

Calendar No. 323

112TH CONGRESS
2D SESSION**S. 2105**

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

IN THE SENATE OF THE UNITED STATES

FEBRUARY 14, 2012

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

FEBRUARY 15, 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”.

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—PROTECTING CRITICAL INFRASTRUCTURE

- Sec. 101. Definitions and responsibilities.
- Sec. 102. Sector-by-sector cyber risk assessments.
- Sec. 103. Procedure for designation of covered critical infrastructure.
- Sec. 104. Sector-by-sector risk-based cybersecurity performance requirements.
- Sec. 105. Security of covered critical infrastructure.
- Sec. 106. Sector-specific agencies.
- Sec. 107. Protection of information.
- Sec. 108. Voluntary technical assistance.
- Sec. 109. Emergency planning.
- Sec. 110. International cooperation.
- Sec. 111. Effect on other laws.

TITLE II—PROTECTING GOVERNMENT NETWORKS

- Sec. 201. FISMA Reform.
- Sec. 202. Management of information technology.
- Sec. 203. Savings provisions.

TITLE III—CLARIFYING AND STRENGTHENING EXISTING ROLES AND AUTHORITIES

- Sec. 301. Consolidation of existing departmental cyber resources and authorities.

TITLE IV—EDUCATION, RECRUITMENT, AND WORKFORCE DEVELOPMENT

- Sec. 401. Definitions.
- Sec. 402. National education and awareness campaign.
- 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.
- Sec. 408. Cybersecurity incentives.

TITLE V—RESEARCH AND DEVELOPMENT

- Sec. 501. Federal cybersecurity research and development.
- Sec. 502. Homeland security cybersecurity research and development.

TITLE VI—FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

- Sec. 601. Federal acquisition risk management strategy.
- Sec. 602. Amendments to Clinger-Cohen provisions to enhance agency planning for information security needs.

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; Federal preemption.
- Sec. 708. Definitions.

TITLE VIII—PUBLIC AWARENESS REPORTS

- Sec. 801. Findings.
- Sec. 802. Report on cyber incidents against Government networks.
- Sec. 803. Reports on prosecution for cybercrime.
- Sec. 804. Report on research relating to secure domain.
- Sec. 805. Report on preparedness of Federal courts to promote cybersecurity.
- Sec. 806. Report on impediments to public awareness.
- Sec. 807. Report on protecting the electrical grid of the United States.

TITLE IX—INTERNATIONAL COOPERATION

- Sec. 901. Definitions.
- Sec. 902. Findings.
- Sec. 903. Sense of Congress.
- Sec. 904. Coordination of international cyber issues within the United States Government.
- Sec. 905. Consideration of cybercrime in foreign policy and foreign assistance programs.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **COMMERCIAL INFORMATION TECHNOLOGY**
 4 **PRODUCT.**—The term “commercial information tech-
 5 nology product” means a commercial item that orga-
 6 nizes or communicates information electronically.

7 (2) **COMMERCIAL ITEM.**—The term “commer-
 8 cial item” has the meaning given the term in section
 9 103 of title 41, United States Code.

10 (3) **COVERED CRITICAL INFRASTRUCTURE.**—
 11 The term “covered critical infrastructure” means a
 12 system or asset designated by the Secretary as cov-

1 ered critical infrastructure in accordance with the
2 procedure established under section 103.

3 (4) COVERED SYSTEM OR ASSET.—The term
4 “covered system or asset” means a system or asset
5 of covered critical infrastructure.

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

10 (6) DEPARTMENT.—The term “Department”
11 means the Department of Homeland Security.

12 (7) FEDERAL AGENCY.—The term “Federal
13 agency” has the meaning given the term “agency”
14 in section 3502 of title 44, United States Code.

15 (8) FEDERAL INFORMATION INFRASTRUC-
16 TURE.—The term “Federal information infrastruc-
17 ture”—

18 (A) means information and information
19 systems that are owned, operated, controlled, or
20 licensed for use by, or on behalf of, any Federal
21 agency, including information systems used or
22 operated by another entity on behalf of a Fed-
23 eral agency; and

24 (B) does not include—

25 (i) a national security system; or

1 (ii) information and information sys-
2 tems that are owned, operated, controlled,
3 or licensed for use by, or on behalf of, the
4 Department of Defense, a military depart-
5 ment, or another element of the intel-
6 ligence community.

7 (9) INCIDENT.—The term “incident” has the
8 meaning given that term in section 3552 of title 44,
9 United States Code, as added by section 201 of this
10 Act.

11 (10) INFORMATION INFRASTRUCTURE.—The
12 term “information infrastructure” means the under-
13 lying framework that information systems and assets
14 rely on to process, transmit, receive, or store infor-
15 mation electronically, including programmable elec-
16 tronic devices and communications networks and any
17 associated hardware, software, or data.

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

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

1 (13) INSTITUTION OF HIGHER EDUCATION.—

2 The term “institution of higher education” has the
3 meaning given that term in section 102 of the High-
4 er Education Act of 1965 (20 U.S.C. 1002).

5 (14) INTELLIGENCE COMMUNITY.—The term
6 “intelligence community” has the meaning given
7 that term under section 3(4) of the National Secu-
8 rity Act of 1947 (50 U.S.C. 401a(4)).

9 (15) NATIONAL INFORMATION INFRASTRUC-
10 TURE.—The term “national information infrastruc-
11 ture” means information and information systems—

12 (A) that are owned, operated, or con-
13 trolled, in whole or in part, within or from the
14 United States; and

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

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

21 (17) OWNER.—The term “owner”—

22 (A) means an entity that owns a covered
23 system or asset; and

24 (B) does not include a company contracted
25 by the owner to manage, run, or operate a cov-

1 ered system or asset, or to provide a specific in-
2 formation technology product or service that is
3 used or incorporated into a covered system or
4 asset.

5 (18) OPERATOR.—The term “operator”—

6 (A) means an entity that manages, runs,
7 or operates, in whole or in part, the day-to-day
8 operations of a covered system or asset; and

9 (B) may include the owner of a covered
10 system or asset.

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

13 **TITLE I—PROTECTING CRITICAL** 14 **INFRASTRUCTURE**

15 **SEC. 101. DEFINITIONS AND RESPONSIBILITIES.**

16 (a) DEFINITIONS.—In this title:

17 (1) CYBER RISK.—The term “cyber risk”
18 means any risk to information infrastructure, includ-
19 ing physical or personnel risks and security
20 vulnerabilities, that, if exploited or not mitigated,
21 could pose a significant risk of disruption to the op-
22 eration of information infrastructure essential to the
23 reliable operation of covered critical infrastructure.

24 (2) SECTOR-SPECIFIC AGENCY.—The term “sec-
25 tor-specific agency” means the relevant Federal

1 agency responsible for infrastructure protection ac-
2 tivities in a designated critical infrastructure sector
3 or key resources category under the National Infra-
4 structure Protection Plan, or any other appropriate
5 Federal agency identified by the President after the
6 date of enactment of this Act.

7 (b) RESPONSIBILITY OF OWNER.—It shall be the re-
8 sponsibility of an owner to comply with the requirements
9 of this Act.

10 **SEC. 102. SECTOR-BY-SECTOR CYBER RISK ASSESSMENTS.**

11 (a) IN GENERAL.—The Secretary, in consultation
12 with entities that own or operate critical infrastructure,
13 the Critical Infrastructure Partnership Advisory Council,
14 and appropriate Information Sharing and Analysis Orga-
15 nizations, and in coordination with the intelligence com-
16 munity, the Department of Defense, the Department of
17 Commerce, sector-specific agencies and other Federal
18 agencies with responsibilities for regulating the security
19 of entities that own or operate critical infrastructure
20 shall—

21 (1) not later than 90 days after the date of en-
22 actment of this Act, conduct a top-level assessment
23 of the cybersecurity threats, vulnerabilities, risks,
24 and probability of a catastrophic incident across all
25 critical infrastructure sectors to determine which

1 sectors pose the greatest immediate risk, in order to
2 guide the allocation of resources for the implementa-
3 tion of this Act; and

4 (2) beginning with the highest priority sectors
5 identified under paragraph (1), conduct, on an ongo-
6 ing, sector-by-sector basis, cyber risk assessments of
7 the critical infrastructure in a manner that—

8 (A) uses state-of-the art threat modeling,
9 simulation, and analysis techniques;

10 (B) incorporates, as appropriate, any exist-
11 ing similar risk assessments; and

12 (C) considers—

13 (i) the actual or assessed threat, in-
14 cluding consideration of adversary capabili-
15 ties and intent, intrusion techniques, pre-
16 paredness, target attractiveness, and deter-
17 rence capabilities;

18 (ii) the extent and likelihood of death,
19 injury, or serious adverse effects to human
20 health and safety caused by damage or un-
21 authorized access to critical infrastructure;

22 (iii) the threat to or impact on na-
23 tional security caused by damage or unau-
24 thorized access to critical infrastructure;

1 (iv) the extent to which damage or
2 unauthorized access to critical infrastruc-
3 ture will disrupt the reliable operation of
4 other critical infrastructure;

5 (v) the harm to the economy that
6 would result from damage or unauthorized
7 access to critical infrastructure;

8 (vi) the risk of national or regional
9 catastrophic damage within the United
10 States caused by damage or unauthorized
11 access to information infrastructure lo-
12 cated outside the United States;

13 (vii) the overall preparedness and re-
14 siliency of each sector against damage or
15 unauthorized access to critical infrastruc-
16 ture, including the effectiveness of market
17 forces at driving security innovation and
18 secure practices; and

19 (viii) any other risk-based security
20 factors appropriate and necessary to pro-
21 tect public health and safety, critical infra-
22 structure, or national and economic secu-
23 rity.

24 (b) INPUT OF OWNERS AND OPERATORS.—

25 (1) IN GENERAL.—The Secretary shall—

1 (A) establish a process under which enti-
2 ties that own or operate critical infrastructure
3 and other relevant private sector experts pro-
4 vide input into the risk assessments conducted
5 under this section; and

6 (B) seek and incorporate private sector ex-
7 pertise available through established public-pri-
8 vate partnerships, including the Critical Infra-
9 structure Partnership Advisory Council and ap-
10 propriate Information Sharing and Analysis Or-
11 ganizations.

12 (2) PROTECTION OF INFORMATION.—Any infor-
13 mation submitted as part of the process established
14 under paragraph (1) shall be protected in accord-
15 ance with section 107.

16 (c) METHODOLOGIES FOR ASSESSING INFORMATION
17 SECURITY RISK.—The Secretary and the Director of the
18 National Institute of Standards and Technology, in con-
19 sultation with entities that own or operate infra-
20 structure and relevant private sector and academic ex-
21 perts, shall—

22 (1) develop repeatable, qualitative, and quan-
23 titative methodologies for assessing information se-
24 curity risk; or

1 (2) use methodologies described in paragraph
2 (1) that are in existence on the date of enactment
3 of this Act and make the methodologies publicly
4 available.

5 (d) SUBMISSION OF RISK ASSESSMENTS.—The Sec-
6 retary shall submit each risk assessment conducted under
7 this section, in a classified or unclassified form as nec-
8 essary, to—

- 9 (1) the President;
10 (2) appropriate Federal agencies; and
11 (3) appropriate congressional committees.

12 **SEC. 103. PROCEDURE FOR DESIGNATION OF COVERED**
13 **CRITICAL INFRASTRUCTURE.**

14 (a) RESPONSIBILITY FOR DESIGNATION OF COVERED
15 CRITICAL INFRASTRUCTURE.—

16 (1) IN GENERAL.—The Secretary, in consulta-
17 tion with entities that own or operate critical infra-
18 structure, the Critical Infrastructure Partnership
19 Advisory Council, appropriate Information Sharing
20 and Analysis Organizations, and other appropriate
21 representatives of State and local governments, shall
22 establish a procedure for the designation of critical
23 infrastructure, on a sector-by-sector basis, as cov-
24 ered critical infrastructure for the purposes of this
25 Act.

1 (2) DUTIES.—In establishing the procedure
2 under paragraph (1), the Secretary shall—

3 (A) prioritize the efforts of the Depart-
4 ment based on the prioritization established
5 under section 102(a)(1);

6 (B) incorporate, to the extent practicable,
7 the input of entities that own or operate critical
8 infrastructure, the Critical Infrastructure Part-
9 nership Advisory Council, appropriate Informa-
10 tion Sharing and Analysis Organizations, and
11 other appropriate representatives of the private
12 sector and State and local governments;

13 (C) coordinate with the head of the sector-
14 specific agency with responsibility for critical
15 infrastructure and the head of any Federal
16 agency with responsibilities for regulating the
17 security of critical infrastructure;

18 (D) develop a mechanism for owners to
19 submit information to assist the Secretary in
20 making determinations under this section; and

21 (E) periodically, but not less often than
22 annually, review and update designations under
23 this section.

24 (b) DESIGNATION OF COVERED CRITICAL INFRA-
25 STRUCTURE.—

1 (1) GUIDELINES FOR DESIGNATION.—In designating covered critical infrastructure for the purposes of this Act, the Secretary shall—

2 (A) designate covered critical infrastructure on a sector-by-sector basis and at the system or asset level;

3 (B) inform owners of the criteria used to identify covered critical infrastructure;

4 (C) only designate a system or asset as covered critical infrastructure if damage or unauthorized access to that system or asset could reasonably result in—

5 (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause—

6 (I) a mass casualty event that includes an extraordinary number of fatalities; or

7 (II) mass evacuations with a prolonged absence;

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

1 (I) failure or substantial disruption
2 tion of a United States financial mar-
3 ket;

4 (II) incapacitation or sustained
5 disruption of a transportation system;
6 or

7 (III) other systemic, long-term
8 damage to the United States economy;
9 or

10 (iii) severe degradation of national se-
11 curity or national security capabilities, in-
12 cluding intelligence and defense functions;
13 and

14 (D) consider the sector-by-sector risk as-
15 sessments developed in accordance with section
16 102.

17 (2) LIMITATIONS.—The Secretary may not des-
18 ignate as covered critical infrastructure under this
19 section—

20 (A) a system or asset based solely on ac-
21 tivities protected by the first amendment to the
22 Constitution of the United States;

23 (B) an information technology product or
24 service based solely on a finding that the prod-

1 uct or service is capable of, or is actually, being
2 used in covered critical infrastructure;

3 (C) a commercial information technology
4 product, including hardware and software; or

5 (D) any service provided in support of a
6 product specified in subparagraph (C), includ-
7 ing installation services, maintenance services,
8 repair services, training services, and any other
9 services provided in support of the product.

10 (3) NOTIFICATION OF IDENTIFICATION OF SYS-
11 TEM OR ASSET.—Not later than 30 days after the
12 Secretary designates a system or asset as covered
13 critical infrastructure under this section, the Sec-
14 retary shall notify the owner of the system or asset
15 that was designated and the basis for the designa-
16 tion.

17 (4) SELF-DESIGNATION OF SYSTEM OR ASSET
18 AS COVERED CRITICAL INFRASTRUCTURE.—The
19 owner of a system or asset may request that the sys-
20 tem or asset be designated as covered critical infra-
21 structure under this section if the owner determines
22 that the system or asset meets the criteria for des-
23 ignation.

24 (5) SYSTEM OR ASSET NO LONGER COVERED
25 CRITICAL INFRASTRUCTURE.—

1 (A) IN GENERAL.—If the Secretary deter-
2 mines that any system or asset that was des-
3 ignated as covered critical infrastructure under
4 this section no longer constitutes covered crit-
5 ical infrastructure, the Secretary shall promptly
6 notify the owner of that system or asset of that
7 determination.

8 (B) SELF-DESIGNATION.—If an owner de-
9 termines that an asset or system previously
10 self-designated as covered critical infrastructure
11 under paragraph (4) no longer meets the cri-
12 teria for designation, the owner shall notify the
13 Secretary of this determination and submit to
14 the redress process under subsection (c).

15 (6) DEFINITION.—In this subsection, the term
16 “damage” has the meaning given that term in sec-
17 tion 1030(e) of title 18, United States Code.

18 (c) REDRESS.—

19 (1) IN GENERAL.—Subject to paragraphs (2)
20 and (3), the Secretary shall develop a mechanism,
21 consistent with subchapter II of chapter 5 of title 5,
22 United States Code, for an owner notified under
23 subsection (b)(3) or for an owner that self-des-
24 ignates under subsection (b)(4) to request that the
25 Secretary review—

1 (A) the designation of a system or asset as
2 covered critical infrastructure;

3 (B) the rejection of the self-designation of
4 an owner of a system or asset as covered crit-
5 ical infrastructure; or

6 (C) a determination under subsection
7 (b)(5)(B).

8 (2) APPEAL TO FEDERAL COURT.—A civil ac-
9 tion seeking judicial review of a final agency action
10 taken under the mechanism developed under para-
11 graph (1) shall be filed in the United States District
12 Court for the District of Columbia.

13 (3) COMPLIANCE.—An owner shall comply with
14 this title relating to covered critical infrastructure
15 until such time as the critical infrastructure is no
16 longer designated as covered critical infrastructure,
17 based on—

18 (A) an appeal under paragraph (1);

19 (B) a determination of the Secretary unre-
20 lated to an appeal; or

21 (C) a final judgment entered in a civil ac-
22 tion seeking judicial review brought in accord-
23 ance with paragraph (2).

1 **SEC. 104. SECTOR-BY-SECTOR RISK-BASED CYBERSECURITY**
2 **PERFORMANCE REQUIREMENTS.**

3 (a) **PURPOSE.**—The purpose of this section is to se-
4 cure the critical infrastructure of the Nation while pro-
5 moting and protecting private sector innovation in design
6 and development of technology for the global market for
7 commercial information technology products, including
8 hardware and software and related products and services.

9 (b) **PERFORMANCE REQUIREMENTS.**—The Secretary,
10 in consultation with owners and operators, the Critical In-
11 frastructure Partnership Advisory Council, and appro-
12 priate Information Sharing and Analysis Organizations,
13 and in coordination with the National Institute of Stand-
14 ards and Technology, the Director of the National Secu-
15 rity Agency, sector-specific agencies, appropriate rep-
16 resentatives from State and local governments, and other
17 Federal agencies with responsibilities for regulating the
18 security of covered critical infrastructure, shall identify or
19 develop, on a sector-by-sector basis, risk-based cybersecu-
20 rity performance requirements (referred to in this section
21 as “performance requirements”) that—

22 (1) require owners to remediate or mitigate
23 identified cyber risks and any associated con-
24 sequences identified under section 102(a) or other-
25 wise; and

1 (2) do not permit any Federal employee or
2 agency to—

3 (A) regulate commercial information tech-
4 nology products, including hardware and soft-
5 ware and related services, including installation
6 services, maintenance services, repair services,
7 training services, and any other services pro-
8 vided in support of the product;

9 (B) require commercial information tech-
10 nology products, including hardware and soft-
11 ware and related services, for use or non-use in
12 covered critical infrastructure; or

13 (C) regulate the design, development, man-
14 ufacturing, or attributes of commercial informa-
15 tion technology products, including hardware
16 and software and related services, for use or
17 non-use in covered critical infrastructure.

18 (c) LIMITATION.—If the Secretary determines that
19 there are regulations in effect on the date of enactment
20 of this Act that apply to covered critical infrastructure and
21 that address some or all of the risks identified under sec-
22 tion 102, the Secretary shall identify or develop perform-
23 ance requirements under this section only if the regula-
24 tions do not require an appropriate level of security.

1 (d) IDENTIFICATION AND DEVELOPMENT OF PER-
2 FORMANCE REQUIREMENTS.—In establishing the per-
3 formance requirements under this section, the Secretary
4 shall—

5 (1) establish a process for entities that own or
6 operate critical infrastructure, voluntary consensus
7 standards development organizations, representatives
8 of State and local government, and the private sec-
9 tor, including sector coordinating councils and ap-
10 propriate Information Sharing and Analysis Organi-
11 zations to propose performance requirements;

12 (2) identify existing industry practices, stand-
13 ards, and guidelines; and

14 (3) select and adopt performance requirements
15 submitted under paragraph (1) or identified under
16 paragraph (2) that satisfy other provisions of this
17 section.

