurity
13 exchange under section 703 shall adopt and
14 comply with the policies and procedures devel-
15 oped under this paragraph.

16 (C) REVIEW BY THE ATTORNEY GEN-
17 ERAL.—The policies and procedures developed
18 under this subsection shall be provided to the
19 Attorney General for review not later than 1
20 year after the date of the enactment of this
21 title, and shall not be issued without the Attor-
22 ney General’s approval.

23 (D) REQUIREMENT FOR INTERIM POLICIES
24 AND PROCEDURES.—The Secretary shall issue
25 interim policies and procedures not later than

1 60 days after the date of the enactment of this
2 title.

3 (E) PROVISION TO CONGRESS.—The poli-
4 cies and procedures issued under this title and
5 any amendments to such policies and proce-
6 dures shall be provided to Congress in an un-
7 classified form and be made public, but may in-
8 clude a classified annex.

9 (4) OVERSIGHT.—

10 (A) REQUIREMENT FOR OVERSIGHT.—The
11 Secretary and the Attorney General shall estab-
12 lish a mandatory program to monitor and over-
13 see compliance with the policies and procedures
14 issued under this subsection.

15 (B) NOTIFICATION OF THE ATTORNEY
16 GENERAL.—The head of each Federal entity
17 that receives information under this title
18 shall—

19 (i) comply with the policies and proce-
20 dures developed by the Secretary and ap-
21 proved by the Attorney General under
22 paragraph (3);

23 (ii) promptly notify the Attorney Gen-
24 eral of significant violations of such poli-
25 cies and procedures; and

1 (iii) provide to the Attorney General
2 any information relevant to the violation
3 that the Attorney General requires.

4 (C) ANNUAL REPORT.—On an annual
5 basis, the Chief Privacy and Civil Liberties Of-
6 ficer of the Department of Justice and the
7 Chief Privacy Officer of the Department, in
8 consultation with the most senior privacy and
9 civil liberties officer or officers of any appro-
10 priate agencies, shall jointly submit to Congress
11 a report assessing the privacy and civil liberties
12 impact of the governmental activities conducted
13 pursuant to this title.

14 (5) REPORTS ON INFORMATION SHARING.—

15 (A) PRIVACY AND CIVIL LIBERTIES OVER-
16 SIGHT BOARD REPORT.—Not later than 2 years
17 after the date of the enactment of this title, and
18 every 2 years thereafter, the Privacy and Civil
19 Liberties Oversight Board shall submit to Con-
20 gress and the President a report providing—

21 (i) an analysis of the practices of pri-
22 vate entities that are performing, moni-
23 toring, operating countermeasures, or dis-
24 closing cybersecurity threat indicators pur-
25 suant to this title;

1 (ii) an assessment of the privacy and
2 civil liberties impact of the activities car-
3 ried out by the Federal entities under this
4 title; and

5 (iii) recommendations for improve-
6 ments to or modifications of the law and
7 the policies and procedures established
8 pursuant to paragraph (3) in order to ad-
9 dress privacy and civil liberties concerns.

10 (B) INSPECTORS GENERAL ANNUAL RE-
11 PORT.—The Inspector General of the Depart-
12 ment, the Inspector General of the Intelligence
13 Community, the Inspector General of the De-
14 partment of Justice, and the Inspector General
15 of the Department of Defense shall, on an an-
16 nual basis, jointly submit to Congress a report
17 on the receipt, use and disclosure of informa-
18 tion shared with a Federal cybersecurity ex-
19 change under this title, including—

20 (i) a review of the use by Federal en-
21 tities of such information for a purpose
22 other than to protect information systems
23 from cybersecurity threats and to mitigate
24 cybersecurity threats, including law en-

1 enforcement access and use pursuant to
2 paragraph (2);

3 (ii) a review of the type of information
4 shared with a Federal cybersecurity ex-
5 change;

6 (iii) a review of the actions taken by
7 Federal entities based on such information;

8 (iv) appropriate metrics to determine
9 the impact of the sharing of such informa-
10 tion with a Federal cybersecurity exchange
11 on privacy and civil liberties;

12 (v) a list of Federal entities receiving
13 such information;

14 (vi) a review of the sharing of such in-
15 formation among Federal entities to iden-
16 tify inappropriate stovepiping of shared in-
17 formation; and

18 (vii) any recommendations of the in-
19 spectors general for improvements or modi-
20 fications to the authorities under this title.