18 (e) REQUIREMENT.—If the Secretary determines that
19 none of the performance requirements submitted or identi-
20 fied under paragraphs (1) and (2) of subsection (d) satisfy
21 the other provisions of this section, the Secretary shall,
22 in consultation with owners and operators, the Critical In-
23 frastructure Partnership Advisory Council, and appro-
24 priate Information Sharing and Analysis Organizations,
25 and in coordination with the National Institute of Stand-

1 ards and Technology, the Director of the National Secu-
2 rity Agency, sector-specific agencies, and other Federal
3 agencies with responsibilities for regulating the security
4 of covered critical infrastructure, develop satisfactory per-
5 formance requirements.

6 (f) EXEMPTION AUTHORITY.—

7 (1) IN GENERAL.—The President, in consulta-
8 tion with the Director of the Office of Management
9 and Budget, may exempt an appropriate part of cov-
10 ered critical infrastructure from the requirements of
11 this title if the President determines that a sector-
12 specific regulatory agency has sufficient specific re-
13 quirements and enforcement mechanisms to effec-
14 tively mitigate the risks identified under section 102.

15 (2) RECONSIDERATION.—The President may
16 reconsider any exemption under paragraph (1) as
17 appropriate.

18 (g) CONSIDERATION.—The Secretary, in establishing
19 performance requirements under this section, shall take
20 into consideration available resources and anticipated con-
21 sequences of a cyber attack.

22 **SEC. 105. SECURITY OF COVERED CRITICAL INFRASTRUC-**
23 **TURE.**

24 (a) IN GENERAL.—Not later than 1 year after the
25 date of enactment of this Act, the Secretary, in consulta-

1 tion with owners and operators, and the Critical Infra-
2 structure Partnership Advisory Council, and in coordina-
3 tion with sector-specific agencies and other Federal agen-
4 cies with responsibilities for regulating the security of cov-
5 ered critical infrastructure, shall promulgate regulations
6 to enhance the security of covered critical infrastructure
7 against cyber risks.

8 (b) RESPONSIBILITIES.—The regulations promul-
9 gated under this section shall establish procedures under
10 which—

11 (1) each owner—

12 (A) is regularly informed of cyber risk as-
13 sessments, identified cybersecurity threats, and
14 the risk-based security performance require-
15 ments appropriate to the sector of the owner es-
16 tablished under section 104;

17 (B) selects and implements the cybersecu-
18 rity measures the owner determines to be best
19 suited to satisfy the risk-based cybersecurity
20 performance requirements established under
21 section 104;

22 (C) develop or update continuity of oper-
23 ations and incident response plans; and

1 (D) shall report, consistent with the pro-
2 tections in section 107, significant cyber inci-
3 dents affecting covered critical infrastructure;

4 (2) the Secretary and each Federal agency with
5 responsibilities for regulating the security of covered
6 critical infrastructure, is notified of the security
7 measure or measures selected by an owner in accord-
8 ance with paragraph (1)(B); and

9 (3) the Secretary—

10 (A) identifies, in consultation with owners
11 and operators, cyber risks that are not capable
12 of effective remediation or mitigation using
13 available standards, industry practices or other
14 available security measures;

15 (B) provides owners the opportunity to de-
16 velop practices or security measures to reme-
17 diate or mitigate the cyber risks identified in
18 section 102 without the prior approval of the
19 Secretary and without affecting the compliance
20 of the covered critical infrastructure with the
21 requirements under this section;

22 (C) in accordance with applicable law relat-
23 ing to the protection of trade secrets, permits
24 owners and operators to report to the Secretary
25 the development of effective practices or secu-

1 rity measures to remediate or mitigate the
2 cyber risks identified under section 102; and

3 (D) shall develop, in conjunction with the
4 Secretary of Defense and the Director of Na-
5 tional Intelligence and in coordination with
6 owners and operators, a procedure for ensuring
7 that owners and operators are, to the maximum
8 extent practicable and consistent with the pro-
9 tection of sources and methods, informed of rel-
10 evant real-time threat information.

11 (c) ENFORCEMENT.—

12 (1) REQUIREMENTS.—The regulations promul-
13 gated under this section shall establish procedures
14 that—

15 (A) require each owner—

16 (i) to certify, on an annual basis, in
17 writing to the Secretary and the head of
18 the Federal agency with responsibilities for
19 regulating the security of the covered crit-
20 ical infrastructure whether the owner has
21 developed and effectively implemented se-
22 curity measures sufficient to satisfy the
23 risk-based security performance require-
24 ments established under section 104; or

1 (ii) to submit a third-party assess-
2 ment in accordance with subsection (d), on
3 an annual basis;

4 (B) provide for civil penalties for any per-
5 son who—

6 (i) violates this section; and

7 (ii) fails to remediate such violation in
8 an appropriate timeframe; and

9 (C) do not confer upon any person, except
10 the Federal agency with responsibilities for reg-
11 ulating the security of the covered critical infra-
12 structure and the Secretary, a right of action
13 against an owner or operator to enforce any
14 provision of this section.

15 (2) PROPOSED SECURITY MEASURES.—An
16 owner may select any security measures that satisfy
17 the risk-based security performance requirements es-
18 tablished under section 104.

19 (3) RECOMMENDED SECURITY MEASURES.—
20 Upon request from an owner or operator, the Sec-
21 retary may recommend a specific security measure
22 that the Secretary believes will satisfy the risk-based
23 security performance requirements established under
24 section 104.

1 (4) SECURITY AND PERFORMANCE-BASED EX-
2 EMPTIONS.—

3 (A) IN GENERAL.—The Secretary shall de-
4 velop a process for an owner to demonstrate
5 that—

6 (i) a covered system or asset is suffi-
7 ciently secured against the risks identified
8 in section 102; or

9 (ii) compliance with risk-based per-
10 formance requirements developed under
11 section 104 would not substantially im-
12 prove the security of the covered system or
13 asset.

14 (B) EXEMPTION AUTHORITY.—Upon a de-
15 termination by the Secretary that a covered sys-
16 tem or asset is sufficiently secured against the
17 risks identified in section 102, or that compli-
18 ance with risk based performance requirements
19 developed under section 104 would not substan-
20 tially improve the security of the system or
21 asset, the Secretary may not require the owner
22 to select or implement cybersecurity measures
23 or submit an annual certification or third party
24 assessment as required under this Act.

1 (C) REQUIREMENT.—The Secretary shall
2 require an owner that was exempted under sub-
3 paragraph (B) to demonstrate that the covered
4 system or asset of the owner is sufficiently se-
5 cured against the risks identified in section
6 102, or that compliance with risk based per-
7 formance requirements developed under section
8 104 would not substantially improve the secu-
9 rity of the system or asset—

10 (i) not less than once every 3 years; or

11 (ii) if the Secretary has reason to be-
12 lieve that the covered system or asset no
13 longer meets the exemption qualifications
14 under subparagraph (B).

15 (5) ENFORCEMENT ACTIONS.—An action to en-
16 force any regulation promulgated pursuant to this
17 section shall be initiated by—

18 (A) the Federal agency with responsibil-
19 ities for regulating the security of the covered
20 critical infrastructure, in consultation with the
21 Secretary; or

22 (B) the Secretary, when—

23 (i) the covered critical infrastructure
24 is not subject to regulation by another
25 Federal agency;

1 (ii) the head of the Federal agency
2 with responsibilities for regulating the se-
3 curity of the covered critical infrastructure
4 requests the Secretary take such action; or

5 (iii) the Federal agency with respon-
6 sibilities for regulating the security of the
7 covered critical infrastructure fails to ini-
8 tiate such action after a request by the
9 Secretary.

10 (d) ASSESSMENTS.—

11 (1) THIRD-PARTY ASSESSMENTS.—The regula-
12 tions promulgated under this section shall establish
13 procedures for third-party private entities to conduct
14 assessments that use reliable, repeatable, perform-
15 ance-based evaluations and metrics to—

16 (A) assess the implementation of the se-
17 lected security measures;

18 (B) assess the effectiveness of the security
19 measure or measures implemented by the owner
20 in satisfying the risk-based security perform-
21 ance requirements established under section
22 104;

23 (C) require that third party assessors—

24 (i) be certified by the Secretary, in
25 consultation with the head of any Federal

1 agency with responsibilities for regulating
2 the security of covered critical infrastruc-
3 ture, after completing a proficiency pro-
4 gram established by the Secretary in con-
5 sultation with owners and operators, the
6 Critical Infrastructure Partnership Advi-
7 sory Council, appropriate Information
8 Sharing and Analysis Organizations, and
9 in coordination with the Director of the
10 National Institute of Standards and Tech-
11 nology, and relevant Federal agencies;

12 (ii) undergo regular retraining and
13 certification;

14 (iii) provide the findings of the third
15 party assessors to the owners and opera-
16 tors; and

17 (iv) submit each independent assess-
18 ment to the owner, the Secretary, and to
19 the Federal agency with responsibilities for
20 regulating the security of the covered crit-
21 ical infrastructure.

22 (2) OTHER ASSESSMENTS.—The regulations
23 promulgated under this section shall establish proce-
24 dures under which the Secretary—

1 (A) may perform cybersecurity assessments
2 of selected covered critical infrastructure, in
3 consultation with relevant agencies, based on—

4 (i) the specific cyber risks affecting or
5 potentially affecting the information infra-
6 structure of the specific system or asset
7 constituting covered critical infrastructure;

8 (ii) any reliable intelligence or other
9 information indicating a cyber risk to the
10 information infrastructure of the specific
11 system or asset constituting covered crit-
12 ical infrastructure;

13 (iii) actual knowledge or reasonable
14 suspicion that an owner is not in compli-
15 ance with risk-based security performance
16 requirements established under section
17 104; or

18 (iv) such other risk-based factors as
19 identified by the Secretary; and

20 (B) may use the resources of any relevant
21 Federal agency with the concurrence of the
22 head of such agency;

23 (C) to the extent practicable uses govern-
24 ment and private sector information security
25 assessment programs that were in existence on

1 the date of enactment of this Act to conduct as-
2 sessments; and

3 (D) provides copies of any Federal Govern-
4 ment assessments to the owner of the covered
5 system or asset.

6 (3) ACCESS TO INFORMATION.—

7 (A) IN GENERAL.—For the purposes of an
8 assessment conducted under paragraph (1) or
9 (2), an owner or operator shall provide an as-
10 sessor any reasonable access necessary to com-
11 plete the assessment.

12 (B) PROTECTION OF INFORMATION.—In-
13 formation provided to the Secretary, the Sec-
14 retary’s designee, or any assessor during the
15 course of an assessment under this section shall
16 be protected from disclosure in accordance with
17 section 107.

18 (e) LIMITATIONS ON CIVIL LIABILITY.—

19 (1) IN GENERAL.—Except as provided in para-
20 graph (2), in any civil action for damages directly
21 caused by an incident related to a cyber risk identi-
22 fied under section 102, an owner or operator shall
23 not be liable for any punitive damages intended to
24 punish or deter if the owner or operator—

1 (A) has implemented security measures, or
2 a combination thereof, that satisfy the security
3 performance requirements established under
4 section 104;

5 (B) has undergone successful assessments,
6 submitted an annual certification or third party
7 assessment required by subsection (c)(1), or
8 been granted an exemption in accordance with
9 subsection (c)(4); and

10 (C) is in substantial compliance with the
11 appropriate risk based cybersecurity perform-
12 ance requirements at the time of the incident
13 related to that cyber risk.

14 (2) LIMITATION.—Paragraph (1) shall only
15 apply to harm directly caused by the incident related
16 to the cyber risk and shall not apply to damages
17 caused by any additional or intervening acts or omis-
18 sions by the owner or operator.

19 **SEC. 106. SECTOR-SPECIFIC AGENCIES.**

20 (a) IN GENERAL.—The head of each sector-specific
21 agency and the head of any Federal agency that is not
22 a sector-specific agency with responsibilities for regulating
23 the security of covered critical infrastructure shall coordi-
24 nate with the Secretary on any activities of the sector-
25 specific agency or Federal agency that relate to the efforts

1 of the agency regarding the cybersecurity and resiliency
2 to cyber attack of critical infrastructure and covered crit-
3 ical infrastructure, within or under the supervision of the
4 agency.

5 (b) DUPLICATIVE REPORTING REQUIREMENTS.—

6 (1) IN GENERAL.—The Secretary shall coordi-
7 nate with the head of each sector-specific agency and
8 the head of any Federal agency that is not a sector-
9 specific agency with responsibilities for regulating
10 the security of covered critical infrastructure to de-
11 termine whether reporting requirements in effect on
12 the date of enactment of this Act substantially fulfill
13 any reporting requirements described in this title.

14 (2) PRIOR REQUIRED REPORTS.—If the Sec-
15 retary determines that a report that was required
16 under a regulatory regime in existence on the date
17 of enactment of this Act substantially satisfies a re-
18 porting requirement under this title, the Secretary
19 shall use such report and may not require an owner
20 or operator to submit an additional report.

21 (3) COORDINATION.—The Secretary shall co-
22 ordinate with the head of each sector-specific agency
23 and the head of any Federal agency that is not a
24 sector-specific agency with responsibilities for regu-
25 lating the security of covered critical infrastructure

1 to eliminate any duplicate reporting or compliance
2 requirements relating to the security or resiliency of
3 critical infrastructure and covered critical infrastruc-
4 ture, within or under the supervision of the agency.

5 (c) REQUIREMENTS.—

6 (1) IN GENERAL.—To the extent that the head
7 of each sector-specific agency and the head of any
8 Federal agency that is not a sector-specific agency
9 with responsibilities for regulating the security of
10 covered critical infrastructure has the authority to
11 establish regulations, rules, or requirements or other
12 required actions that are applicable to the security
13 of critical infrastructure and covered critical infra-
14 structure, the head of the agency shall—

15 (A) notify the Secretary in a timely fashion
16 of the intent to establish the regulations, rules,
17 requirements, or other required actions;

18 (B) coordinate with the Secretary to en-
19 sure that the regulations, rules, requirements,
20 or other required actions are consistent with,
21 and do not conflict or impede, the activities of
22 the Secretary under this title; and

23 (C) in coordination with the Secretary, en-
24 sure that the regulations, rules, requirements,
25 or other required actions are implemented, as

1 they relate to covered critical infrastructure, in
2 accordance with subsection (a).

3 (2) **RULE OF CONSTRUCTION.**—Nothing in this
4 section shall be construed to provide additional au-
5 thority for any sector-specific agency or any Federal
6 agency that is not a sector-specific agency with re-
7 sponsibilities for regulating the security of critical
8 infrastructure or covered critical infrastructure to
9 establish standards or other measures that are appli-
10 cable to the security of critical infrastructure not
11 otherwise authorized by law.

12 **SEC. 107. PROTECTION OF INFORMATION.**

13 (a) **DEFINITION.**—In this section, the term “covered
14 information”—

15 (1) means—

16 (A) any information that constitutes a
17 privileged or confidential trade secret or com-
18 mercial or financial transaction that is appro-
19 priately marked at the time it is provided by
20 entities that own or operate critical infrastruc-
21 ture in sector-by-sector risk assessments con-
22 ducted under section 102;

23 (B) any information required to be sub-
24 mitted by owners and operators under section
25 105; and

1 (C) any information submitted by State
2 and local governments, private entities, and
3 international partners of the United States re-
4 garding threats, vulnerabilities, risks, and inci-
5 dents affecting—

6 (i) the Federal information infrastruc-
7 ture;

8 (ii) information infrastructure that is
9 owned, operated, controlled, or licensed for
10 use by, or on behalf of, the Department of
11 Defense, a military department, or another
12 element of the intelligence community; or

13 (iii) critical infrastructure; and

14 (2) does not include any information described
15 under paragraph (1), if that information is sub-
16 mitted to—

17 (A) conceal violations of law, inefficiency,
18 or administrative error;

19 (B) prevent embarrassment to a person,
20 organization, or agency; or

21 (C) interfere with competition in the pri-
22 vate sector.

23 (b) VOLUNTARILY SHARED CRITICAL INFRASTRUC-
24 TURE INFORMATION.—Covered information submitted in
25 accordance with this section shall be treated as voluntarily

1 shared critical infrastructure information under section
2 214 of the Homeland Security Act (6 U.S.C. 133), except
3 that the requirement of such section 214 that the informa-
4 tion be voluntarily submitted, including the requirement
5 for an express statement, shall not be required for protec-
6 tion of information under this section to apply.

7 (c) GUIDELINES.—

8 (1) IN GENERAL.—Subject to paragraph (2),
9 the Secretary shall develop and issue guidelines, in
10 consultation with the Attorney General and the Crit-
11 ical Infrastructure Partnership Advisory Council, ap-
12 propriate Information Sharing and Analysis Organi-
13 zations, as necessary to implement this section.

14 (2) REQUIREMENTS.—The guidelines developed
15 under this section shall—

16 (A) include provisions for the sharing of
17 information among governmental and non-
18 governmental officials and entities in further-
19 ance of carrying out the authorities and respon-
20 sibilities of the Secretary;

21 (B) be consistent, to the maximum extent
22 possible, with policy guidance and implementa-
23 tion standards developed by the National Ar-
24 chives and Records Administration for con-
25 trolled unclassified information, including with

1 respect to marking, safeguarding, dissemina-
2 tion, and dispute resolution; and

3 (C) describe, with as much detail as pos-
4 sible, the categories and type of information en-
5 tities should voluntarily submit.

6 (d) PROCESS FOR REPORTING SECURITY THREATS,
7 VULNERABILITIES, RISKS, AND INCIDENTS.—

8 (1) ESTABLISHMENT OF PROCESS.—The Sec-
9 retary shall establish through regulation, and pro-
10 vide information to the public regarding, a process
11 by which any person may submit a report to the
12 Secretary regarding cybersecurity threats,
13 vulnerabilities, risks, and incidents affecting—

14 (A) the Federal information infrastructure;

15 (B) information infrastructure that is
16 owned, operated, controlled, or licensed for use
17 by, or on behalf of, the Department of Defense,
18 a military department, or another element of
19 the intelligence community; or

20 (C) critical infrastructure.

21 (2) ACKNOWLEDGMENT OF RECEIPT.—If a re-
22 port submitted under paragraph (1) includes the
23 identity of the person making the report, the Sec-
24 retary shall respond promptly to the person and ac-
25 knowledge receipt of the report.

1 (3) STEPS TO ADDRESS PROBLEM.—Consistent
2 with existing authority, the Secretary shall review
3 and consider the information provided in any report
4 submitted under paragraph (1) and, at the sole,
5 unreviewable discretion of the Secretary, determine
6 what, if any, steps are necessary or appropriate to
7 address any threats, vulnerabilities, risks, and inci-
8 dents identified.

9 (4) DISCLOSURE OF IDENTITY.—

10 (A) IN GENERAL.—Except as provided in
11 subparagraph (B), or with the written consent
12 of the person, the Secretary may not disclose
13 the identity of a person who has provided infor-
14 mation described in paragraph (1).

15 (B) REFERRAL TO THE ATTORNEY GEN-
16 ERAL.—

17 (i) IN GENERAL.—The Secretary shall
18 disclose to the Attorney General the iden-
19 tity of a person who has provided informa-
20 tion described in paragraph (1) if the mat-
21 ter is referred to the Attorney General for
22 enforcement.

23 (ii) NOTICE.—The Secretary shall
24 provide reasonable advance notice to the
25 person described in clause (i) if disclosure

1 of that person's identity is to occur, unless
2 such notice would risk compromising a
3 criminal or civil enforcement investigation
4 or proceeding.

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

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

11 (2) prevent the classification of information
12 submitted under this section if that information
13 meets the standards for classification under Execu-
14 tive Order 12958, or any successor thereto, or affect
15 measures and controls relating to the protection of
16 classified information as prescribed by Federal stat-
17 ute or under Executive Order 12958, or any suc-
18 cessor thereto;

19 (3) limit the right of an individual to make any
20 disclosure—

21 (A) protected or authorized under section
22 2302(b)(8) or 7211 of title 5, United States
23 Code;

24 (B) to an appropriate official of informa-
25 tion that the individual reasonably believes evi-

1 dences a violation of any law, rule, or regula-
2 tion, gross mismanagement, or substantial and
3 specific danger to public health, safety, or secu-
4 rity, and that is protected under any Federal or
5 State law (other than those referenced in sub-
6 paragraph (A)) that shields the disclosing indi-
7 vidual against retaliation or discrimination for
8 having made the disclosure if such disclosure is
9 not specifically prohibited by law and if such in-
10 formation is not specifically required by Execu-
11 tive order to be kept secret in the interest of
12 national defense or the conduct of foreign af-
13 fairs; or

14 (C) to the Special Counsel, the Inspector
15 General of an agency, or any other employee
16 designated by the head of an agency to receive
17 similar disclosures;

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

22 (5) authorize information to be withheld from
23 Congress, the Comptroller General, or the Inspector
24 General of the Department;

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

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

5 (f) AUDIT.—

6 (1) IN GENERAL.—Not later than 1 year after
7 the date of enactment of this Act, the Inspector
8 General of the Department shall conduct an audit of
9 the management of information submitted under
10 this section and report the findings to appropriate
11 committees of Congress.

12 (2) CONTENTS.—The audit under paragraph
13 (1) shall include assessments of—

14 (A) whether the information is adequately
15 safeguarded against inappropriate disclosure;

16 (B) the processes for marking and dissemi-
17 nating the information and resolving any dis-
18 putes;

19 (C) how the information is used for the
20 purposes of this section, and whether that use
21 is effective;

22 (D) whether information sharing has been
23 effective to fulfill the purposes of this section;

1 (E) whether the kinds of information sub-
2 mitted have been appropriate and useful, or
3 overbroad or overnarrow;

4 (F) whether the information protections
5 allow for adequate accountability and trans-
6 parency of the regulatory, enforcement, and
7 other aspects of implementing this title; and

8 (G) any other factors at the discretion of
9 the Inspector General.

10 **SEC. 108. VOLUNTARY TECHNICAL ASSISTANCE.**

11 Subject to the availability of resources, in accordance
12 with applicable law relating to the protection of trade se-
13 crets, and at the discretion of the Secretary, the Secretary
14 shall provide voluntary technical assistance at the request
15 of an owner or operator of covered critical infrastructure,
16 to assist the owner or operator in meeting the require-
17 ments of section 105, including implementing required se-
18 curity or emergency measures, restoring the critical infra-
19 structure in the event of destruction or serious disruption,
20 and developing emergency response plans.

21 **SEC. 109. EMERGENCY PLANNING.**

22 (a) EMERGENCY PLANNING.—In partnership with
23 owners and operators, the Secretary, in coordination with
24 the heads of sector-specific agencies and the heads of other
25 Federal agencies with responsibilities for regulating the

1 security of covered critical infrastructure, shall exercise re-
2 sponse and restoration plans, including plans required
3 under section 105(b) to—

4 (1) assess performance and improve the capa-
5 bilities and procedures of government and private
6 sector entities to respond to a major cyber incident;
7 and

8 (2) clarify specific roles, responsibilities, and
9 authorities of government and private sector entities
10 when responding to a major cyber incident.

11 **SEC. 110. INTERNATIONAL COOPERATION.**

12 (a) IN GENERAL.—The Secretary, in coordination
13 with the Secretary of State or the head of the sector-spe-
14 cific agencies and the head of any Federal agency with
15 responsibilities for regulating the security of covered crit-
16 ical 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 security measures or other measures to
6 the information infrastructure to mitigate or reme-
7 diate 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. 111. EFFECT ON OTHER LAWS.**

14 (a) PREEMPTION OF STATE CYBERSECURITY
15 LAWS.—This Act shall supersede any statute, provision of
16 a statute, regulation, or rule of a State or political subdivi-
17 sion of a State that expressly requires comparable cyberse-
18 curity practices to protect covered critical infrastructure.

19 (b) PRESERVATION OF OTHER STATE LAW.—Except
20 as expressly provided in subsection (a) and section 105(e),
21 nothing in this Act shall be construed to preempt the ap-
22 plicability of any other State law or requirement.

1 **TITLE II—PROTECTING**
2 **GOVERNMENT NETWORKS**

3 **SEC. 201. FISMA REFORM.**

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

7 “SUBCHAPTER II—INFORMATION SECURITY

8 **“§ 3551. Purposes**

9 “The purposes of this subchapter are to—

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

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

23 “(3) provide for development and maintenance
24 of controls required to protect agency information
25 and information systems and contribute to the over-

1 all improvement of agency information security pos-
2 ture; and

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

9 **“§ 3552. Definitions**

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

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

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

20 “(2) CONTINUOUS MONITORING.—The term
21 ‘continuous monitoring’ means the ongoing real time
22 or near real-time process used to determine if the
23 complete set of planned, required, and deployed se-
24 curity controls within an information system con-
25 tinue to be effective over time in light of rapidly

1 changing information technology and threat develop-
2 ment. To the maximum extent possible, this also re-
3 quires automation of that process to enable cost ef-
4 fective, efficient, and consistent monitoring and pro-
5 vide a more dynamic view of the security state of
6 those deployed controls.

7 “(3) INCIDENT.—The term ‘incident’ means an
8 occurrence that—

9 “(A) actually or imminently jeopardizes,
10 without lawful authority, the integrity, con-
11 fidentiality, or availability of information or an
12 information system; or

13 “(B) constitutes a violation or imminent
14 threat of violation of law, security policies, secu-
15 rity procedures, or acceptable use policies.

16 “(4) INFORMATION SECURITY.—The term ‘in-
17 formation security’ means protecting information
18 and information systems from unauthorized access,
19 use, disclosure, disruption, modification, or destruc-
20 tion in order to provide—

21 “(A) integrity, which means guarding
22 against improper information modification or
23 destruction, and includes ensuring nonrepudi-
24 ation and authenticity;

1 “(B) confidentiality, which means pre-
2 serving authorized restrictions on access and
3 disclosure, including means for protecting per-
4 sonal privacy and proprietary information; and

5 “(C) availability, which means ensuring
6 timely and reliable access to and use of infor-
7 mation.

8 “(5) INFORMATION TECHNOLOGY.—The term
9 ‘information technology’ has the meaning given that
10 term in section 11101 of title 40.

11 “(6) NATIONAL SECURITY SYSTEM.—

12 “(A) IN GENERAL.—The term ‘national se-
13 curity system’ means any information system
14 (including any telecommunications system) used
15 or operated by an agency or by a contractor of
16 an agency, or other organization on behalf of an
17 agency—

18 “(i) the function, operation, or use of
19 which—

20 “(I) involves intelligence activi-
21 ties;

22 “(II) involves cryptologic activi-
23 ties related to national security;

24 “(III) involves command and
25 control of military forces;

1 “(IV) involves equipment that is
2 an integral part of a weapon or weap-
3 ons system; or

4 “(V) subject to subparagraph
5 (B), is critical to the direct fulfillment
6 of military or intelligence missions; or

7 “(ii) that is protected at all times by
8 procedures established for information that
9 have been specifically authorized under cri-
10 teria established by an Executive order or
11 an Act of Congress to be kept classified in
12 the interest of national defense or foreign
13 policy.

14 “(B) EXCLUSION.—Subparagraph
15 (A)(i)(V) does not include a system that is to
16 be used for routine administrative and business
17 applications (including payroll, finance, logis-
18 tics, and personnel management applications).

19 “(7) SECRETARY.—The term ‘Secretary’ means
20 the Secretary of Homeland Security.

21 “(8) THREAT ASSESSMENT.—The term ‘threat
22 assessment’ means the real time or near real time
23 process of formally evaluating the degree of threat
24 to an information system or enterprise and describ-
25 ing the nature of the threat. Threat assessments

1 consist of identifying threat sources, possible threat
2 events, vulnerabilities within a system or network
3 environment, determining the likelihood that an
4 identified threat will occur and the possible adverse
5 impacts of such an occurrence. This requires auto-
6 mation of that process and rapid sharing of emerg-
7 ing threat information among government agencies.

8 **“§ 3553. Federal information security authority and**
9 **coordination**

10 “(a) IN GENERAL.—Except as provided in sub-
11 sections (f) and (g), the Secretary shall oversee agency in-
12 formation security policies and practices, including the de-
13 velopment and oversight of information security policies
14 and directives and compliance with this subchapter.

15 “(b) DUTIES.—The Secretary shall—

16 “(1) develop, issue, and oversee the implemen-
17 tation of information security policies and directives,
18 which shall be compulsory and binding on agencies
19 to the extent determined appropriate by the Sec-
20 retary, including—

21 “(A) policies and directives consistent with
22 the standards promulgated under section 11331
23 of title 40 to identify and provide information
24 security protections that are commensurate
25 with the risk and impact resulting from the un-

1 authorized access, use, disclosure, disruption,
2 modification, or destruction of—

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

7 “(ii) information systems used or op-
8 erated by an agency or by a contractor of
9 an agency or other organization on behalf
10 of an agency;

11 “(B) minimum operational requirements
12 for network operations centers and security op-
13 erations centers of agencies to facilitate the
14 protection of and provide common situational
15 awareness for all agency information and infor-
16 mation systems;

17 “(C) reporting requirements, consistent
18 with relevant law, regarding information secu-
19 rity incidents;

20 “(D) requirements for agencywide informa-
21 tion security programs, including continuous
22 monitoring of information security;

23 “(E) performance requirements and
24 metrics for the security of agency information
25 systems;

1 “(F) training requirements to ensure that
2 agencies are able to fully and timely comply
3 with directions issued by the Secretary under
4 this subchapter;

5 “(G) training requirements regarding pri-
6 vacy, civil rights, civil liberties, and information
7 oversight for agency information security em-
8 ployees;

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

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

13 “(2) review agency information security pro-
14 grams required to be developed under section
15 3554(b);

16 “(3) develop and conduct targeted risk assess-
17 ments and operational evaluations for agency infor-
18 mation and information systems in consultation with
19 the heads of other agencies or governmental and pri-
20 vate entities that own and operate such systems,
21 that may include threat, vulnerability, and impact
22 assessments and penetration testing;

23 “(4) operate consolidated intrusion detection,
24 prevention, or other protective capabilities and use
25 associated countermeasures for the purpose of pro-

1 tecting agency information and information systems
2 from information security threats;

3 “(5) in conjunction with other agencies and the
4 private sector, assess and foster the development of
5 information security technologies and capabilities for
6 use across multiple agencies;

7 “(6) designate an entity to receive reports and
8 information about information security incidents,
9 threats, and vulnerabilities affecting agency informa-
10 tion systems;

11 “(7) provide incident detection, analysis, miti-
12 gation, and response information and remote or on-
13 site technical assistance to the heads of agencies;
14 and

15 “(8) coordinate with appropriate agencies and
16 officials to ensure, to the maximum extent feasible,
17 that policies and directives issued under paragraph
18 (1) are complementary with—

19 “(A) standards and guidelines developed
20 for national security systems; and

21 “(B) policies and directives issues by the
22 Secretary of Defense, Director of the Central
23 Intelligence Agency, and Director of National
24 Intelligence under subsection (g)(1).

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

14 “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

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

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

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

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

15 “(C) information obtained under activities
16 authorized under this subsection will only be re-
17 tained, used, or disclosed to protect agency in-
18 formation systems from information security
19 threats, mitigate against such threats, or, with
20 the approval of the Attorney General, for law
21 enforcement purposes when the information is
22 evidence of a crime which has been, is being, or
23 is about to be committed;

24 “(D) notice has been provided to users of
25 agency information systems concerning the po-

1 tential for acquisition, interception, retention,
2 use, and disclosure of communications and
3 other system traffic; and

4 “(E) the activities are implemented pursu-
5 ant to policies and procedures governing the ac-
6 quisition, interception, retention, use, and dis-
7 closure of communications and other system
8 traffic that have been reviewed and approved by
9 the Attorney General.

10 “(3) PRIVATE ENTITIES.—The Secretary may
11 enter into contracts or other agreements, or other-
12 wise request and obtain the assistance of, private en-
13 tities that provide electronic communication or infor-
14 mation security services to acquire, intercept, retain,
15 use, and disclose communications and other system
16 traffic in accordance with this subsection.

17 “(e) DIRECTIONS TO AGENCIES.—

18 “(1) AUTHORITY.—

19 “(A) IN GENERAL.—Notwithstanding sec-
20 tion 3554, and subject to subparagraph (B), in
21 response to a known or reasonably suspected in-
22 formation security threat, vulnerability, or inci-
23 dent that represents a substantial threat to the
24 information security of an agency, the Secretary
25 may direct other agency heads to take any law-

1 ful action with respect to the operation of the
2 information systems, including those owned or
3 operated by another entity on behalf of an
4 agency, that collect, process, store, transmit,
5 disseminate, or otherwise maintain agency in-
6 formation, for the purpose of protecting the in-
7 formation system from or mitigating an infor-
8 mation security threat.

9 “(B) EXCEPTION.—The authorities of the
10 Secretary under this subsection shall not apply
11 to a system described in paragraph (2), (3), or
12 (4) of subsection (g).

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

14 The Secretary shall—

15 “(A) in coordination with the Director of
16 the Office of Management and Budget and in
17 consultation with Federal contractors, as appro-
18 priate, establish procedures governing the cir-
19 cumstances under which a directive may be
20 issued under this subsection, which shall in-
21 clude—

22 “(i) thresholds and other criteria;

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

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

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

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

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

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

13 “(D) notify the Director of the Office of
14 Management and Budget and head of any af-
15 fected agency immediately upon the issuance of
16 a directive under this subsection.

17 “(3) IMMINENT THREATS.—

18 “(A) IN GENERAL.—If the Secretary deter-
19 mines that there is an imminent threat to agen-
20 cy information systems and a directive under
21 this subsection is not reasonably likely to result
22 in a timely response to the threat, the Secretary
23 may authorize the use of protective capabilities
24 under the control of the Secretary for commu-
25 nications or other system traffic transiting to or

1 from or stored on an agency information system
2 without prior consultation with the affected
3 agency for the purpose of ensuring the security
4 of the information or information system or
5 other agency information systems.

6 “(B) LIMITATION ON DELEGATION.—The
7 authority under this paragraph may not be del-
8 egated to an official in a position lower than
9 Assistant Secretary.

10 “(C) NOTICE.—The Secretary or designee
11 of the Secretary shall immediately notify the
12 Director of the Office of Management and
13 Budget and the head and chief information offi-
14 cer (or equivalent official) of each affected
15 agency of—

16 “(i) any action taken under this sub-
17 section; and

18 “(ii) the reasons for and duration and
19 nature of the action.

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

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

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

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

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

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

13 “(f) NATIONAL SECURITY SYSTEMS.—

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

16 “(2) INFORMATION SECURITY.—Information se-
17 curity policies, directives, standards, and guidelines
18 for national security systems shall be overseen as di-
19 rected by the President and, in accordance with that
20 direction, carried out under the authority of the
21 heads of agencies that operate or exercise authority
22 over national security systems.

23 “(g) DELEGATION OF AUTHORITIES.—

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

4 “(A) the Secretary of Defense in the case
5 of systems described in paragraph (2);

6 “(B) the Director of the Central Intel-
7 ligence Agency in the case of systems described
8 in paragraph (3); and

9 “(C) the Director of National Intelligence
10 in the case of systems described in paragraph
11 (4).

12 “(2) DEPARTMENT OF DEFENSE.—The systems
13 described in this paragraph are systems that are op-
14 erated by the Department of Defense, a contractor
15 of the Department of Defense, or another entity on
16 behalf of the Department of Defense that process
17 any information the unauthorized access, use, disclo-
18 sure, disruption, modification, or destruction of
19 which would have a debilitating impact on the mis-
20 sion of the Department of Defense.

21 “(3) CENTRAL INTELLIGENCE AGENCY.—The
22 systems described in this paragraph are systems
23 that are operated by the Central Intelligence Agen-
24 cy, a contractor of the Central Intelligence Agency,
25 or another entity on behalf of the Central Intel-

1 ligence Agency that process any information the un-
2 authorized access, use, disclosure, disruption, modi-
3 fication, or destruction of which would have a debili-
4 tating impact on the mission of the Central Intel-
5 ligence Agency.

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

18 “(5) INTEGRATION OF INFORMATION.—The
19 Secretary of Defense, the Director of the Central In-
20 telligence Agency, and the Director of National In-
21 telligence shall carry out their responsibilities under
22 this subsection in coordination with the Secretary
23 and share relevant information in a timely manner
24 with the Secretary relating to the security of agency
25 information and information systems, including sys-

1 tems described in paragraphs (2), (3), and (4), to
2 enable the Secretary to carry out the responsibilities
3 set forth in this section and to maintain comprehen-
4 sive situational awareness regarding information se-
5 curity incidents, threats, and vulnerabilities affecting
6 agency information systems, consistent with stand-
7 ards and guidelines for national security systems,
8 issued in accordance with law and as directed by the
9 President.