21 (C) FORM.—Each report required under
22 this paragraph shall be submitted in unclassi-
23 fied form, but may include a classified annex.

24 (6) SANCTIONS.—The head of each Federal en-
25 tity that conducts activities under this title shall de-

1 velop and enforce appropriate sanctions for officers,
 2 employees, or agents of such entities who conducts
 3 such activities—

4 (A) outside the normal course of their
 5 specified duties;

6 (B) in a manner inconsistent with the dis-
 7 charge of the responsibilities of such entity; or

8 (C) in contravention of the requirements,
 9 policies, and procedures required by this sub-
 10 section.

11 (7) FEDERAL GOVERNMENT LIABILITY FOR
 12 VIOLATIONS OF THIS TITLE.—

13 (A) IN GENERAL.—If a Federal entity in-
 14 tentionally or willfully violates a provision of
 15 this title or a regulation promulgated under this
 16 title, the United States shall be liable to a per-
 17 son adversely affected by such violation in an
 18 amount equal to the sum of—

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

22 (ii) the costs of the action together
 23 with reasonable attorney fees as deter-
 24 mined by the court.

1 (B) VENUE.—An action to enforce liability
2 created under this subsection may be brought
3 in the district court of the United States in—

4 (i) the district in which the complain-
5 ant resides;

6 (ii) the district in which the principal
7 place of business of the complainant is lo-
8 cated;

9 (iii) the district in which the Federal
10 entity that disclosed the information is lo-
11 cated; or

12 (iv) the District of Columbia.

13 (C) STATUTE OF LIMITATIONS.—No action
14 shall lie under this subsection unless such ac-
15 tion is commenced not later than 2 years after
16 the date of the violation that is the basis for the
17 action.

18 (D) EXCLUSIVE CAUSE OF ACTION.—A
19 cause of action under this subsection shall be
20 the exclusive means available to a complainant
21 seeking a remedy for a disclosure of informa-
22 tion in violation of this title by a Federal entity.

1 **SEC. 705. SHARING OF CLASSIFIED CYBERSECURITY**
2 **THREAT INDICATORS.**

3 (a) SHARING OF CLASSIFIED CYBERSECURITY
4 THREAT INDICATORS.—The procedures established under
5 section 703(a)(2) shall provide that classified cybersecu-
6 rity threat indicators may only be—

7 (1) shared with certified entities;

8 (2) shared in a manner that is consistent with
9 the need to protect the national security of the
10 United States;

11 (3) shared with a person with an appropriate
12 security clearance to receive such cybersecurity
13 threat indicators; and

14 (4) used by a certified entity in a manner that
15 protects such cybersecurity threat indicators from
16 unauthorized disclosure.

17 (b) REQUIREMENT FOR GUIDELINES.—Not later
18 than 60 days after the date of the enactment of this title,
19 the Director of National Intelligence shall issue guidelines
20 providing that appropriate Federal officials may, as the
21 Director considers necessary to carry out this title—

22 (1) grant a security clearance on a temporary
23 or permanent basis to an employee of a certified en-
24 tity;

1 (2) grant a security clearance on a temporary
2 or permanent basis to a certified entity and approval
3 to use appropriate facilities; or

4 (3) expedite the security clearance process for
5 such an employee or entity, if appropriate, in a man-
6 ner consistent with the need to protect the national
7 security of the United States.

8 (c) DISTRIBUTION OF PROCEDURES AND GUIDE-
9 LINES.—Following the establishment of the procedures
10 under section 703(a)(2) and the issuance of the guidelines
11 under subsection (b), the Secretary and the Director of
12 National Intelligence shall expeditiously distribute such
13 procedures and guidelines to—

14 (1) appropriate governmental entities and pri-
15 vate entities;

16 (2) the Committee on Armed Services, the
17 Committee on Commerce, Science, and Transpor-
18 tation, the Committee on Homeland Security and
19 Governmental Affairs, the Committee on the Judici-
20 ary, and the Select Committee on Intelligence of the
21 Senate; and

22 (3) the Committee on Armed Services, the
23 Committee on Energy and Commerce, the Com-
24 mittee on Homeland Security, the Committee on the