10 **“§ 3554. Agency responsibilities**

11 “(a) IN GENERAL.—The head of each agency shall—

12 “(1) be responsible for—

13 “(A) providing information security protec-
14 tions commensurate with the risk resulting
15 from unauthorized access, use, disclosure, dis-
16 ruption, modification, or destruction of—

17 “(i) information collected, created,
18 processed, stored, disseminated, or other-
19 wise used or maintained by or on behalf of
20 the agency; or

21 “(ii) information systems used or op-
22 erated by the agency or by a contractor of
23 the agency or other organization on behalf
24 of the agency;

1 “(B) complying with this subchapter, in-
2 cluding—

3 “(i) the policies and directives issued
4 under section 3553, including any direc-
5 tions under section 3553(e); and

6 “(ii) information security policies, di-
7 rectives, standards, and guidelines for na-
8 tional security systems issued in accord-
9 ance with law and as directed by the Presi-
10 dent;

11 “(C) complying with the requirements of
12 the information security standards prescribed
13 under section 11331 of title 40, including any
14 required security configuration checklists; and

15 “(D) ensuring that information security
16 management processes are integrated with
17 agency strategic and operational planning pro-
18 cesses;

19 “(2) ensure that senior agency officials provide
20 information security for the information and infor-
21 mation systems that support the operations and as-
22 sets under the control of the officials, including
23 through—

24 “(A) assessing, with a frequency commen-
25 surate with risk, the risk and impact that could

1 result from the unauthorized access, use, disclo-
2 sure, disruption, modification, or destruction of
3 the information or information systems;

4 “(B) determining the levels of information
5 security appropriate to protect the information
6 and information systems in accordance with the
7 policies and directives issued under section
8 3553(b) and standards prescribed under section
9 11331 of title 40;

10 “(C) implementing policies, procedures,
11 and capabilities to reduce risks to an acceptable
12 level in a cost-effective manner;

13 “(D) security testing and evaluation, in-
14 cluding continuously monitoring the effective
15 implementation of information security controls
16 and techniques, threats, vulnerabilities, assets,
17 and other aspects of information security as ap-
18 propriate; and

19 “(E) reporting information about informa-
20 tion security incidents, threats, and
21 vulnerabilities in a timely manner as required
22 under policies and procedures established under
23 subsection (b)(7);

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

4 “(4) delegate to the chief information officer or
5 equivalent official (or to a senior agency official who
6 reports to the chief information officer or equivalent
7 official) the authority to ensure and primary respon-
8 sibility for ensuring compliance with this subchapter,
9 including—

10 “(A) overseeing the establishment and
11 maintenance of an agencywide security oper-
12 ations capability that on a continuous basis
13 can—

14 “(i) detect, report, respond to, con-
15 tain, and mitigate information security in-
16 cidents that impair adequate security of
17 the agency information and information
18 systems in a timely manner and in accord-
19 ance with the policies and directives issued
20 under section 3553(b); and

21 “(ii) report any information security
22 incident described under clause (i) to the
23 entity designated under section 3553(b)(6);

1 “(B) developing, maintaining, and over-
2 seeing an agencywide information security pro-
3 gram as required under subsection (b);

4 “(C) developing, maintaining, and over-
5 seeing information security policies, procedures,
6 and control techniques to address all applicable
7 requirements, including those issued under sec-
8 tion 3553 and section 11331 of title 40;

9 “(D) training and overseeing employees
10 and contractors of the agency with significant
11 responsibilities for information security with re-
12 spect to such responsibilities; and

13 “(E) assisting senior agency officials con-
14 cerning their responsibilities under paragraph
15 (2);

16 “(5) the agency has trained and obtained secu-
17 rity clearances for an adequate number of employees
18 to assist the agency in complying with this sub-
19 chapter, including the policies and directives issued
20 under section 3553(b);

21 “(6) ensure that the chief information officer
22 (or other senior agency official designated under
23 paragraph (4)), in coordination with other senior
24 agency officials, reports to the head of the agency on

1 the effectiveness of the agency information security
2 program, including the progress of remedial actions;

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

6 “(A) possesses the necessary qualifications
7 to administer the duties of the official under
8 this subchapter; and

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

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

16 “(b) AGENCY PROGRAM.—The head of each agency
17 shall develop, document, and implement an agencywide in-
18 formation security program, which shall be reviewed under
19 section 3553(b)(2), to provide information security for the
20 information and information systems that support the op-
21 erations and assets of the agency, including those provided
22 or managed by another agency, contractor, or other
23 source, which shall include—

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

4 “(A) considers information security
5 threats, vulnerabilities, and consequences;

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

9 “(2) policies and procedures that—

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

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

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

19 “(D) ensure compliance with—

20 “(i) this subchapter;

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

24 “(iii) any other applicable require-
25 ments;

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

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

11 “(A) information security risks associated
12 with their activities;

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

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

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

21 “(A) risk-based continuous monitoring of
22 the operational status and security of agency
23 information systems to enable evaluation of the
24 effectiveness of and compliance with informa-
25 tion security policies, procedures, and practices,

1 including a relevant and appropriate selection of
2 management, operational, and technical controls
3 of information systems identified in the inven-
4 tory required under section 3505(c);

5 “(B) penetration testing exercises and
6 operational evaluations in accordance with the
7 requirements issued under section 3553(b) to
8 evaluate whether the agency adequately protects
9 against, detects, and responds to incidents;

10 “(C) vulnerability scanning, intrusion de-
11 tection and prevention, and penetration testing,
12 in accordance with the requirements issued
13 under section 3553(b); and

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

17 “(6) a process for ensuring that remedial ac-
18 tions are taken to mitigate information security
19 vulnerabilities commensurate with risk and impact,
20 and otherwise address any deficiencies in the infor-
21 mation security policies, procedures, and practices of
22 the agency;

23 “(7) policies and procedures to ensure detec-
24 tion, mitigation, reporting, and responses to infor-
25 mation security incidents, in accordance with the

1 policies and directives issued under section 3553(b),
2 including—

3 “(A) ensuring timely internal reporting of
4 information security incidents;

5 “(B) establishing and maintaining appro-
6 priate technical capabilities to detect and miti-
7 gate risks associated with information security
8 incidents;

9 “(C) notifying and consulting with the en-
10 tity designated by the Secretary under section
11 3553(b)(6); and

12 “(D) notifying and consulting with—

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

15 “(ii) any other entity, in accordance
16 with law and as directed by the President;
17 and

18 “(8) plans and procedures to ensure continuity
19 of operations for information systems that support
20 the operations and assets of the agency.

21 “(c) AGENCY REPORTING.—The head of each agency
22 shall—

23 “(1) report annually to the Secretary on the
24 adequacy and effectiveness of information security
25 policies, procedures, and practices, including—

1 “(A) compliance of the agency with the re-
2 quirements of this subchapter;

3 “(B) a conclusion as to the effectiveness of
4 the information security policies, procedures,
5 and practices of the agency based on a deter-
6 mination of the aggregate effect of identified
7 deficiencies;

8 “(C) an identification and analysis of, in-
9 cluding actions and plans to address, any sig-
10 nificant deficiencies identified in such policies,
11 procedures and practices; and

12 “(D) any information or evaluation re-
13 quired under the reporting requirements issued
14 under section 3553(b);

15 “(2) make the report required under paragraph
16 (1) available to the appropriate authorization and
17 appropriations committees of Congress and the
18 Comptroller General of the United States; and

19 “(3) address the adequacy and effectiveness of
20 the information security policies, procedures, and
21 practices of the agency as required for management
22 and budget plans and reports, as appropriate.

23 “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—
24 Notwithstanding any other provision of law, the head of
25 each agency is authorized to allow the Secretary, or a pri-

1 vate entity providing assistance to the Secretary under
2 section 3553, to acquire, intercept, retain, use, and dis-
3 close communications, system traffic, records, or other in-
4 formation transiting to or from or stored on an agency
5 information system for the purpose of protecting agency
6 information and information systems from information se-
7 curity threats or mitigating the threats in connection with
8 the implementation of the information security capabilities
9 authorized by paragraph (3) or (4) of section 3553(b).

10 **“§ 3555. Annual assessments**

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

18 “(b) CONTENTS.—Each assessment conducted under
19 subsection (a) shall—

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

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

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

4 “(c) CERTAIN INFORMATION SYSTEMS.—

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

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

13 “(A) the Secretary of Defense for informa-
14 tion systems under the control of the Depart-
15 ment of Defense;

16 “(B) the Director of the Central Intel-
17 ligence Agency for information systems under
18 the control of the Central Intelligence Agency;
19 and

20 “(C) the Director of National Intelligence
21 for information systems under the control of
22 the Office of the Director of National Intel-
23 ligence.

24 “(d) AGENCY-SPECIFIC ASSESSMENTS.—Each as-
25 sessment conducted under subsection (a) that relates, in

1 whole or in part, to the information systems of an agency
2 shall be made available to the head of the agency.

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

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

16 **“§ 3556. Independent evaluations**

17 “(a) IN GENERAL.—Not less than once every 2 years,
18 an independent evaluation shall be performed of the infor-
19 mation security program and practices of each agency in
20 accordance with the guidance developed under subsection
21 (d) to determine the effectiveness of the programs and
22 practices in addressing risk.

23 “(b) CONTENTS.—Each evaluation performed under
24 subsection (a) shall include—

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

5 “(2) an assessment of compliance with this sub-
6 chapter and any significant deficiencies; and

7 “(3) a conclusion as to the effectiveness of the
8 information security policies, procedures, and prac-
9 tices of the agency in addressing risk based on a de-
10 termination of the aggregate effect of identified defi-
11 ciencies.

12 “(c) CONDUCT OF INDEPENDENT EVALUATIONS.—
13 An evaluation of an agency under subsection (a) shall be
14 performed by—

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

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

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

23 “(d) GUIDANCE.—The Council of Inspectors General
24 on Integrity and Efficiency, in consultation with the Sec-
25 retary, the Comptroller General of the United States, and

1 the Director of the National Institute of Standards and
2 Technology, shall issue and maintain guidance for per-
3 forming timely, cost-effective, and risk-based evaluations
4 under subsection (a).

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

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

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

17 “(1) the adequacy and effectiveness of the in-
18 formation security policies and practices of agencies;

19 and

20 “(2) implementation of this subchapter.

21 **“§ 3557. National security systems**

22 “The head of each agency operating or exercising
23 control of a national security system shall be responsible
24 for ensuring that the agency—

1 “(1) provides information security protections
2 commensurate with the risk and magnitude of the
3 harm resulting from the unauthorized use, disclo-
4 sure, disruption, modification, or destruction of the
5 information contained in the national security sys-
6 tem;

7 “(2) implements information security policies
8 and practices as required by standards and guide-
9 lines for national security systems issued in accord-
10 ance with law and as directed by the President; and

11 “(3) complies with this subchapter.

12 **“§ 3558. Effect on existing law**

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

16 (b) TECHNICAL AND CONFORMING AMENDMENT.—
17 The table of sections for chapter 35 of title 44 is amended
18 by striking the matter relating to subchapters II and III
19 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.”.

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

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

4 **“§ 11331. Responsibilities for Federal information sys-**
5 **tems standards**

6 “(a) DEFINITIONS.—In this section:

7 “(1) FEDERAL INFORMATION SYSTEM.—The
8 term ‘Federal information system’ means an infor-
9 mation system used or operated by an executive
10 agency, by a contractor of an executive agency, or by
11 another entity on behalf of an executive agency.

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

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

18 “(b) STANDARDS AND GUIDELINES.—

19 “(1) AUTHORITY TO PRESCRIBE.—Except as
20 provided under paragraph (2), and based on the
21 standards and guidelines developed by the National
22 Institute of Standards and Technology under para-
23 graphs (2) and (3) of section 20(a) of the National
24 Institute of Standards and Technology Act (15
25 U.S.C. 278g–3(a)), the Secretary of Commerce, in
26 consultation with the Secretary of Homeland Secu-

1 rity, shall prescribe standards and guidelines relat-
2 ing to Federal information systems.

3 “(2) NATIONAL SECURITY SYSTEMS.—Stand-
4 ards and guidelines for national security systems
5 shall be developed, prescribed, enforced, and over-
6 seen as otherwise authorized by law and as directed
7 by the President.

8 “(c) MANDATORY REQUIREMENTS.—

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

16 “(2) REQUIRED MANDATORY STANDARDS.—

17 “(A) IN GENERAL.—The Secretary of
18 Commerce shall require executive agencies to
19 comply with the standards described in sub-
20 paragraph (B).

21 “(B) CONTENTS.—The standards de-
22 scribed in this subparagraph are information
23 security standards that—

24 “(i) provide minimum information se-
25 curity requirements as determined under

1 section 20(b) of the National Institute of
2 Standards and Technology Act (15 U.S.C.
3 278g-3(b)); and

4 “(ii) are otherwise necessary to im-
5 prove the security of Federal information
6 and Federal information systems.

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

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

1 “(f) APPLICATION OF MORE STRINGENT STAND-
2 ARDS.—The head of an executive agency may employ
3 standards for the cost-effective information security for
4 Federal information systems of that agency that are more
5 stringent than the standards prescribed by the Secretary
6 of Commerce under subsection (b)(1) if the more stringent
7 standards—

8 “(1) contain any standards with which the Sec-
9 retary of Commerce has required the agency to com-
10 ply; and

11 “(2) are otherwise consistent with the policies
12 and directives issued under section 3553(b) of title
13 44.

14 “(g) DECISIONS ON PROMULGATION OF STAND-
15 ARDS.—The decision by the Secretary of Commerce re-
16 garding the promulgation of any standard under this sec-
17 tion shall occur not later than 6 months after the submis-
18 sion of the proposed standard to the Secretary of Com-
19 merce by the National Institute of Standards and Tech-
20 nology, as provided under section 20 of the National Insti-
21 tute of Standards and Technology Act (15 U.S.C. 278g-
22 3).”.

23 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

1 (1) Section 3502(8)) of title 44, United States
2 Code, is amended by inserting “hosting,” after “col-
3 lection,”;

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

7 (A) in section 20(a)(2) (15 U.S.C. 278g-
8 3(a)(2)), by striking “section 3532(b)(2)” and
9 inserting “section 3552(b)”; and

10 (B) in section 21(b) (15 U.S.C. 278g-
11 4(b))—

12 (i) in paragraph (2), by inserting “,
13 the Secretary of Homeland Security,” after
14 “the Institute”; and

15 (ii) in paragraph (3), by inserting
16 “the Secretary of Homeland Security,”
17 after “the Secretary of Commerce,”.

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

22 (4) Part IV of title 10, United States Code, is
23 amended—

1 (A) in section 2222(j)(5), by striking “sec-
2 tion 3542(b)(2)” and inserting “section
3 3552(b)”;

4 (B) in section 2223(c)(3), by striking “sec-
5 tion 3542(b)(2)” and inserting “section
6 3552(b)”;

7 (C) in section 2315, by striking “section
8 3542(b)(2)” and inserting “section 3552(b)”.

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

13 **SEC. 203. SAVINGS PROVISIONS.**

14 (a) **IN GENERAL.**—Policies and compliance guidance
15 issued by the Director of the Office of Management and
16 Budget before the date of enactment of this Act under
17 section 3543(a)(1) of title 44 (as in effect on the day be-
18 fore the date of enactment of this Act) shall continue in
19 effect, according to their terms, until modified, termi-
20 nated, superseded, or repealed under section 3553(b)(1)
21 of title 44, as added by this Act.

22 (b) **OTHER STANDARDS AND GUIDELINES.**—Stand-
23 ards and guidelines issued by the Secretary of Commerce
24 or by the Director of the Office of Management and Budg-
25 et before the date of enactment of this Act under section

1 11331(b)(1) of title 40 (as in effect on the day before the
 2 date of enactment of this Act) shall continue in effect, ac-
 3 cording to their terms, until modified, terminated, super-
 4 seded, or repealed under section 11331(b)(1), as added by
 5 this Act.

6 **TITLE III—CLARIFYING AND**
 7 **STRENGTHENING EXISTING**
 8 **ROLES AND AUTHORITIES**

9 **SEC. 301. CONSOLIDATION OF EXISTING DEPARTMENTAL**
 10 **CYBER RESOURCES AND AUTHORITIES.**

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

14 **“Subtitle E—Cybersecurity**

15 **“SEC. 241. DEFINITIONS.**

16 “In this subtitle:

17 “(1) AGENCY INFORMATION INFRASTRUC-
 18 TURE.—The term ‘agency information infrastruc-
 19 ture’ means the Federal information infrastructure
 20 of a particular Federal agency.

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

24 “(3) COVERED CRITICAL INFRASTRUCTURE.—
 25 The term ‘covered critical infrastructure’ means a

1 system or asset designated by the Secretary as covered
2 critical infrastructure in accordance with the
3 procedure established under section 103 of the Cy-
4 bersecurity Act of 2012.

5 “(4) DAMAGE.—The term ‘damage’ has the
6 meaning given that term in section 1030(e) of title
7 18, United States Code.

8 “(5) FEDERAL AGENCY.—The term ‘Federal
9 agency’ has the meaning given the term ‘agency’ in
10 section 3502 of title 44, United States Code.

11 “(6) FEDERAL CYBERSECURITY CENTER.—The
12 term ‘Federal cybersecurity center’ has the meaning
13 given that term in section 708 of the Cybersecurity
14 Act of 2012.

15 “(7) FEDERAL ENTITY.—The term ‘Federal en-
16 tity’ has the meaning given that term in section 708
17 of the Cybersecurity Act of 2012.

18 “(8) FEDERAL INFORMATION INFRASTRUC-
19 TURE.—The term ‘Federal information infrastruc-
20 ture’—

21 “(A) means information and information
22 systems that are owned, operated, controlled, or
23 licensed for use by, or on behalf of, any Federal
24 agency, including information systems used or

1 operated by another entity on behalf of a Fed-
2 eral agency; and

3 “(B) does not include—

4 “(i) a national security system; or

5 “(ii) information and information sys-
6 tems that are owned, operated, controlled,
7 or licensed for use by, or on behalf of, the
8 Department of Defense, a military depart-
9 ment, or another element of the intel-
10 ligence community.

11 “(9) INCIDENT.—The term ‘incident’ has the
12 meaning given that term in section 3552 of title 44,
13 United States Code.

14 “(10) INFORMATION SECURITY.—The term ‘in-
15 formation security’ has the meaning given that term
16 in section 3552 of title 44, United States Code.

17 “(11) INFORMATION SYSTEM.—The term ‘infor-
18 mation system’ has the meaning given that term in
19 section 3502 of title 44, United States Code.

20 “(12) INTELLIGENCE COMMUNITY.—The term
21 ‘intelligence community’ has the meaning given that
22 term in section 3(4) of the National Security Act of
23 1947 (50 U.S.C. 401a(4)).

24 “(13) NATIONAL SECURITY AND EMERGENCY
25 PREPAREDNESS COMMUNICATIONS INFRASTRUC-

1 TURE.—The term ‘national security and emergency
2 preparedness communications infrastructure’ means
3 the systems supported or covered by the Office of
4 Emergency Communications and the National Com-
5 munications System on the date of enactment of the
6 Cybersecurity Act of 2012 or otherwise described in
7 Executive Order 12472, or any successor thereto, re-
8 lating to national security and emergency prepared-
9 ness communications functions.

10 “(14) NATIONAL INFORMATION INFRASTRUC-
11 TURE.—The term ‘national information infrastruc-
12 ture’ means information and information systems—

13 “(A) that are owned, operated, or con-
14 trolled within or from the United States; and

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

17 “(15) NATIONAL SECURITY SYSTEM.—The term
18 ‘national security system’ has the meaning given
19 that term in section 3552 of title 44, United States
20 Code.

21 “(16) NON-FEDERAL ENTITY.—The term ‘non-
22 Federal entity’ has the meaning given that term in
23 section 708 of the Cybersecurity Act of 2012.

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

2 “(a) ESTABLISHMENT.—There is established within
3 the Department a National Center for Cybersecurity and
4 Communications.

5 “(b) TRANSFER OF FUNCTIONS.—There are trans-
6 ferred to the Center the National Cyber Security Division,
7 the Office of Emergency Communications, and the Na-
8 tional Communications System, including all the func-
9 tions, personnel, assets, authorities, and liabilities of the
10 National Cyber Security Division, the Office of Emergency
11 Communications, and the National Communications Sys-
12 tem.

13 “(c) DIRECTOR.—The Center shall be headed by a
14 Director, who shall be appointed by the President, by and
15 with the advice and consent of the Senate, and who shall
16 report directly to the Secretary.

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

18 “(1) manage Federal efforts to secure, protect,
19 and ensure the resiliency of the Federal information
20 infrastructure, national information infrastructure,
21 and national security and emergency preparedness
22 communications infrastructure of the United States,
23 working cooperatively with appropriate government
24 agencies and the private sector;

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

4 “(3) prioritize the efforts of the Center to ad-
5 dress the most significant risks and incidents that
6 have caused or are likely to cause damage to the
7 Federal information infrastructure, the national in-
8 formation infrastructure, and national security and
9 emergency preparedness communications infrastruc-
10 ture of the United States;

11 “(4) ensure, in coordination with the privacy of-
12 ficer designated under subsection (j), the Privacy
13 Officer appointed under section 222, and the Direc-
14 tor of the Office of Civil Rights and Civil Liberties
15 appointed under section 705, that the activities of
16 the Center comply with all policies, regulations, and
17 laws protecting the privacy and civil liberties of
18 United States persons; and

19 “(5) perform such other duties as the Secretary
20 may require relating to the security and resiliency of
21 the Federal information infrastructure, national in-
22 formation infrastructure, and the national security
23 and emergency preparedness communications infra-
24 structure of the United States.

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

3 “(1) engage in activities and otherwise coordi-
4 nate Federal efforts to identify, protect against, re-
5 mediate, and mitigate, respond to, and recover from
6 cybersecurity threats, consequences, vulnerabilities
7 and incidents impacting the Federal information in-
8 frastructure and the national information infrastruc-
9 ture, including by providing support to entities that
10 own or operate national information infrastructure,
11 at their request;

12 “(2) conduct risk-based assessments of the Fed-
13 eral information infrastructure, and risk assessments
14 of critical infrastructure;

15 “(3) develop, oversee the implementation of,
16 and enforce policies, principles, and guidelines on in-
17 formation security for the Federal information infra-
18 structure, including exercise of the authorities under
19 the Federal Information Security Management Act
20 of 2002 (title III of Public Law 107–347; 116 Stat.
21 2946);

22 “(4) evaluate and facilitate the adoption of
23 technologies designed to enhance the protection of
24 information infrastructure, including making such
25 technologies available to entities that own or operate

1 national information infrastructure, with or without
2 reimbursement, as necessary to accomplish the pur-
3 poses of this section;

4 “(5) oversee the responsibilities related to na-
5 tional security and emergency preparedness commu-
6 nications infrastructure, including the functions of
7 the Office of Emergency Communications and the
8 National Communications System;

9 “(6)(A) maintain comprehensive situational
10 awareness of the security of the Federal information
11 infrastructure and the national information infra-
12 structure for the purpose of enabling and supporting
13 activities under subparagraph (e)(1); and

14 “(B) provide classified and unclassified infor-
15 mation to entities that own or operate national in-
16 formation infrastructure to support efforts by such
17 entities to secure such infrastructure and for en-
18 hancing overall situational awareness;

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

24 “(8) develop, in coordination with the Assistant
25 Secretary for Infrastructure Protection, other Fed-

1 eral agencies, the private sector, and State and local
2 governments a national incident response plan that
3 details the roles of Federal agencies, State and local
4 governments, and the private sector, and coordinate
5 national cyber incident response efforts;

6 “(9) consult, in coordination with the Secretary
7 of State, with appropriate international partners to
8 enhance the security of the Federal information in-
9 frastructure, national information infrastructure,
10 and information infrastructure located outside the
11 United States the disruption of which could result in
12 national or regional catastrophic damage in the
13 United States; and

14 “(10) coordinate the activities undertaken by
15 Federal agencies to—

16 “(A) protect Federal information infra-
17 structure and national information infrastruc-
18 ture; and

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

22 “(11) perform such other duties as the Sec-
23 retary may require relating to the security and resil-
24 iency of the Federal information infrastructure, na-
25 tional information infrastructure, and national secu-

1 rity and emergency preparedness communications in-
2 frastructure of the United States.

3 “(f) USE OF EXISTING MECHANISMS FOR COLLABO-
4 RATION.—To avoid unnecessary duplication or waste, in
5 carrying out the authorities and responsibilities of the
6 Center under this subtitle, to the maximum extent prac-
7 ticable, the Director of the Center shall make use of exist-
8 ing mechanisms for collaboration and information sharing,
9 including mechanisms relating to the identification and
10 communication of cybersecurity threats, vulnerabilities,
11 and associated consequences, established by other compo-
12 nents of the Department or other Federal agencies and
13 the information sharing mechanisms established under
14 title VII of the Cybersecurity Act of 2012.

15 “(g) DEPUTY DIRECTORS.—

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

18 “(A) have expertise in infrastructure pro-
19 tection; and

20 “(B) ensure that the operations of the
21 Center and the Office of Infrastructure Protec-
22 tion avoid duplication and use, to the maximum
23 extent practicable, joint mechanisms for infor-
24 mation sharing and coordination with the pri-
25 vate sector.

1 “(2) INTELLIGENCE COMMUNITY.—The Direc-
2 tor of National Intelligence, with the concurrence of
3 the Secretary, shall identify an employee of an ele-
4 ment of the intelligence community to serve as a
5 Deputy Director of the Center. The employee shall
6 be detailed to the Center on a reimbursable basis for
7 such period as is agreed to by the Director of the
8 Center and the Director of National Intelligence,
9 and, while serving as Deputy Director, shall report
10 directly to the Director of the Center.

11 “(h) CYBERSECURITY EXERCISE PROGRAM.—The
12 Director of the Center shall develop and implement a na-
13 tional cybersecurity exercise program with the participa-
14 tion of State and local governments, international partners
15 of the United States, and the private sector.

16 “(i) LIAISON OFFICERS.—

17 “(1) REQUIRED DETAIL OF LIAISON OFFI-
18 CERS.—The Secretary of Defense, the Attorney Gen-
19 eral, the Secretary of Commerce, and the Director of
20 National Intelligence shall assign personnel to the
21 Center to act as full-time liaisons.

22 “(2) OPTIONAL DETAIL OF LIAISON OFFI-
23 CERS.—The head of any Federal agency not de-
24 scribed in paragraph (1), with the concurrence of

1 the Director of the Center, may assign personnel to
2 the Center to act as liaisons.

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

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

10 “(k) SUFFICIENCY OF RESOURCES PLAN.—

11 “(1) REPORT.—Not later than 120 days after
12 the date of enactment of the Cybersecurity Act of
13 2012, the Director of the Office of Management and
14 Budget shall submit to the appropriate committees
15 of Congress and the Comptroller General of the
16 United States a report on the resources and staff
17 necessary to carry out fully the responsibilities under
18 this subtitle, including the availability of existing re-
19 sources and staff.

20 “(2) COMPTROLLER GENERAL REVIEW.—The
21 Comptroller General of the United States shall
22 evaluate the reasonableness and adequacy of the re-
23 port submitted by the Director of the Office of Man-
24 agement and Budget under paragraph (1) and sub-

1 mit to the appropriate committees of Congress a re-
2 port regarding the same.

3 “(1) NO RIGHT OR BENEFIT.—The provision of as-
4 sistance or information under this section to governmental
5 or private entities that own or operate critical infrastruc-
6 ture shall be at the discretion of the Secretary. The provi-
7 sion of certain assistance or information to a governmental
8 or private entity pursuant to this section shall not create
9 a right or benefit, substantive or procedural, to similar
10 assistance or information for any other governmental or
11 private entity.

12 **“SEC. 243. DEPARTMENT OF HOMELAND SECURITY INFOR-**
13 **MATION SHARING.**

14 “(a) IN GENERAL.—

15 “(1) ASSESSMENT.—Not later than 180 days
16 after the date of enactment of the Cybersecurity Act
17 of 2012, the Director of the Center, in consultation
18 with the private sector, relevant government agen-
19 cies, and nongovernmental organizations, shall con-
20 duct an assessment of existing and proposed infor-
21 mation sharing models to identify best practices for
22 sharing information across government and with the
23 private sector, including through cybersecurity ex-
24 changes designated pursuant to section 703 of the
25 Cybersecurity Act of 2012.

1 “(2) INFORMATION SHARING.—The Director of
2 the Center shall periodically review procedures estab-
3 lished under subsection (b) and the program estab-
4 lished in accordance with subsection (c) to ensure
5 that classified and unclassified cybersecurity infor-
6 mation, including information relating to threats,
7 vulnerabilities, traffic, trends, incidents, and other
8 anomalous activities affecting the Federal informa-
9 tion infrastructure, national information infrastruc-
10 ture, or information systems, are being appropriately
11 shared between and among appropriate Federal and
12 non-Federal entities, including Federal cybersecurity
13 centers, Federal and non-Federal network and secu-
14 rity operations centers, cybersecurity exchanges, and
15 non-Federal entities responsible for such information
16 systems.

17 “(b) FEDERAL AGENCIES.—

18 “(1) INFORMATION SHARING PROGRAM.—The
19 Director of the Center, in consultation with the
20 members of the Chief Information Officers Council
21 established under section 3603 of title 44, United
22 States Code, shall establish a program for sharing
23 information with and between the Center and other
24 Federal agencies that includes processes and proce-
25 dures—

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

14 “(B) under which Federal agencies provide
15 the Director of the Center, upon request, with
16 information concerning the security of the Fed-
17 eral information infrastructure, information in-
18 frastructure that is owned, operated, controlled,
19 or licensed for use by, or on behalf of, the De-
20 partment of Defense, a military department, or
21 another element of the intelligence community,
22 or the national information infrastructure nec-
23 essary to carry out the duties of the Director of
24 the Center under this subtitle or any other pro-
25 vision of law.

1 “(2) ACCESS TO INFORMATION.—

2 “(A) IN GENERAL.—The Director of the
3 Center shall ensure—

4 “(i) that the head of each Federal
5 agency has timely access to data, including
6 appropriate raw and processed data, re-
7 garding the information infrastructure of
8 the Federal agency; and

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

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

21 “(C) IMMEDIATE NOTIFICATION RE-
22 QUIRED.—Unless otherwise directed by the
23 President, any Federal agency with a national
24 security system shall, consistent with the level
25 of the risk, immediately notify the Director of

1 the Center regarding any incident affecting the
2 security of a national security system.

3 “(c) PRIVATE SECTOR, STATE AND LOCAL GOVERN-
4 MENTS, AND INTERNATIONAL PARTNERS.—

5 “(1) INFORMATION SHARING PROGRAM.—The
6 Director of the Center shall establish a program for
7 sharing cybersecurity threat and vulnerability infor-
8 mation in support of activities under section
9 242(e)(1) between the Center, cybersecurity ex-
10 changes designated pursuant to section 703 of the
11 Cybersecurity Act of 2012, State and local govern-
12 ments, the private sector, and international partners,
13 which shall include processes and procedures that—

14 “(A) expand and enhance the sharing of
15 timely and actionable cybersecurity threat and
16 vulnerability information by the Federal Gov-
17 ernment with owners and operators of the na-
18 tional information infrastructure;

19 “(B) establish criteria under which owners
20 or operators of covered critical infrastructure
21 information systems shall share information
22 about incidents affecting covered critical infra-
23 structure, and other relevant data with the Fed-
24 eral Government;

1 “(C) ensure voluntary information sharing
2 with and from the private sector, State and
3 local governments, and international partners of
4 the United States on—

5 “(i) cybersecurity threats,
6 vulnerabilities, incidents, and anomalous
7 activities affecting the national information
8 infrastructure; and

9 “(ii) means and methods of identi-
10 fying, preventing, responding to, mitigating
11 and remediating cybersecurity threats, and
12 vulnerabilities;

13 “(D) establish a method of accessing clas-
14 sified or unclassified information, as appro-
15 priate and in accordance with applicable laws
16 protecting trade secrets, that will provide situa-
17 tional awareness of the security of the Federal
18 information infrastructure and the national in-
19 formation infrastructure relating to cybersecu-
20 rity threats, and vulnerabilities, including traf-
21 fic, trends, incidents, damage, and other anom-
22 alous activities affecting the Federal informa-
23 tion infrastructure or the national information
24 infrastructure;

1 “(E) establish guidance on the form, con-
2 tent, and priority of incident reports that shall
3 be submitted under subsection (c)(1)(B), which
4 shall—

5 “(i) include appropriate mechanisms
6 to protect personally identifiable informa-
7 tion; and

8 “(ii) prioritize the reporting of inci-
9 dents based on the risk the incident poses
10 to the disruption of the reliable operation
11 of the covered critical infrastructure; and

12 “(F) establish a procedure for notifying an
13 information technology provider if a vulner-
14 ability is detected in the product or service pro-
15 duced by the information technology provider
16 and, where possible, working with the informa-
17 tion technology provider to remediate the vul-
18 nerability before any public disclosure of the
19 vulnerability so as to minimize the opportunity
20 for the vulnerability to be exploited.

21 “(2) COORDINATION.—In carrying out the du-
22 ties under this subsection, the Director of the Center
23 shall coordinate, as appropriate, with Federal and
24 non-Federal entities engaged in similar information
25 sharing efforts.

1 “(3) EVALUATION OF ACCESS TO CLASSIFIED
2 INFORMATION.—The Director of the Center, in co-
3 ordination with the Director of National Intelligence,
4 shall conduct an annual evaluation of the sufficiency
5 of access to classified information by owners and op-
6 erators of national information infrastructure.

7 “(4) EVALUATION.—The Director of the Center
8 shall create and promote a mechanism for owners
9 and operators of national information infrastructure
10 to provide feedback about the operations of the Cen-
11 ter and recommendations for improvements of the
12 Center, including recommendations to improve the
13 sharing of classified and unclassified information.

14 “(5) GUIDELINES.—The Director of the Center,
15 in consultation with the Attorney General, the Direc-
16 tor of National Intelligence, and the Privacy Officer
17 established under section 242(j), shall develop guide-
18 lines to protect the privacy and civil liberties of
19 United States persons and intelligence sources and
20 methods, while carrying out this subsection.

21 “(d) VOLUNTARILY SHARED INFORMATION.—Cov-
22 ered information, as defined in section 107 of the Cyberse-
23 curity Act of 2012, submitted to the Center in accordance
24 with this subtitle shall be treated as voluntarily shared
25 critical infrastructure information under section 214, ex-

1 cept that the requirement of section 214 that the informa-
2 tion be voluntarily submitted, including the requirement
3 for an express statement, shall not be required for submis-
4 sions of covered information.

5 “(e) LIMITATION ON USE OF VOLUNTARILY SUB-
6 MITTED INFORMATION FOR REGULATORY ENFORCEMENT
7 ACTIONS.—A Federal entity may not use information sub-
8 mitted under this subtitle as evidence in a regulatory en-
9 forcement action against the individual or entity that law-
10 fully submitted the information.

11 **“SEC. 244. ACCESS TO INFORMATION.**

12 “Unless otherwise directed by the President—

13 “(1) the Director of the Center shall have ac-
14 cess to, receive, and analyze law enforcement infor-
15 mation, intelligence information, terrorism informa-
16 tion, and any other information in the possession of
17 Federal agencies relevant to the security of the Fed-
18 eral information infrastructure, information infra-
19 structure that is owned, operated, controlled, or li-
20 censed for use by, or on behalf of, the Department
21 of Defense, a military department, or another ele-
22 ment of the intelligence community, or national in-
23 formation infrastructure and, consistent with appli-
24 cable law, may also receive such information, from
25 State and local governments (including law enforce-

1 ment agencies), and private entities, including infor-
2 mation provided by any contractor to a Federal
3 agency regarding the security of the agency informa-
4 tion infrastructure; and

5 “(2) any Federal agency in possession of law
6 enforcement information, intelligence information,
7 terrorism information, or any other information rel-
8 evant to the security of the Federal information in-
9 frastructure, information infrastructure that is
10 owned, operated, controlled, or licensed for use by,
11 or on behalf of, the Department of Defense, a mili-
12 tary department, or another element of the intel-
13 ligence community, or national information infra-
14 structure shall provide that information to the Di-
15 rector of the Center in a timely manner.

16 **“SEC. 245. NATIONAL CENTER FOR CYBERSECURITY AND**
17 **COMMUNICATIONS ACQUISITION AUTHORI-**
18 **TIES.**

19 “(a) IN GENERAL.—The National Center for Cyber-
20 security and Communications is authorized to use the au-
21 thorities under subsections (c)(1) and (d)(1)(B) of section
22 2304 of title 10, United States Code, instead of the au-
23 thorities under subsections (a)(1) and (b)(2) of section
24 3304 of title 41, United States Code, subject to all other

1 requirements of sections 3301 and 3304 of title 41, United
2 States Code.

3 “(b) GUIDELINES.—Not later than 90 days after the
4 date of enactment of the Cybersecurity Act of 2012, the
5 chief procurement officer of the Department of Homeland
6 Security shall issue guidelines for use of the authority
7 under subsection (a).

8 “(c) TERMINATION.—The National Center for Cyber-
9 security and Communications may not use the authority
10 under subsection (a) on and after the date that is 3 years
11 after the date of enactment of this Act.

12 “(d) REPORTING.—

13 “(1) IN GENERAL.—On a semiannual basis, the
14 Director of the Center shall submit a report on use
15 of the authority granted by subsection (a) to—

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

18 “(B) the Committee on Homeland Security
19 of the House of Representatives.

20 “(2) CONTENTS.—Each report submitted under
21 paragraph (1) shall include, at a minimum—

22 “(A) the number of contract actions taken
23 under the authority under subsection (a) during
24 the period covered by the report; and

1 “(B) for each contract action described in
2 subparagraph (A)—

3 “(i) the total dollar value of the con-
4 tract action;

5 “(ii) a summary of the market re-
6 search conducted by the National Center
7 for Cybersecurity and Communications, in-
8 cluding a list of all offerors who were con-
9 sidered and those who actually submitted
10 bids, in order to determine that use of the
11 authority was appropriate; and

12 “(iii) a copy of the justification and
13 approval documents required by section
14 3304(e) of title 41, United States Code.

15 “(3) CLASSIFIED ANNEX.—A report submitted
16 under this subsection shall be submitted in an un-
17 classified form, but may include a classified annex,
18 if necessary.

19 **“SEC. 246. RECRUITMENT AND RETENTION PROGRAM FOR**
20 **THE NATIONAL CENTER FOR CYBERSECU-**
21 **RITY AND COMMUNICATIONS.**

22 “(a) DEFINITIONS.—In this section:

23 “(1) COLLECTIVE BARGAINING AGREEMENT.—
24 The term ‘collective bargaining agreement’ has the

1 meaning given that term in section 7103(a)(8) of
2 title 5, United States Code.

3 “(2) QUALIFIED EMPLOYEE.—The term ‘quali-
4 fied employee’ means an employee who performs
5 functions relating to the security of Federal systems
6 and critical information infrastructure.

7 “(b) GENERAL AUTHORITY.—

8 “(1) ESTABLISH POSITIONS, APPOINT PER-
9 SONNEL, AND FIX RATES OF PAY.—The Secretary
10 may exercise with respect to qualified employees of
11 the Department the same authority of that the Sec-
12 retary of Defense has with respect to civilian intel-
13 ligence personnel under sections 1601, 1602, and
14 1603 of title 10, United States Code, to establish as
15 positions in the excepted service, to appoint individ-
16 uals to those positions, and fix pay. Such authority
17 shall be exercised subject to the same conditions and
18 limitations applicable to the Secretary of Defense
19 with respect to civilian intelligence personnel of the
20 Department of Defense.

21 “(2) SCHOLARSHIP PROGRAM.—The Secretary
22 may exercise with respect to qualified employees of
23 the Department the same authority of the Secretary
24 of Defense has with respect to civilian personnel
25 under section 2200a of title 10, United States Code,

1 to the same extent, and subject to the same condi-
2 tions and limitations, that the Secretary of Defense
3 may exercise such authority with respect to civilian
4 personnel of the Department of Defense.

5 “(3) PLAN FOR EXECUTION OF AUTHORI-
6 TIES.—Not later than 120 days after the date of en-
7 actment of this subtitle, the Secretary shall submit
8 a report to the appropriate committees of Congress
9 with a plan for the use of the authorities provided
10 under this subsection.

11 “(4) COLLECTIVE BARGAINING AGREEMENTS.—
12 Nothing in paragraph (1) may be construed to im-
13 pair the continued effectiveness of a collective bar-
14 gaining agreement with respect to an office, compo-
15 nent, subcomponent, or equivalent of the Depart-
16 ment that is a successor to an office, component,
17 subcomponent, or equivalent of the Department cov-
18 ered by the agreement before the succession.

19 “(5) REQUIRED REGULATIONS.—The Secretary,
20 in coordination with the Director of the Center and
21 the Director of the Office of Personnel Management,
22 shall prescribe regulations for the administration of
23 this section.

24 “(c) MERIT SYSTEM PRINCIPLES AND CIVIL SERV-
25 ICE PROTECTIONS: APPLICABILITY.—

1 “(1) APPLICABILITY OF MERIT SYSTEM PRIN-
2 CIPLES.—The Secretary shall exercise the authority
3 under subsection (b) in a manner consistent with the
4 merit system principles set forth in section 2301 of
5 title 5, United States Code.

6 “(2) CIVIL SERVICE PROTECTIONS.—Section
7 1221, section 2302, and chapter 75 of title 5,
8 United States Code, shall apply to the positions es-
9 tablished under subsection (b)(1).