1 Judiciary, and the Permanent Select Committee on
2 Intelligence of the House of Representatives.

3 **SEC. 706. LIMITATION ON LIABILITY AND GOOD FAITH DE-**
4 **FENSE FOR CYBERSECURITY ACTIVITIES.**

5 (a) IN GENERAL.—No civil or criminal cause of ac-
6 tion shall lie or be maintained in any Federal or State
7 court against any entity acting as authorized by this title,
8 and any such action shall be dismissed promptly for activi-
9 ties authorized by this title consisting of—

10 (1) the cybersecurity monitoring activities au-
11 thorized by paragraph (1), (3) or (4) of section
12 701(a); or

13 (2) the voluntary disclosure of a lawfully ob-
14 tained cybersecurity threat indicator—

15 (A) to a cybersecurity exchange pursuant
16 to section 704(a);

17 (B) by a provider of cybersecurity services
18 to a customer of that provider;

19 (C) to a private entity or governmental en-
20 tity that provides or manages critical infra-
21 structure (as that term is used in section 1016
22 of the Critical Infrastructures Protection Act of
23 2001 (42 U.S.C. 5195c)); or

24 (D) to any other private entity under sec-
25 tion 702(a), if the cybersecurity threat indicator

1 is also disclosed within a reasonable time to a
2 cybersecurity exchange.

3 (b) GOOD FAITH DEFENSE.—If a civil or criminal
4 cause of action is not barred under subsection (a), a rea-
5 sonable good faith reliance that this title permitted the
6 conduct complained of is a complete defense against any
7 civil or criminal action brought under this title or any
8 other law.

9 (c) LIMITATION ON USE OF CYBERSECURITY
10 THREAT INDICATORS FOR REGULATORY ENFORCEMENT
11 ACTIONS.—No Federal entity may use a cybersecurity
12 threat indicator received pursuant to this title as evidence
13 in a regulatory enforcement action against the entity that
14 lawfully shared the cybersecurity threat indicator with a
15 cybersecurity exchange that is a Federal entity.

16 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
17 ENFORCEMENT, NATIONAL SECURITY, OR HOMELAND
18 SECURITY PURPOSES.—No civil or criminal cause of ac-
19 tion shall lie or be maintained in any Federal or State
20 court against any entity, and any such action shall be dis-
21 missed promptly, for a failure to disclose a cybersecurity
22 threat indicator if—

23 (1) the Attorney General or the Secretary de-
24 termines that disclosure of a cybersecurity threat in-
25 dicator would impede a civil or criminal investigation

1 and submits a written request to delay notification
2 for up to 30 days, except that the Attorney General
3 or the Secretary may, by a subsequent written re-
4 quest, revoke such delay or extend the period of time
5 set forth in the original request made under this
6 paragraph if further delay is necessary; or

7 (2) the Secretary, the Attorney General, or the
8 Director of National Intelligence determines that
9 disclosure of a cybersecurity threat indicator would
10 threaten national or homeland security and submits
11 a written request to delay notification, except that
12 the Secretary, the Attorney General, or the Director,
13 may, by a subsequent written request, revoke such
14 delay or extend the period of time set forth in the
15 original request made under this paragraph if fur-
16 ther delay is necessary.

17 (e) LIMITATION ON LIABILITY FOR FAILURE TO
18 ACT.—No civil or criminal cause of action shall lie or be
19 maintained in any Federal or State court against any pri-
20 vate entity, or any officer, employee, or agent of such an
21 entity, and any such action shall be dismissed promptly,
22 for the reasonable failure to act on information received
23 under this title.

24 (f) DEFENSE FOR BREACH OF CONTRACT.—Compli-
25 ance with lawful restrictions placed on the disclosure or

1 use of cybersecurity threat indicators is a complete defense
2 to any tort or breach of contract claim originating in a
3 failure to disclose cybersecurity threat indicators to a third
4 party.

5 (g) LIMITATION ON LIABILITY PROTECTIONS.—Any
6 person who, knowingly or acting in gross negligence, vio-
7 lates a provision of this title or a regulation promulgated
8 under this title shall—

9 (1) not receive the protections of this title; and

10 (2) be subject to any criminal or civil cause of
11 action that may arise under any other State or Fed-
12 eral law prohibiting the conduct in question.