10 “(d) REQUIREMENTS.—Before the initial exercise of
11 any authority authorized under subsection (b)(1) the Sec-
12 retary shall—

13 “(1) seek input from affected employees, and
14 the union representatives of affected employees as
15 applicable, and Federal manager and professional
16 associations into the design and implementation of a
17 fair, credible, and transparent system for exercising
18 any authority under subsection (b)(1);

19 “(2) make a good faith attempt to resolve any
20 employee concerns regarding proposed changes in
21 conditions of employment through discussions with
22 the groups described in paragraph (1);

23 “(3) develop a program to provide training to
24 supervisors of cybersecurity employees at the De-
25 partment on the use of the new authorities, includ-

1 ing actions, options, and strategies a supervisor may
2 use in—

3 “(A) developing and discussing relevant
4 goals and objectives with the employee, commu-
5 nicating and discussing progress relative to per-
6 formance goals and objectives, and conducting
7 performance appraisals;

8 “(B) mentoring and motivating employees,
9 and improving employee performance and pro-
10 ductivity;

11 “(C) fostering a work environment charac-
12 terized by fairness, respect, equal opportunity,
13 and attention to the quality of work of the em-
14 ployees;

15 “(D) effectively managing employees with
16 unacceptable performance;

17 “(E) addressing reports of a hostile work
18 environment, reprisal, or harassment of or by
19 another supervisor or employee; and

20 “(F) otherwise carrying out the duties and
21 responsibilities of a supervisor;

22 “(4) develop a program to provide training to
23 supervisors of cybersecurity employees at the De-
24 partment on the prohibited personnel practices
25 under section 2302 of title 5, United States Code,

1 (particularly with respect to the practices described
2 in paragraphs (1) and (8) of section 2302(b) of title
3 5, United States Code), employee collective bar-
4 gaining and union participation rights, and the pro-
5 cedures and processes used to enforce employee
6 rights; and

7 “(5) develop a program under which experi-
8 enced supervisors mentor new supervisors by—

9 “(A) sharing knowledge and advice in
10 areas such as communication, critical thinking,
11 responsibility, flexibility, motivating employees,
12 teamwork, leadership, and professional develop-
13 ment; and

14 “(B) pointing out strengths and areas for
15 development.

16 “(e) SUPERVISOR REQUIREMENT.—

17 “(1) IN GENERAL.—Except as provided in para-
18 graph (2), not later than 1 year after the date of en-
19 actment of the Cybersecurity Act of 2012 and every
20 3 years thereafter, every supervisor of cybersecurity
21 employees at the Department shall complete the pro-
22 grams established under paragraphs (3) and (4) of
23 subsection (d).

24 “(2) EXCEPTION.—A supervisor of cybersecu-
25 rity employees at the Department who is appointed

1 after the date of enactment of the Cybersecurity Act
2 of 2012 shall complete the programs established
3 under paragraphs (3) and (4) of subsection (d) not
4 later than 1 year after the date on which the super-
5 visor is appointed to the position, and every 3 years
6 thereafter.

7 “(3) ONGOING PARTICIPATION.—Participation
8 by supervisors of cybersecurity employees at the De-
9 partment in the program established under sub-
10 section (d)(5) shall be ongoing.

11 “(f) CONVERSION TO COMPETITIVE SERVICE.—In
12 consultation with the Director of the Center, the Secretary
13 may grant competitive civil service status to a qualified
14 employee appointed to the excepted service under sub-
15 section (b) if that employee is employed in the Center or
16 is transferring to the Center.

17 “(g) ANNUAL REPORT.—Not later than 1 year after
18 the date of enactment of this subtitle, and every year
19 thereafter for 4 years, the Secretary shall submit to the
20 appropriate committees of Congress a detailed report
21 that—

22 “(1) discusses the process used by the Sec-
23 retary in accepting applications, assessing can-
24 didates, ensuring adherence to veterans’ preference,

1 and selecting applicants for vacancies to be filled by
2 a qualified employee;

3 “(2) describes—

4 “(A) how the Secretary plans to fulfill the
5 critical need of the Department to recruit and
6 retain qualified employees;

7 “(B) the measures that will be used to
8 measure progress; and

9 “(C) any actions taken during the report-
10 ing period to fulfill such critical need;

11 “(3) discusses how the planning and actions
12 taken under paragraph (2) are integrated into the
13 strategic workforce planning of the Department;

14 “(4) provides metrics on actions occurring dur-
15 ing the reporting period, including—

16 “(A) the number of qualified employees
17 hired by occupation and grade and level or pay
18 band;

19 “(B) the total number of veterans hired;

20 “(C) the number of separations of qualified
21 employees by occupation and grade and level or
22 pay band;

23 “(D) the number of retirements of quali-
24 fied employees by occupation and grade and
25 level or pay band; and

1 “(E) the number and amounts of recruit-
2 ment, relocation, and retention incentives paid
3 to qualified employees by occupation and grade
4 and level or pay band.

5 **“SEC. 247. PROHIBITED CONDUCT.**

6 “None of the authorities provided under this subtitle
7 shall authorize the Director of the Center, the Center, the
8 Department, or any other Federal entity to—

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

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

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.) is amended by
 2 inserting after the item relating to section 237 the fol-
 3 lowing:

“Subtitle E—Cybersecurity

“Sec. 241. Definitions.

“Sec. 242. Consolidation of existing resources.

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

“Sec. 244. Access to information.

“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.

“Sec. 247. Prohibited conduct.”.

4 **TITLE IV—EDUCATION, RE-**
 5 **CRUITMENT, AND WORK-**
 6 **FORCE DEVELOPMENT**

7 **SEC. 401. DEFINITIONS.**

8 In this title:

9 (1) **CYBERSECURITY MISSION.**—The term “cy-
 10 bersecurity mission” means activities that encom-
 11 pass the full range of threat reduction, vulnerability
 12 reduction, deterrence, international engagement, in-
 13 cident response, resiliency, and recovery policies and
 14 activities, including computer network operations, in-
 15 formation assurance, law enforcement, diplomacy,
 16 military, and intelligence missions as such activities
 17 relate to the security and stability of cyberspace.

18 (2) **CYBERSECURITY MISSION OF A FEDERAL**
 19 **AGENCY.**—The term “cybersecurity mission of a
 20 Federal agency” means the portion of a cybersecu-

1 rity mission that is the responsibility of a Federal
2 agency.

3 **SEC. 402. NATIONAL EDUCATION AND AWARENESS CAM-**
4 **PAIGN.**

5 (a) IN GENERAL.—The Secretary, in consultation
6 with appropriate Federal agencies shall develop and imple-
7 ment outreach and awareness programs on cybersecurity,
8 including—

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

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

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

23 (2) in coordination with the Secretary of Com-
24 merce, development of a program to publicly recog-
25 nize or identify products, services, and companies,

1 including owners and operators, that meet the high-
2 est standards of cybersecurity.

3 (b) CONSIDERATIONS.—In carrying out the authority
4 described in subsection (a), the Secretary of Commerce,
5 the Secretary, and the Director of the National Institute
6 of Standards and Technology shall leverage existing pro-
7 grams designed to inform the public of safety and security
8 of products or services, including self-certifications and
9 independently-verified assessments regarding the quan-
10 tification and valuation of information security risk.

11 **SEC. 403. NATIONAL CYBERSECURITY COMPETITION AND**
12 **CHALLENGE.**

13 (a) TALENT COMPETITION AND CHALLENGE.—

14 (1) IN GENERAL.—The Secretary of Homeland
15 Security and the Secretary of Commerce shall estab-
16 lish a program to conduct competitions and chal-
17 lenges and ensure the effective operation of national
18 and statewide competitions and challenges that seek
19 to identify, develop, and recruit talented individuals
20 to work in Federal agencies, State and local govern-
21 ment agencies, and the private sector to perform du-
22 ties relating to the security of the Federal informa-
23 tion infrastructure or the national information infra-
24 structure.

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

4 (A) students enrolled in grades 9 through
5 12;

6 (B) students enrolled in a postsecondary
7 program of study leading to a baccalaureate de-
8 gree at an institution of higher education;

9 (C) students enrolled in a
10 postbaccalaureate program of study leading to
11 an institution of higher education;

12 (D) institutions of higher education and
13 research institutions;

14 (E) veterans; and

15 (F) other groups or individuals as the Sec-
16 retary of Homeland Security and the Secretary
17 of Commerce determine appropriate.

18 (3) SUPPORT OF OTHER COMPETITIONS AND
19 CHALLENGES.—The program established under
20 paragraph (1) may support other competitions and
21 challenges not established under this subsection
22 through affiliation and cooperative agreements
23 with—

24 (A) Federal agencies;

1 (B) regional, State, or school programs
2 supporting the development of cyber profes-
3 sionals;

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

5 (D) other private sector organizations.

6 (4) AREAS OF TALENT.—The program estab-
7 lished under paragraph (1) shall seek to identify, de-
8 velop, and recruit exceptional talent relating to—

9 (A) ethical hacking;

10 (B) penetration testing;

11 (C) vulnerability assessment;

12 (D) continuity of system operations;

13 (E) cyber forensics;

14 (F) offensive and defensive cyber oper-
15 ations; and

16 (G) other areas to fulfill the cybersecurity
17 mission as the Director determines appropriate.

18 (5) INTERNSHIPS.—The Director of the Office
19 of Personnel Management shall establish, in coordi-
20 nation with the Director of the National Center for
21 Cybersecurity and Communications, a program to
22 provide, where appropriate, internships or other
23 work experience in the Federal government to the
24 winners of the competitions and challenges.

1 (b) NATIONAL RESEARCH AND DEVELOPMENT COM-
2 PETITION AND CHALLENGE.—

3 (1) IN GENERAL.—The Director of the National
4 Science Foundation, in consultation with appropriate
5 Federal agencies, shall establish a program of cyber-
6 security competitions and challenges to stimulate in-
7 novation in basic and applied cybersecurity research,
8 technology development, and prototype demonstra-
9 tion that has the potential for application to the in-
10 formation technology activities of the Federal Gov-
11 ernment.

12 (2) PARTICIPATION.—Participants in the com-
13 petitions and challenges of the program established
14 under paragraph (1) shall include—

15 (A) students enrolled in grades 9 through
16 12;

17 (B) students enrolled in a postsecondary
18 program of study leading to a baccalaureate de-
19 gree at an institution of higher education;

20 (C) students enrolled in a
21 postbaccalaureate program of study leading to
22 an institution of higher education;

23 (D) institutions of higher education and
24 research institutions;

25 (E) veterans; and

1 (F) other groups or individuals as the Di-
2 rector of the National Science Foundation de-
3 termines appropriate.

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

7 (A) shall consult widely both within and
8 outside the Federal Government; and

9 (B) may empanel advisory committees.

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

18 **SEC. 404. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
19 **PROGRAM.**

20 (a) IN GENERAL.—The Director of the National
21 Science Foundation, in coordination with the Secretary,
22 shall establish a Federal Cyber Scholarship-for-Service
23 program to recruit and train the next generation of infor-
24 mation technology professionals, industry control system
25 security professionals, and security managers to meet the

1 needs of the cybersecurity mission for the Federal Govern-
2 ment and State, local, and tribal governments.

3 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

4 The program established under subsection (a) shall—

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

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

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

23 (4) provide a procedure by which the National
24 Science Foundation or a Federal agency may, con-
25 sistent with regulations of the Office of Personnel

1 Management, request and fund security clearances
2 for scholarship recipients, including providing for
3 clearances during summer internships and after the
4 recipient receives the degree; and

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

9 (c) HIRING AUTHORITY.—

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

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

18 (B) exempt from competitive service.

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

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

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

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

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

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

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

22 **SEC. 405. ASSESSMENT OF CYBERSECURITY FEDERAL**
23 **WORKFORCE.**

24 (a) IN GENERAL.—The Director of the Office of Per-
25 sonnel Management and the Secretary, in coordination

1 with the Director of National Intelligence, the Secretary
2 of Defense, and the Chief Information Officers Council es-
3 tablished under section 3603 of title 44, United States
4 Code, shall assess the readiness and capacity of the Fed-
5 eral workforce to meet the needs of the cybersecurity mis-
6 sion of the Federal Government.

7 (b) STRATEGY.—

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

18 (2) CONTENTS.—The strategy developed under
19 paragraph (1) shall include—

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

22 (B) a 10-year projections of Federal work-
23 force needs.

24 (c) UPDATES.—The Director of the Office of Per-
25 sonnel Management, in consultation with the Director of

1 the National Center for Cybersecurity and Communica-
2 tions and the Director of the Office of Management and
3 Budget, shall update the strategy developed under sub-
4 section (b) as needed.

5 **SEC. 406. FEDERAL CYBERSECURITY OCCUPATION CLASSI-**
6 **FICATIONS.**

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

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

19 **SEC. 407. TRAINING AND EDUCATION.**

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

23 (b) TRAINING.—

24 (1) FEDERAL GOVERNMENT EMPLOYEES AND
25 FEDERAL CONTRACTORS.—The Director of the Of-

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

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

13 (A) role-based security awareness training;

14 (B) recommended cybersecurity practices;

15 (C) cybersecurity recommendations for
16 traveling abroad;

17 (D) unclassified counterintelligence infor-
18 mation;

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

21 (F) information regarding malicious activ-
22 ity online;

23 (G) information regarding cybersecurity
24 and law enforcement;

25 (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 ecutive 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) EDUCATION.—

12 (1) FEDERAL EMPLOYEES.—The Director of
13 the Office of Personnel Management, in coordination
14 with the Secretary of Education, the Director of the
15 National Science Foundation, and the Director of
16 the National Center for Cybersecurity and Commu-
17 nications, shall develop and implement a strategy to
18 provide Federal employees who work in cybersecurity
19 missions with the opportunity to obtain additional
20 education.

21 (2) K THROUGH 12 EDUCATION.—The Sec-
22 retary of Education, in coordination with the Direc-
23 tor of the National Center for Cybersecurity and
24 Communications and State and local governments,
25 shall develop model curriculum standards, guide-

1 lines, and recommended courses to address cyber
2 safety, cybersecurity, and cyber ethics for students
3 in kindergarten through grade 12.

4 (3) INSTITUTIONS OF HIGHER EDUCATION AND
5 CAREER AND TECHNICAL INSTITUTIONS.—

6 (A) SECRETARY OF EDUCATION.—The
7 Secretary of Education, in coordination with
8 the Secretary, and after consultation with ap-
9 propriate private entities, shall—

10 (i) develop model curriculum stand-
11 ards and guidelines to address cyber safe-
12 ty, cybersecurity, and cyber ethics for all
13 students enrolled in institutions of higher
14 education, and all students enrolled in ca-
15 reer and technical institutions, in the
16 United States; and

17 (ii) analyze and develop recommended
18 courses for students interested in pursuing
19 careers in information technology, commu-
20 nications, computer science, engineering,
21 mathematics, and science, as those sub-
22 jects relate to cybersecurity.

23 (B) OFFICE OF PERSONNEL MANAGE-
24 MENT.—The Director of the Office of Personnel
25 Management, in coordination with the Director

1 of the National Center for Cybersecurity and
2 Communications, shall develop strategies and
3 programs—

4 (i) to recruit students enrolled in in-
5 stitutions of higher education, and stu-
6 dents enrolled in career and technical insti-
7 tutions in the United States to serve as
8 Federal employees engaged in cybersecu-
9 rity missions; and

10 (ii) that provide internship and part-
11 time work opportunities with the Federal
12 Government for students enrolled in insti-
13 tutions of higher education and career and
14 technical institutions in the United States.

15 **SEC. 408. CYBERSECURITY INCENTIVES.**

16 The head of each Federal agency shall adopt best
17 practices, developed by the Office of Personnel Manage-
18 ment, regarding effective ways to educate and motivate
19 employees of the Federal Government to demonstrate
20 leadership in cybersecurity, including—

21 (1) promotions and other nonmonetary awards;

22 and

23 (2) publicizing information sharing accomplish-
24 ments by individual employees and, if appropriate,
25 the tangible benefits that resulted.

1 **TITLE V—RESEARCH AND**
2 **DEVELOPMENT**

3 **SEC. 501. FEDERAL CYBERSECURITY RESEARCH AND DE-**
4 **VELOPMENT.**

5 (a) **FUNDAMENTAL CYBERSECURITY RESEARCH.—**

6 The Director of the Office of Science and Technology Pol-
7 icy (referred to in this section as the “Director”), in co-
8 ordination with the Secretary and the head of any relevant
9 Federal agency, shall develop a national cybersecurity re-
10 search and development plan.

11 (b) **REQUIREMENTS.—**The plan required to be devel-
12 oped under subsection (a) shall encourage computer and
13 information science and engineering research to meet chal-
14 lenges in cybersecurity, including—

15 (1) how to design and build complex software-
16 intensive systems that are secure and reliable when
17 first deployed;

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

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

24 (4) how to guarantee the privacy of the iden-
25 tity, information, or lawful transactions of an indi-

1 vidual when stored in distributed systems or trans-
2 mitted over networks;

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

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

8 (7) how to support privacy in conjunction with
9 improved security;

10 (8) how to address the growing problem of in-
11 sider threat; and

12 (9) how improved consumer education and dig-
13 ital literacy initiatives can address human factors
14 that contribute to cybersecurity.

15 (c) SECURE CODING RESEARCH.—The Director shall
16 support research—

17 (1) that evaluates selected secure coding edu-
18 cation and improvement programs; and

19 (2) of new methods of integrating secure coding
20 improvement into the core curriculum of computer
21 science programs and of other programs where grad-
22 uates of such programs have a substantial prob-
23 ability of developing software after graduation.

24 (d) ASSESSMENT OF SECURE CODING EDUCATION IN
25 COLLEGES AND UNIVERSITIES.—

1 (1) REPORT.—Not later than 1 year after the
2 date of enactment of this Act, the Director shall
3 submit to the Committee on Commerce, Science, and
4 Transportation of the Senate and the Committee on
5 Science and Technology of the House of Representa-
6 tives a report on the state of secure coding education
7 in institutions of higher education of the United
8 States for each institution that received National
9 Science Foundation funding in excess of \$1,000,000
10 during fiscal year 2011.

11 (2) CONTENTS OF REPORT.—The report re-
12 quired under paragraph (1) shall include—

13 (A) the number of students who earned
14 baccalaureate degrees in computer science or in
15 each other program where graduates have a
16 substantial probability of being engaged in soft-
17 ware design or development after graduation;

18 (B) the percentage of the students de-
19 scribed in subparagraph (A) who completed
20 substantive secure coding education or improve-
21 ment programs during their undergraduate ex-
22 perience; and

23 (C) descriptions of the length and content
24 of the education and improvement programs
25 and an evaluation of the effectiveness of those

1 programs based on the students' scores on
2 standard tests of secure coding and design
3 skills.

4 (e) 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.

9 (2) ESTABLISHMENT OF PROGRAM.—

10 (A) IN GENERAL.—Based on the results of
11 the review conducted under paragraph (1), the
12 Director shall establish a program to award
13 grants to institutions of higher education to es-
14 tablish cybersecurity test beds capable of real-
15 istic modeling of real-time cyber attacks and de-
16 fenses.

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

22 (3) PURPOSE.—The purpose of the program es-
23 tablished under paragraph (2) shall be to support
24 the rapid development of new cybersecurity defenses,
25 techniques, and processes by improving under-

1 standing and assessing the latest technologies in a
2 real-world environment.

3 (f) COORDINATION WITH OTHER RESEARCH INITIA-
4 TIVES.—The Director shall—

5 (1) ensure that the research and development
6 program carried out under this section is consistent
7 with any strategy to increase the security and resil-
8 ience of cyberspace; and

9 (2) to the extent practicable, coordinate re-
10 search and development activities with other ongoing
11 research and development security-related initiatives,
12 including research being conducted by—

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

15 (B) the Department;

16 (C) the National Academy of Sciences;

17 (D) other Federal agencies;

18 (E) other Federal and private research lab-
19 oratories, research entities, and universities and
20 institutions of higher education, and relevant
21 nonprofit organizations; and

22 (F) international partners of the United
23 States.

24 (g) NSF COMPUTER AND NETWORK SECURITY RE-
25 SEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Se-

1 curity Research and Development Act (15 U.S.C.
2 7403(a)(1)) is amended—

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

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

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

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

11 “(K) secure software engineering and soft-
12 ware assurance, including—

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

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

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

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

25 “(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; and

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

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

17 (i) NETWORKING AND INFORMATION TECHNOLOGY
18 RESEARCH AND DEVELOPMENT PROGRAM.—Section
19 204(a)(1) of the High-Performance Computing Act of
20 1991 (15 U.S.C. 5524(a)(1)) is amended—

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

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

24 “(D) develop and propose standards and
25 guidelines, and develop measurement techniques

1 and test methods, for enhanced cybersecurity
2 for computer networks and common user inter-
3 faces to systems; and”.