13 **SEC. 707. CONSTRUCTION AND FEDERAL PREEMPTION.**

14 (a) CONSTRUCTION.—Nothing in this title may be
15 construed—

16 (1) to limit any other existing authority or law-
17 ful requirement to monitor information systems and
18 information that is stored on, processed by, or
19 transiting such information systems, operate coun-
20 termeasures, and retain, use or disclose lawfully ob-
21 tained information;

22 (2) to permit the unauthorized disclosure of—

23 (A) information that has been determined
24 by the Federal Government pursuant to an Ex-
25 ecutive order or statute to require protection

1 against unauthorized disclosure for reasons of
2 national defense or foreign relations;

3 (B) any restricted data (as that term is de-
4 fined in paragraph (y) of section 11 of the
5 Atomic Energy Act of 1954 (42 U.S.C. 2014));

6 (C) information related to intelligence
7 sources and methods; or

8 (D) information that is specifically subject
9 to a court order or a certification, directive, or
10 other authorization by the Attorney General
11 precluding such disclosure;

12 (3) to provide additional authority to, or modify
13 an existing authority of, the Department of Defense
14 or the National Security Agency or any other ele-
15 ment of the intelligence community to control, mod-
16 ify, require, or otherwise direct the cybersecurity ef-
17 forts of a non-Federal entity or a Federal entity;

18 (4) to limit or modify an existing information
19 sharing relationship;

20 (5) to prohibit a new information sharing rela-
21 tionship;

22 (6) to require a new information sharing rela-
23 tionship between a Federal entity and a private enti-
24 ty;

1 (7) to limit the ability of a non-Federal entity
2 or a Federal entity to receive data about its informa-
3 tion systems, including lawfully obtained cybersecu-
4 rity threat indicators;

5 (8) to authorize or prohibit any law enforce-
6 ment, homeland security, or intelligence activities
7 not otherwise authorized or prohibited under another
8 provision of law;

9 (9) to permit price-fixing, allocating a market
10 between competitors, monopolizing or attempting to
11 monopolize a market, boycotting, or exchanges of
12 price or cost information, customer lists, or informa-
13 tion regarding future competitive planning;

14 (10) to authorize or limit liability for actions
15 that would violate the regulations adopted by the
16 Federal Communications Commission on preserving
17 the open Internet, or any successor regulations
18 thereto, nor to modify or alter the obligations of pri-
19 vate entities under such regulations; or

20 (11) to prevent a governmental entity from
21 using information not acquired through a cybersecu-
22 rity exchange for regulatory purposes.

23 (b) FEDERAL PREEMPTION.—This title supersedes
24 any law or requirement of a State or political subdivision
25 of a State that restricts or otherwise expressly regulates

1 the provision of cybersecurity services or the acquisition,
2 interception, retention, use or disclosure of communica-
3 tions, records, or other information by private entities to
4 the extent such law contains requirements inconsistent
5 with this title.

6 (c) PRESERVATION OF OTHER STATE LAW.—Except
7 as expressly provided, nothing in this title shall be con-
8 strued to preempt the applicability of any other State law
9 or requirement.

10 (d) NO CREATION OF A RIGHT TO INFORMATION.—
11 The provision of information to a non-Federal entity
12 under this title does not create a right or benefit to similar
13 information by any other non-Federal entity.

14 (e) PROHIBITION ON REQUIREMENT TO PROVIDE IN-
15 FORMATION TO THE FEDERAL GOVERNMENT.—Nothing
16 in this title may be construed to permit a Federal entity—

17 (1) to require a non-Federal entity to share in-
18 formation with the Federal Government;

19 (2) to condition the disclosure of unclassified or
20 classified cybersecurity threat indicators pursuant to
21 this title with a non-Federal entity on the provision
22 of cybersecurity threat information to the Federal
23 Government; or

24 (3) to condition the award of any Federal
25 grant, contract or purchase on the provision of cy-

1 bersecurity threat indicators to a Federal entity, if
2 the provision of such indicators does not reasonably
3 relate to the nature of activities, goods, or services
4 covered by the award.

5 (f) LIMITATION ON USE OF INFORMATION.—No cy-
6 bersecurity threat indicators obtained pursuant to this
7 title may be used, retained, or disclosed by a Federal enti-
8 ty or non-Federal entity, except as authorized under this
9 title.

10 (g) DECLASSIFICATION AND SHARING OF INFORMA-
11 TION.—Consistent with the exemptions from public disclo-
12 sure of section 704(d), the Director of National Intel-
13 ligence, in consultation with the Secretary and the head
14 of the Federal entity in possession of the information,
15 shall facilitate the declassification and sharing of informa-
16 tion in the possession of a Federal entity that is related
17 to cybersecurity threats, as the Director deems appro-
18 priate.

19 (h) REPORT ON IMPLEMENTATION.—Not later than
20 2 years after the date of the enactment of this title, the
21 Secretary, the Director of National Intelligence, the Attor-
22 ney General, and the Secretary of Defense shall jointly
23 submit to Congress a report that—

24 (1) describes the extent to which the authorities
25 conferred by this title have enabled the Federal Gov-

1 ernment and the private sector to mitigate cyberse-
2 curity threats;

3 (2) discloses any significant acts of noncompli-
4 ance by a non-Federal entity with this title, with
5 special emphasis on privacy and civil liberties, and
6 any measures taken by the Federal Government to
7 uncover such noncompliance;

8 (3) describes in general terms the nature and
9 quantity of information disclosed and received by
10 governmental entities and private entities under this
11 title; and

12 (4) identifies the emergence of new threats or
13 technologies that challenge the adequacy of the law,
14 including the definitions, authorities and require-
15 ments of this title, for keeping pace with the threat.

16 (i) REQUIREMENT FOR ANNUAL REPORT.—On an
17 annual basis, the Director of National Intelligence shall
18 provide a report to the Select Committee on Intelligence
19 of the Senate and the Permanent Select Committee on In-
20 telligence of the House of Representatives on the imple-
21 mentation of section 705. Such report, which shall be sub-
22 mitted in a classified and in an unclassified form, shall
23 include a list of private entities that receive classified cy-
24 bersecurity threat indicators under this title, except that
25 the unclassified report shall not contain information that

1 may be used to identify specific private entities unless
2 such private entities consent to such identification.

3 **SEC. 708. DEFINITIONS.**

4 In this title:

5 (1) CERTIFIED ENTITY.—The term “certified
6 entity” means a protected entity, a self-protected en-
7 tity, or a provider of cybersecurity services that—

8 (A) possesses or is eligible to obtain a se-
9 curity clearance, as determined by the Director
10 of National Intelligence; and

11 (B) is able to demonstrate to the Director
12 of National Intelligence that such provider or
13 such entity can appropriately protect and use
14 classified cybersecurity threat indicators.

15 (2) COUNTERMEASURE.—The term “counter-
16 measure” means automated or manual actions to
17 modify, redirect, or block information that is stored
18 on, processed by, or transiting an information sys-
19 tem that is known or suspected to contain cybersecu-
20 rity threat indicators for the purpose of protecting
21 an information system from cybersecurity threats,
22 conducted on an information system owned or oper-
23 ated by or on behalf of the party to be protected or
24 operated by a private entity acting as a provider of
25 electronic communication services, remote computing

1 services, or cybersecurity services to the party to be
2 protected.

3 (3) CYBERSECURITY CRIME.—The term “cyber-
4 security crime” means the violation of a provision of
5 State or Federal law relating to computer crimes, in-
6 cluding a violation of any provision of title 18,
7 United States Code, enacted or amended by the
8 Computer Fraud and Abuse Act of 1986 (Public
9 Law 99–474; 100 Stat. 1213).

10 (4) CYBERSECURITY EXCHANGE.—The term
11 “cybersecurity exchange” means any governmental
12 entity or private entity designated by the Secretary
13 of Homeland Security, in consultation with the Di-
14 rector of National Intelligence, the Attorney Gen-
15 eral, and the Secretary of Defense, to receive and
16 distribute cybersecurity threat indicators under sec-
17 tion 703(a).

18 (5) CYBERSECURITY SERVICES.—The term “cy-
19 bersecurity services” means products, goods, or serv-
20 ices intended to detect, mitigate, or prevent cyberse-
21 curity threats.

22 (6) CYBERSECURITY THREAT.—The term “cy-
23 bersecurity threat” means any action that may re-
24 sult in unauthorized access to, exfiltration of, manip-
25 ulation of, harm of, or impairment to the integrity,

1 confidentiality, or availability of an information sys-
2 tem or information that is stored on, processed by,
3 or transiting an information system, except that
4 none of the following shall be considered a cyberse-
5 curity threat—

6 (A) actions protected by the first amend-
7 ment to the Constitution of the United States;
8 and

9 (B) exceeding authorized access of an in-
10 formation system, if such access solely involves
11 a violation of consumer terms of service or con-
12 sumer licensing agreements.