4 **SEC. 502. HOMELAND SECURITY CYBERSECURITY RE-**
5 **SEARCH AND DEVELOPMENT.**

6 Subtitle D of title II of the Homeland Security Act
7 of 2002 (6 U.S.C. 161 et seq.) is amended by adding at
8 the end the following:

9 **“SEC. 238. CYBERSECURITY RESEARCH AND DEVELOP-**
10 **MENT.**

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

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

21 “(1) advance the development and accelerate
22 the deployment of more secure versions of funda-
23 mental Internet protocols and architectures, includ-
24 ing for the secure domain name addressing system
25 and routing security;

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

4 “(3) improve and create mitigation and recov-
5 ery methodologies, including techniques for contain-
6 ment of attacks and development of resilient net-
7 works and systems;

8 “(4) develop and support infrastructure and
9 tools to support cybersecurity research and develop-
10 ment efforts, including modeling, test beds, and data
11 sets for assessment of new cybersecurity tech-
12 nologies;

13 “(5) assist the development and support of
14 technologies to reduce vulnerabilities in process con-
15 trol systems;

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

18 “(7) test, evaluate, and facilitate, with appro-
19 priate protections for any proprietary information
20 concerning the technologies, the transfer of tech-
21 nologies associated with the engineering of less vul-
22 nerable software and securing the information tech-
23 nology software development lifecycle;

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

1 “(9) assist the development of technologies de-
2 signed to increase the security and resiliency of tele-
3 communications networks;

4 “(10) advance the protection of privacy and
5 civil liberties in cybersecurity technology and prac-
6 tices; and

7 “(11) address other risks identified by the Di-
8 rector of the National Center for Cybersecurity and
9 Communications.

10 “(c) COORDINATION WITH OTHER RESEARCH INI-
11 TIATIVES.—The Under Secretary for Science and Tech-
12 nology—

13 “(1) shall ensure that the research and develop-
14 ment program carried out under subsection (a) is
15 consistent with any strategy to increase the security
16 and resilience of cyberspace;

17 “(2) shall, to the extent practicable, coordinate
18 the research and development activities of the De-
19 partment with other ongoing research and develop-
20 ment security-related initiatives, including research
21 being conducted by—

22 “(A) the National Institute of Standards
23 and Technology;

24 “(B) the National Science Foundation;

25 “(C) the National Academy of Sciences;

1 “(D) other Federal agencies;

2 “(E) other Federal and private research
3 laboratories, research entities, and universities
4 and institutions of higher education, and rel-
5 evant nonprofit organizations; and

6 “(F) international partners of the United
7 States;

8 “(3) shall carry out any research and develop-
9 ment project under subsection (a) through a reim-
10 bursable agreement with an appropriate Federal
11 agency, if the Federal agency—

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

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

16 “(4) may make grants to, or enter into coopera-
17 tive agreements, contracts, other transactions, or re-
18 imburseable agreements with, the entities described in
19 paragraph (2); and

20 “(5) shall submit a report to the appropriate
21 committees of Congress on a review of the cyberse-
22 curity activities, and the capacity, of the national
23 laboratories and other research entities available to
24 the Department to determine if the establishment of

1 a national laboratory dedicated to cybersecurity re-
2 search and development is necessary.”.

3 **TITLE VI—FEDERAL ACQUISI-**
4 **TION RISK MANAGEMENT**
5 **STRATEGY**

6 **SEC. 601. FEDERAL ACQUISITION RISK MANAGEMENT**
7 **STRATEGY.**

8 (a) IN GENERAL.—The Secretary, in coordination
9 with relevant private sector and academic experts and each
10 Federal entity described in paragraphs (1) through (9) of
11 subsection (b), shall develop and periodically update an ac-
12 quisition risk management strategy designed to ensure,
13 based on mission criticality and cost effectiveness, the se-
14 curity of the Federal information infrastructure.

15 (b) COORDINATION.—In developing the acquisition
16 risk management strategy required under subsection (a),
17 the Secretary shall coordinate with—

- 18 (1) the Secretary of Defense;
- 19 (2) the Secretary of Commerce;
- 20 (3) the Secretary of State;
- 21 (4) the Director of National Intelligence;
- 22 (5) the Administrator of General Services;
- 23 (6) the Administrator for Federal Procurement
24 Policy;

1 (7) the members of the Chief Information Offi-
2 cers Council established under section 3603 of title
3 44, United States Code;

4 (8) the Chief Acquisition Officers Council estab-
5 lished under section 1311 of title 41, United States
6 Code; and

7 (9) the Chief Financial Officers Council estab-
8 lished under section 302 of the Chief Financial Offi-
9 cers Act of 1990 (31 U.S.C. 901 note).

10 (c) ELEMENTS.—The risk management strategy de-
11 veloped under subsection (a) shall—

12 (1) address risks in the acquisition of any part
13 of the Federal information infrastructure; and

14 (2) include developing processes that—

15 (A) incorporate all-source intelligence anal-
16 ysis into assessments of the integrity of the
17 supply chain for the Federal information infra-
18 structure;

19 (B) incorporate internationally recognized
20 standards, guidelines, and best practices, in-
21 cluding those developed by the private sector,
22 for supply chain integrity;

23 (C) enhance capabilities to test and evalu-
24 ate software and hardware within or for use in
25 the Federal information infrastructure, and,

1 where appropriate, make the capabilities avail-
2 able for use by the private sector;

3 (D) protect the intellectual property and
4 trade secrets of suppliers of information and
5 communications technology products and serv-
6 ices;

7 (E) share with the private sector, to the
8 fullest extent possible, the risks identified in the
9 supply chain and working with the private sec-
10 tor to mitigate those threats as identified;

11 (F) identify specific acquisition practices of
12 Federal agencies that increase risks to the sup-
13 ply chain and develop a process to provide rec-
14 ommendations for revisions to those processes;
15 and

16 (G) to the maximum extent practicable,
17 promote the ability of Federal agencies to pro-
18 cure authentic commercial off-the-shelf informa-
19 tion and communications technology products
20 and services from a diverse pool of suppliers,
21 consistent with the preferences for the acquisi-
22 tion of commercial items under section 2377 of
23 title 10, United States Code, and section 3307
24 of title 41, United States Code.

1 **SEC. 602. AMENDMENTS TO CLINGER-COHEN PROVISIONS**
2 **TO ENHANCE AGENCY PLANNING FOR INFOR-**
3 **MATION SECURITY NEEDS.**

4 Chapter 113 of title 40, United States Code, is
5 amended—

6 (1) in section 11302—

7 (A) in subsection (f), by striking “tech-
8 nology.” and inserting “technology, including
9 information technology or network information
10 security requirements.”;

11 (B) in subsection (i)—

12 (i) by inserting “, including informa-
13 tion security requirements,” after “infor-
14 mation resources management”; and

15 (ii) by adding at the end the fol-
16 lowing: “The Administrator for Federal
17 Procurement Policy, in coordination with
18 the Chief Information Officers Council and
19 the Federal Acquisition Institute, shall en-
20 sure that contracting officers and the indi-
21 viduals preparing descriptions of the Gov-
22 ernment requirements and statements of
23 work have adequate training in informa-
24 tion security requirements, including in in-
25 formation technology security contracts.”;

1 (C) in subsection (j), by adding at the end
2 the following: “The Director shall review and
3 report on possible impediments in the acquisi-
4 tion process or elsewhere that are acting to slow
5 agency uptake of the newest, most secure tech-
6 nologies.”; and

7 (D) by adding at the end the following:

8 “(1) MULTIPLE AWARD SCHEDULE FOR INFORMA-
9 TION SECURITY.—The Administrator of General Services
10 shall develop a special item number under Schedule 70
11 for information security products and services and consoli-
12 date those products and services under that special item
13 number to promote acquisition.

14 “(m) REDUCING THE USE OF COUNTERFEIT PROD-
15 UCTS.—Not later than 180 days after the date of enact-
16 ment of the Cybersecurity Act of 2012, the Director shall
17 issue guidance requiring, to the extent practicable, Federal
18 agencies to purchase information technology products only
19 through the authorized channels or distributors of a sup-
20 plier.”; and

21 (2) in section 11312(b)(3), by inserting “, in-
22 formation security improvement,” after “risk-ad-
23 justed return on investment”.

1 **TITLE VII—INFORMATION**
2 **SHARING**

3 **SEC. 701. AFFIRMATIVE AUTHORITY TO MONITOR AND DE-**
4 **FEND AGAINST CYBERSECURITY THREATS.**

5 Notwithstanding chapter 119, 121, or 206 of title 18,
6 United States Code, the Foreign Intelligence Surveillance
7 Act of 1978 (50 U.S.C. 1801 et seq.), and the Commu-
8 nications Act of 1934 (47 U.S.C. 151 et seq.), any private
9 entity may—

10 (1) monitor information systems of the entity
11 and information that is stored on, processed by, or
12 transiting the information systems for cybersecurity
13 threats;

14 (2) monitor a third party's information systems
15 and information that is stored on, processed by, or
16 transiting the information systems for cybersecurity
17 threats, if the third party lawfully authorizes the
18 monitoring;

19 (3) operate countermeasures on information
20 systems of the entity to protect the information sys-
21 tems and information that is stored on, processed
22 by, or transiting the information systems; and

23 (4) operate countermeasures on a third party's
24 information systems to protect the third party's in-
25 formation systems and information that is stored on,

1 processed by, or transiting the information systems,
2 if the third party lawfully authorizes the counter-
3 measures.

4 **SEC. 702. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
5 **THREAT INDICATORS AMONG PRIVATE ENTI-**
6 **TIES.**

7 (a) **AUTHORITY TO DISCLOSE.**—Notwithstanding any
8 other provision of law, any private entity may disclose law-
9 fully obtained cybersecurity threat indicators to any other
10 private entity.

11 (b) **USE AND PROTECTION OF INFORMATION.**—A pri-
12 vate entity disclosing or receiving cybersecurity threat in-
13 dicators under subsection (a)—

14 (1) shall make reasonable efforts to safeguard
15 communications, records, system traffic, or other in-
16 formation that can be used to identify specific per-
17 sons from unauthorized access or acquisition;

18 (2) shall comply with any lawful restrictions
19 placed on the disclosure or use of cybersecurity
20 threat indicators by the disclosing entity, including,
21 if requested, the removal of information that can be
22 used to identify specific persons from such indica-
23 tors;

24 (3) may not use the cybersecurity threat indica-
25 tors to gain an unfair competitive advantage to the

1 detriment of the entity that authorized such sharing;
2 and

3 (4) may only use, retain, or further disclose the
4 cybersecurity threat indicators for the purpose of
5 protecting an information system or information
6 that is stored on, processed by, or transiting an in-
7 formation system from cybersecurity threats or miti-
8 gating the threats.

9 **SEC. 703. CYBERSECURITY EXCHANGES.**

10 (a) DESIGNATION OF CYBERSECURITY EX-
11 CHANGES.—The Secretary, in consultation with the Direc-
12 tor of National Intelligence, the Attorney General, and the
13 Secretary of Defense, shall establish—

14 (1) a process for designating appropriate Fed-
15 eral entities (such as 1 or more Federal cybersecu-
16 rity centers) and non-Federal entities as cybersecu-
17 rity exchanges;

18 (2) procedures to facilitate and encourage the
19 sharing of classified and unclassified cybersecurity
20 threat indicators with designated cybersecurity ex-
21 changes and other appropriate Federal entities and
22 non-Federal entities; and

23 (3) a process for identifying certified entities
24 authorized to receive classified cybersecurity threat
25 indicators in accordance with paragraph (2).

1 (b) PURPOSE.—The purpose of a cybersecurity ex-
2 change is to efficiently receive and distribute cybersecurity
3 threat indicators in accordance with this title.

4 (c) REQUIREMENT FOR A LEAD FEDERAL CYBERSE-
5 CURITY EXCHANGE.—

6 (1) IN GENERAL.—The Secretary, in consulta-
7 tion with the Director of National Intelligence, the
8 Attorney General, and the Secretary of Defense,
9 shall designate a Federal entity as the lead cyberse-
10 curity exchange to serve as the focal point within the
11 Federal Government for cybersecurity information
12 sharing among Federal entities and with non-Fed-
13 eral entities.

14 (2) RESPONSIBILITIES.—The lead cybersecurity
15 exchange designated under paragraph (1) shall—

16 (A) receive and distribute cybersecurity
17 threat indicators in accordance with this title;

18 (B) facilitate information sharing, inter-
19 action, and collaboration among and between—

20 (i) Federal entities;

21 (ii) State, local, tribal, and territorial
22 governments;

23 (iii) private entities;

24 (iv) academia;

1 (v) international partners, in consulta-
2 tion with the Secretary of State; and

3 (vi) other cybersecurity exchanges;

4 (C) disseminate timely and actionable cy-
5 bersecurity threat, vulnerability, mitigation, and
6 warning information, including alerts,
7 advisories, indicators, signatures, and mitiga-
8 tion and response measures, to improve the se-
9 curity and protection of information systems;

10 (D) coordinate with other Federal and
11 non-Federal entities, as appropriate, to inte-
12 grate information from Federal and non-Fed-
13 eral entities, including Federal cybersecurity
14 centers, non-Federal network or security oper-
15 ation centers, other cybersecurity exchanges,
16 and non-Federal entities that disclose cyberse-
17 curity threat indicators under section 704(a) to
18 provide situational awareness of the United
19 States information security posture and foster
20 information security collaboration among infor-
21 mation system owners and operators;

22 (E) conduct, in consultation with private
23 entities and relevant Federal and other govern-
24 mental entities, regular assessments of existing
25 and proposed information sharing models to

1 eliminate bureaucratic obstacles to information
2 sharing and identify best practices for such in-
3 formation sharing; and

4 (F) coordinate with other Federal entities,
5 as appropriate, to compile and analyze informa-
6 tion about risks and incidents that threaten in-
7 formation systems, including information volun-
8 tarily submitted in accordance with section
9 704(a) or otherwise in accordance with applica-
10 ble laws.

11 (3) SCHEDULE FOR DESIGNATION.—

12 (A) INITIAL DESIGNATION.—Not later
13 than 60 days after the date of enactment of
14 this Act, the Secretary shall designate a lead
15 cybersecurity exchange under paragraph (1).

16 (B) INTERIM DESIGNATION.—The Na-
17 tional Cybersecurity and Communications Inte-
18 gration Center of the Department shall serve as
19 the interim lead cybersecurity exchange until
20 the Secretary designates a lead cybersecurity
21 exchange under paragraph (1).

22 (d) ADDITIONAL FEDERAL CYBERSECURITY EX-
23 CHANGES.—In accordance with the process and proce-
24 dures established under subsection (a), the Secretary, in
25 consultation with the Director of National Intelligence, the

1 Attorney General, and the Secretary of Defense, may des-
2 ignate additional existing Federal entities as cybersecurity
3 exchanges, if the cybersecurity exchanges are subject to
4 the requirements for use, retention, and disclosure of in-
5 formation by a cybersecurity exchange under section
6 704(b) and the special requirements for Federal entities
7 under section 704(g).

8 (e) REQUIREMENTS FOR NON-FEDERAL CYBERSECUR-
9 RITY EXCHANGES.—

10 (1) IN GENERAL.—In considering whether to
11 designate a non-Federal entity as a cybersecurity ex-
12 change to receive cybersecurity threat indicators
13 under section 704(a), and what entity to designate,
14 the Secretary shall consider the following factors:

15 (A) The net effect that an additional cy-
16 bersecurity exchange would have on the overall
17 cybersecurity of the United States.

18 (B) Whether the designation could sub-
19 stantially improve the overall cybersecurity of
20 the United States by serving as a hub for re-
21 ceiving and sharing cybersecurity threat indica-
22 tors, including the capacity of the non-Federal
23 entity for performing those functions.

1 (C) The capacity of the non-Federal entity
2 to safeguard cybersecurity threat indicators
3 from unauthorized disclosure and use.

4 (D) The adequacy of the policies and pro-
5 cedures of the non-Federal entity to protect
6 personally identifiable information from unau-
7 thorized disclosure and use.

8 (E) The ability of the non-Federal entity
9 to sustain operations using entirely non-Federal
10 sources of funding.

11 (2) REGULATIONS.—The Secretary may pro-
12 mulgate regulations as may be necessary to carry
13 out this subsection.

14 (f) CONSTRUCTION WITH OTHER AUTHORITIES.—
15 Nothing in this section may be construed to alter the au-
16 thorities of a Federal cybersecurity center, unless such cy-
17 bersecurity center is acting in its capacity as a designated
18 cybersecurity exchange.

19 (g) NO NEW BUREAUCRACIES.—Nothing in this sec-
20 tion may be construed to authorize additional layers of
21 Federal bureaucracy for the receipt and disclosure of cy-
22 bersecurity threat indicators.

23 (h) REPORT ON DESIGNATION OF CYBERSECURITY
24 EXCHANGE.—Not later than 90 days after the date on
25 which the Secretary designates the initial cybersecurity ex-

1 change under this section, the Secretary, the Director of
2 National Intelligence, the Attorney General, and the Sec-
3 retary of Defense shall jointly submit to Congress a writ-
4 ten report that—

5 (1) describes the processes established to des-
6 ignate cybersecurity exchanges under subsection (a);

7 (2) summarizes the policies and procedures es-
8 tablished under section 704(g); and

9 (3) if the Secretary has not designated any non-
10 Federal entities as a cybersecurity exchange, pro-
11 vides recommendations concerning the advisability of
12 designating non-Federal entities as cybersecurity ex-
13 changes.

14 **SEC. 704. VOLUNTARY DISCLOSURE OF CYBERSECURITY**
15 **THREAT INDICATORS TO A CYBERSECURITY**
16 **EXCHANGE.**

17 (a) **AUTHORITY TO DISCLOSE.**—Notwithstanding any
18 other provision of law, a non-Federal entity may disclose
19 lawfully obtained cybersecurity threat indicators to a cy-
20 bersecurity exchange.

21 (b) **USE, RETENTION, AND DISCLOSURE OF INFOR-**
22 **MATION BY A CYBERSECURITY EXCHANGE.**—Except as
23 provided in subsection (g), a cybersecurity exchange may
24 only use, retain, or further disclose information provided
25 under subsection (a) in order to protect information sys-

1 tems from cybersecurity threats or mitigate cybersecurity
2 threats.

3 (c) USE AND PROTECTION OF INFORMATION RE-
4 CEIVED FROM A CYBERSECURITY EXCHANGE.—A non-
5 Federal entity receiving cybersecurity threat indicators
6 from a cybersecurity exchange—

7 (1) shall make reasonable efforts to safeguard
8 communications, records, system traffic, and other
9 information that can be used to identify specific per-
10 sons from unauthorized access or acquisition;

11 (2) shall comply with any lawful restrictions
12 placed on the disclosure or use of cybersecurity
13 threat indicators by the cybersecurity exchange or a
14 third party, if the cybersecurity exchange received
15 the information from the third party, including, if
16 requested, the removal of information that can be
17 used to identify specific persons from the indicators;

18 (3) may not use the cybersecurity threat indica-
19 tors to gain an unfair competitive advantage to the
20 detriment of the third party that authorized the
21 sharing; and

22 (4) may only use, retain, or further disclose the
23 cybersecurity threat indicators for the purpose of
24 protecting an information system or information
25 that is stored on, processed by, or transiting an in-

1 formation system from cybersecurity threats or miti-
2 gating such threats.

3 (d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any
4 cybersecurity threat indicator disclosed by a non-Federal
5 entity to a cybersecurity exchange under subsection (a)
6 shall be—

7 (1) exempt from disclosure under section
8 552(b)(3) of title 5, United States Code, or any
9 comparable State law; and

10 (2) treated as voluntarily shared information
11 under section 552 of title 5, United States Code, or
12 any comparable State law.