13 (7) CYBERSECURITY THREAT INDICATOR.—The
14 term “cybersecurity threat indicator” means infor-
15 mation—

16 (A) that is reasonably necessary to de-
17 scribe—

18 (i) malicious reconnaissance, including
19 anomalous patterns of communications
20 that reasonably appear to be transmitted
21 for the purpose of gathering technical in-
22 formation related to a cybersecurity threat;

23 (ii) a method of defeating a technical
24 control;

25 (iii) a technical vulnerability;

1 (iv) a method of defeating an oper-
2 ational control;

3 (v) a method of causing a user with
4 legitimate access to an information system
5 or information that is stored on, processed
6 by, or transiting an information system to
7 unwittingly enable the defeat of a technical
8 control or an operational control;

9 (vi) malicious cyber command and
10 control;

11 (vii) the actual or potential harm
12 caused by an incident, including informa-
13 tion exfiltrated as a result of defeating a
14 technical control or an operational control
15 when it is necessary in order to identify or
16 describe a cybersecurity threat;

17 (viii) any other attribute of a cyberse-
18 curity threat, if disclosure of such attribute
19 is not otherwise prohibited by law; or

20 (ix) any combination thereof; and

21 (B) from which reasonable efforts have
22 been made to remove information that can be
23 used to identify specific persons unrelated to
24 the cybersecurity threat.

1 (8) FEDERAL CYBERSECURITY CENTER.—The
2 term “Federal cybersecurity center” means the De-
3 partment of Defense Cyber Crime Center, the Intel-
4 ligence Community Incident Response Center, the
5 United States Cyber Command Joint Operations
6 Center, the National Cyber Investigative Joint Task
7 Force, the National Security Agency/Central Secu-
8 rity Service Threat Operations Center, the United
9 States Computer Emergency Readiness Team, or
10 successors to such centers.

11 (9) FEDERAL ENTITY.—The term “Federal en-
12 tity” means an agency or department of the United
13 States, or any component, officer, employee, or
14 agent of such an agency or department.

15 (10) GOVERNMENTAL ENTITY.—The term “gov-
16 ernmental entity” means any Federal entity and
17 agency or department of a State, local, tribal, or ter-
18 ritorial government other than an educational insti-
19 tution, or any component, officer, employee, or agent
20 of such an agency or department.

21 (11) INFORMATION SYSTEM.—The term “infor-
22 mation system” means a discrete set of information
23 resources organized for the collection, processing,
24 maintenance, use, sharing, dissemination, or disposi-
25 tion of information, including communications with,

1 or commands to, specialized systems such as indus-
2 trial and process control systems, telephone switch-
3 ing and private branch exchanges, and environ-
4 mental control systems.

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

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

19 (14) MONITOR.—The term “monitor” means
20 the interception, acquisition, or collection of informa-
21 tion that is stored on, processed by, or transiting an
22 information system for the purpose of identifying cy-
23 bersecurity threats.

1 (15) NON-FEDERAL ENTITY.—The term “non-
2 Federal entity” means a private entity or a govern-
3 mental entity other than a Federal entity.

4 (16) OPERATIONAL CONTROL.—The term
5 “operational control” means a security control for
6 an information system that primarily is implemented
7 and executed by people.

8 (17) PRIVATE ENTITY.—The term “private en-
9 tity” has the meaning given the term “person” in
10 section 1 of title 1, United States Code, and does
11 not include a governmental entity.

12 (18) PROTECT.—The term “protect” means ac-
13 tions undertaken to secure, defend, or reduce the
14 vulnerabilities of an information system, mitigate cy-
15 bersecurity threats, or otherwise enhance informa-
16 tion security or the resiliency of information systems
17 or assets.

18 (19) TECHNICAL CONTROL.—The term “tech-
19 nical control” means a hardware or software restric-
20 tion on, or audit of, access or use of an information
21 system or information that is stored on, processed
22 by, or transiting an information system that is in-
23 tended to ensure the confidentiality, integrity, or
24 availability of that system.

1 (20) TECHNICAL VULNERABILITY.—The term
2 “technical vulnerability” means any attribute of
3 hardware or software that could enable or facilitate
4 the defeat of a technical control.

5 (21) THIRD PARTY.—The term “third party”
6 includes Federal entities and non-Federal entities.

Calendar No. 470

112TH CONGRESS
2D Session

S. 3414

A BILL

To enhance the security and resiliency of the cyber
and communications infrastructure of the United
States.

JULY 23, 2012

Read the second time and placed on the calendar