13 (e) EXEMPTION FROM EX PARTE LIMITATIONS.—
14 Any cybersecurity threat indicator disclosed by a non-Fed-
15 eral entity to a cybersecurity exchange under subsection
16 (a) shall not be subject to the rules of any governmental
17 entity or judicial doctrine regarding ex parte communica-
18 tions with a decision making official.

19 (f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any
20 cybersecurity threat indicator disclosed by a non-Federal
21 entity to a cybersecurity exchange under subsection (a)
22 may not be construed to be a waiver of any applicable
23 privilege or protection provided under Federal, State, trib-
24 al, or territorial law, including any trade secret protection.

1 (g) SPECIAL REQUIREMENTS FOR FEDERAL ENTI-
2 TIES.—

3 (1) PERMITTED DISCLOSURES.—Notwith-
4 standing any other provision of law and consistent
5 with the requirements of this subsection, a Federal
6 entity that lawfully intercepts, acquires, or otherwise
7 obtains or possesses any communication, record, or
8 other information from its electronic communica-
9 tions system, may disclose that communication,
10 record, or other information if—

11 (A) the disclosure is made for the purpose
12 of—

13 (i) protecting the information system
14 of a Federal entity from cybersecurity
15 threats; or

16 (ii) mitigating cybersecurity threats
17 to—

18 (I) another component, officer,
19 employee, or agent of the Federal en-
20 tity with cybersecurity responsibilities;

21 (II) any cybersecurity exchange;
22 or

23 (III) a private entity that is act-
24 ing as a provider of electronic commu-
25 nication services, remote computing

1 service, or cybersecurity services to a
2 Federal entity; and

3 (B) the recipient of the communication,
4 record, or other information agrees to comply
5 with the Federal entity's lawful requirements
6 regarding the protection and further disclosure
7 of the information, except to the extent the re-
8 quirements are inconsistent with the policies
9 and procedures developed by the Secretary and
10 approved by the Attorney General under para-
11 graph (4).

12 (2) DISCLOSURE TO LAW ENFORCEMENT.—A
13 cybersecurity exchange that is a Federal entity may
14 disclose cybersecurity threat indicators received
15 under subsection (a) to a law enforcement entity
16 if—

17 (A) the information appears to relate to a
18 crime which has been, is being, or is about to
19 be committed; and

20 (B) the disclosure is permitted under the
21 procedures developed by the Secretary and ap-
22 proved by the Attorney General under para-
23 graph (4).

24 (3) FURTHER DISCLOSURE AND USE OF INFOR-
25 MATION BY A FEDERAL ENTITY.—

1 (A) AUTHORITY TO RECEIVE CYBERSECURITY
2 RITY THREAT INDICATORS.—A Federal entity
3 that is not a cybersecurity exchange may re-
4 ceive cybersecurity threat indicators from a cy-
5 bersecurity exchange under section 703, but
6 shall only use or retain the cybersecurity threat
7 indicators in a manner that is consistent with
8 this subsection in order—

9 (i) to protect information systems
10 from cybersecurity threats and to mitigate
11 cybersecurity threats; or

12 (ii) to disclose the cybersecurity threat
13 indicators to a law enforcement agency
14 under paragraph (2).

15 (B) AUTHORITY TO USE CYBERSECURITY
16 THREAT INDICATORS.—A Federal entity that is
17 not a cybersecurity exchange shall ensure, by
18 written agreement, that when disclosing cyber-
19 security threat indicators to a non-Federal enti-
20 ty under this section, the non-Federal entity
21 shall use or retain the cybersecurity threat indi-
22 cators in a manner that is consistent with the
23 requirements under section 702(b) on the use
24 and protection of information and paragraph
25 (2) of this subsection.

1 (4) PRIVACY AND CIVIL LIBERTIES.—

2 (A) REQUIREMENT FOR POLICIES AND
3 PROCEDURES.—In consultation with privacy
4 and civil liberties experts, the Director of Na-
5 tional Intelligence, and the Secretary of De-
6 fense, the Secretary shall develop and periodi-
7 cally review policies and procedures governing
8 the receipt, retention, use, and disclosure of cy-
9 bersecurity threat indicators by a Federal entity
10 obtained in connection with activities authorized
11 under this title, which shall—

12 (i) minimize the impact on privacy
13 and civil liberties, consistent with the need
14 to protect information systems from cyber-
15 security threats and mitigate cybersecurity
16 threats;

17 (ii) reasonably limit the receipt, reten-
18 tion, use and disclosure of cybersecurity
19 threat indicators associated with specific
20 persons consistent with the need to carry
21 out the responsibilities of this title, includ-
22 ing establishing a process for the timely
23 destruction of cybersecurity threat indica-
24 tors that are received under this section
25 that do not reasonably appear to be related

1 to protecting information systems from cy-
2 bersecurity threats and mitigating cyberse-
3 curity threats, unless the indicators appear
4 to relate to a crime which has been, is
5 being, or is about to be committed;

6 (iii) include requirements to safeguard
7 cybersecurity threat indicators that can be
8 used to identify specific persons from un-
9 authorized access or acquisition; and

10 (iv) protect the confidentiality of cy-
11 bersecurity threat indicators associated
12 with specific persons to the greatest extent
13 practicable and require recipients to be in-
14 formed that such indicators may only be
15 used for protecting information systems
16 against cybersecurity threats, mitigating
17 against cybersecurity threats, or disclosed
18 to law enforcement under paragraph (2).

19 (B) ADOPTION OF POLICIES AND PROCE-
20 DURES.—The head of a Federal agency respon-
21 sible for a Federal entity designated as a cyber-
22 security exchange under section 703 shall adopt
23 and comply with the policies and procedures de-
24 veloped under this subsection.

1 (C) REVIEW BY THE ATTORNEY GEN-
2 ERAL.—Not later than 1 year after the date of
3 the enactment of this Act, the Attorney General
4 shall review and approve policies and proce-
5 dures developed under this subsection.

6 (D) PROVISION TO CONGRESS.—The poli-
7 cies and procedures issued under this sub-
8 section and any amendments to such policies
9 and procedures shall be provided to Congress.

10 (5) OVERSIGHT.—

11 (A) REQUIREMENT FOR OVERSIGHT.—The
12 Secretary and the Attorney General shall estab-
13 lish a mandatory program to monitor and over-
14 see compliance with the policies and procedures
15 issued under this subsection.

16 (B) NOTIFICATION OF THE ATTORNEY
17 GENERAL.—The head of each Federal entity
18 that receives information under this title
19 shall—

20 (i) comply with the policies and proce-
21 dures developed by the Secretary and ap-
22 proved by the Attorney General under
23 paragraph (4);

1 (ii) promptly notify the Attorney Gen-
2 eral of significant violations of the policies
3 and procedures; and

4 (iii) provide the Attorney General with
5 any information relevant to the violation
6 that any Attorney General requires.

7 (C) ANNUAL REPORT.—On an annual
8 basis, the Chief Privacy and Civil Liberties Of-
9 ficer of the Department of Justice and the De-
10 partment of Homeland Security, in consultation
11 with the most senior privacy and civil liberties
12 officer or officers of any appropriate agencies,
13 shall jointly submit to Congress a report assess-
14 ing the privacy and civil liberties impact of the
15 activities of the Federal Government conducted
16 under this title.

17 (6) PRIVACY AND CIVIL LIBERTIES OVERSIGHT
18 BOARD.—Not later than 2 years after the date of
19 enactment of this Act, the Privacy and Civil Lib-
20 erties Oversight Board shall submit to Congress and
21 the President a report providing—

22 (A) an assessment of the privacy and civil
23 liberties impact of the activities carried out by
24 the Federal entities under this title; and

1 (B) recommendations for improvements to
2 or modifications of the law to address privacy
3 and civil liberties concerns.

4 (7) SANCTIONS.—The heads of Federal entities
5 shall develop and enforce appropriate sanctions for
6 officers, employees, or agents of the Federal entities
7 who conduct activities under this title—

8 (A) outside the normal course of their
9 specified duties;

10 (B) in a manner inconsistent with the dis-
11 charge of the responsibilities of the Federal en-
12 tities; or

13 (C) in contravention of the requirements,
14 policies and procedures required under this sub-
15 section.

16 **SEC. 705. SHARING OF CLASSIFIED CYBERSECURITY**
17 **THREAT INDICATORS.**

18 (a) SHARING OF CLASSIFIED CYBERSECURITY
19 THREAT INDICATORS.—The procedures established under
20 section 703(a)(2) shall provide that classified cybersecu-
21 rity threat indicators may only be—

22 (1) shared with certified entities;

23 (2) shared in a manner that is consistent with
24 the need to protect the national security of the
25 United States;

1 (3) shared with a person with an appropriate
2 security clearance to receive the cybersecurity threat
3 indicators; and

4 (4) used by a certified entity in a manner that
5 protects the cybersecurity threat indicators from un-
6 authorized disclosure.

7 (b) REQUIREMENT FOR GUIDELINES.—Not later
8 than 60 days after the date of enactment of this Act, the
9 Director of National Intelligence shall issue guidelines pro-
10 viding that appropriate Federal officials may, as the Di-
11 rector considers necessary to carry out this title—

12 (1) grant a security clearance on a temporary
13 or permanent basis to an employee of a certified en-
14 tity;

15 (2) grant a security clearance on a temporary
16 or permanent basis to a certified entity and approval
17 to use appropriate facilities; or

18 (3) expedite the security clearance process for a
19 certified entity or employee of a certified entity, if
20 appropriate, in a manner consistent with the need to
21 protect the national security of the United States.

22 (c) DISTRIBUTION OF PROCEDURES AND GUIDE-
23 LINES.—Following the establishment of the procedures
24 under section 703(a)(2) and the issuance of the guidelines
25 under subsection (b), the Secretary and the Director of

1 National Intelligence shall expeditiously distribute the pro-
2 cedures and guidelines to—

3 (1) appropriate governmental entities and pri-
4 vate entities;

5 (2) the Committee on Armed Services, the
6 Committee on Commerce, Science, and Transpor-
7 tation, the Committee on Homeland Security and
8 Governmental Affairs, the Committee on the Judici-
9 ary, and the Select Committee on Intelligence of the
10 Senate; and

11 (3) the Committee on Armed Services, the
12 Committee on Energy and Commerce, the Com-
13 mittee on Homeland Security, the Committee on the
14 Judiciary, and the Permanent Select Committee on
15 Intelligence of the House of Representatives.

16 **SEC. 706. LIMITATION ON LIABILITY AND GOOD FAITH DE-**
17 **FENSE FOR CYBERSECURITY ACTIVITIES.**

18 (a) IN GENERAL.—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, based on—

22 (1) the cybersecurity monitoring activities au-
23 thorized by paragraphs (1) and (2) of section 701;
24 or

1 (2) the voluntary disclosure of a lawfully ob-
2 tained cybersecurity threat indicator—

3 (A) to a cybersecurity exchange under sec-
4 tion 704(a);

5 (B) by a provider of cybersecurity services
6 to a customer of the provider;

7 (C) to a private entity or governmental en-
8 tity that provides or manages critical infra-
9 structure; or

10 (D) to any other private entity under sec-
11 tion 702(a), if the cybersecurity threat indicator
12 is also disclosed within a reasonable time to a
13 cybersecurity exchange.

14 (b) GOOD FAITH DEFENSE.—If a civil or criminal
15 cause of action is not barred under subsection (a), good
16 faith reliance that this title permitted the conduct com-
17 plained of is a complete defense against any civil or crimi-
18 nal action brought under this title or any other law.

19 (c) LIMITATION ON USE OF CYBERSECURITY
20 THREAT INDICATORS FOR REGULATORY ENFORCEMENT
21 ACTIONS.—No Federal entity may use a cybersecurity
22 threat indicator received under this title as evidence in a
23 regulatory enforcement action against the entity that law-
24 fully shared the cybersecurity threat indicator with a cy-
25 bersecurity exchange that is a Federal entity.

1 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
2 ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—No
3 civil or criminal cause of action shall lie or be maintained
4 in any Federal or State court against any entity, and any
5 such action shall be dismissed promptly, for a failure to
6 disclose a cybersecurity threat indicator if—

7 (1) the Attorney General determines that dis-
8 closure of a cybersecurity threat indicator would im-
9 pede a civil or criminal investigation and submits a
10 written request to delay notification for up to 30
11 days, except that the Attorney General may, by a
12 subsequent written request, revoke such delay or ex-
13 tend the period of time set forth in the original re-
14 quest made under this paragraph if further delay is
15 necessary; or

16 (2) the Secretary, the Attorney General, or the
17 Director of National Intelligence determines that
18 disclosure of a cybersecurity threat indicator would
19 threaten national or homeland security and submits
20 a written request to delay notification, except that
21 the Secretary, the Attorney General or the Director
22 of National Intelligence may, by a subsequent writ-
23 ten request, revoke such delay or extend the period
24 of time set forth in the original request made under
25 this paragraph if further delay is necessary.

1 (e) LIMITATION ON LIABILITY FOR FAILURE TO
2 ACT.—No civil or criminal cause of action shall lie or be
3 maintained in any Federal or State court against any pri-
4 vate entity, or any officer, employee, or agent of such an
5 entity, and any such action shall be dismissed promptly,
6 for the reasonable failure to act on information received
7 under this title.

8 (f) LIMITATION ON PROTECTIONS.—Any person who
9 knowingly and willfully violates restrictions under this title
10 shall not receive the protections under this title.

11 (g) PRIVATE RIGHT OF ACTION.—Nothing in this
12 title may be construed to limit liability for a failure to
13 comply with the requirements of section 702(b) and sec-
14 tion 704(c) on the use and protection of information.

15 (h) DEFENSE FOR BREACH OF CONTRACT.—Compli-
16 ance with lawful restrictions placed on the disclosure or
17 use of cybersecurity threat indicators is a complete defense
18 to any tort or breach of contract claim originating in a
19 failure to disclose cybersecurity threat indicators to a third
20 party.

21 **SEC. 707. CONSTRUCTION; FEDERAL PREEMPTION.**

22 (a) CONSTRUCTION.—Nothing in this title may be
23 construed—

24 (1) to permit the unauthorized disclosure of—

1 (A) information that has been determined
2 by the Federal Government pursuant to an Ex-
3 ecutive Order or statute to require protection
4 against unauthorized disclosure for reasons of
5 national defense or foreign relations;

6 (B) any restricted data (as that term is de-
7 fined in paragraph (y) of section 11 of the
8 Atomic Energy Act of 1954 (42 U.S.C. 2014));

9 (C) information related to intelligence
10 sources and methods; or

11 (D) information that is specifically subject
12 to a court order or a certification, directive, or
13 other authorization by the Attorney General
14 precluding such disclosure;

15 (2) to limit or prohibit otherwise lawful dislo-
16 sures of communications, records, or information by
17 a private entity to a cybersecurity exchange or any
18 other governmental or private entity not conducted
19 under this title;

20 (3) to limit the ability of a private entity or
21 governmental entity to receive data about the infor-
22 mation systems of the entity, including lawfully ob-
23 tained cybersecurity threat indicators;

24 (4) to authorize or prohibit any law enforce-
25 ment, homeland security, or intelligence activities

1 not otherwise authorized or prohibited under another
2 provision of law;

3 (5) to permit price-fixing, allocating a market
4 between competitors, monopolizing or attempting to
5 monopolize a market, boycotting, or exchanges of
6 price or cost information, customer lists, or informa-
7 tion regarding future competitive planning; or

8 (6) to prevent a governmental entity from using
9 information not acquired through a cybersecurity ex-
10 change for regulatory purposes.

11 (b) FEDERAL PREEMPTION.—This title supersedes
12 any law or requirement of a State or political subdivision
13 of a State that restricts or otherwise expressly regulates
14 the provision of cybersecurity services or the acquisition,
15 interception, retention, use or disclosure of communica-
16 tions, records, or other information by private entities to
17 the extent such law contains requirements inconsistent
18 with this title.

19 (c) PRESERVATION OF OTHER STATE LAW.—Except
20 as expressly provided, nothing in this title shall be con-
21 strued to preempt the applicability of any other State law
22 or requirement.

23 (d) NO CREATION OF A RIGHT TO INFORMATION.—
24 The provision of information to a non-Federal entity

1 under this title shall not create a right or benefit to similar
2 information by any other non-Federal entity.

3 (e) PROHIBITION ON REQUIREMENT TO PROVIDE IN-
4 FORMATION TO THE FEDERAL GOVERNMENT.—Nothing
5 in this title, except as expressly stated, may be construed
6 to permit a Federal entity—

7 (1) to require a non-Federal entity to share in-
8 formation with the Federal Government; or

9 (2) to condition the disclosure of unclassified or
10 classified cybersecurity threat indicators under this
11 title with a non-Federal entity on the provision of
12 cybersecurity threat information to the Federal Gov-
13 ernment.

14 (f) LIMITATION ON USE OF INFORMATION.—No cy-
15 bersecurity threat indicators obtained under this title may
16 be used, retained, or disclosed by a Federal entity or non-
17 Federal entity, except as authorized under this title.

18 (g) DECLASSIFICATION AND SHARING OF INFORMA-
19 TION.—Consistent with the exemptions from public disclo-
20 sure of section 704(d), the Director of National Intel-
21 ligence, in consultation with the Secretary, shall facilitate
22 the declassification and sharing of information in the pos-
23 session of a Federal entity that is related to cybersecurity
24 threats, as the Director of National Intelligence deter-
25 mines appropriate.

1 (h) REPORT ON IMPLEMENTATION.—Not later than
2 2 years after the date of enactment of this Act, the Sec-
3 retary, the Director of National Intelligence, the Attorney
4 General, and the Secretary of Defense shall jointly submit
5 to Congress a report that—

6 (1) describes the extent to which the authorities
7 conferred by this title have enabled the Federal Gov-
8 ernment and the private sector to mitigate cyberse-
9 curity threats;

10 (2) discloses any significant acts of noncompli-
11 ance by a non-Federal entity with this title, with
12 special emphasis on privacy and civil liberties, and
13 any measures taken by the Federal Government to
14 uncover such noncompliance;

15 (3) describes in general terms the nature and
16 quantity of information disclosed and received by
17 governmental entities and private entities under this
18 title; and

19 (4) proposes changes to the law, including the
20 definitions, authorities and requirements under this
21 title, that are necessary to ensure the law keeps pace
22 with the threat while protecting privacy and civil lib-
23 erties.

24 (i) REQUIREMENT FOR ANNUAL REPORT.—On an
25 annual basis, the Director of National Intelligence shall

1 provide a report to the Select Committee on Intelligence
2 of the Senate and the Permanent Select Committee on In-
3 telligence of the House of Representatives on the imple-
4 mentation of section 705. Each report under this sub-
5 section, which shall be submitted in an unclassified form,
6 but may include a classified annex, shall include a list of
7 private entities that receive classified cybersecurity threat
8 indicators under this title, except that the unclassified re-
9 port shall not contain information that may be used to
10 identify specific private entities unless such private enti-
11 ties consent to such identification.

12 **SEC. 708. DEFINITIONS.**

13 In this title:

14 (1) **CERTIFIED ENTITY.**—The term “certified
15 entity” means a protected entity, a self-protected en-
16 tity, or a provider of cybersecurity services that—

17 (A) possesses or is eligible to obtain a se-
18 curity clearance, as determined by the Director
19 of National Intelligence; and

20 (B) is able to demonstrate to the Director
21 of National Intelligence that the provider or en-
22 tity can appropriately protect and use classified
23 cybersecurity threat indicators.

24 (2) **COUNTERMEASURE.**—The term “counter-
25 measure” means automated or manual actions with

1 defensive intent to modify or block data packets as-
2 sociated with electronic or wire communications,
3 internet traffic, program code, or other system traf-
4 fic transiting to or from or stored on an information
5 system for the purpose of protecting the information
6 system from cybersecurity threats, conducted on an
7 information system owned or operated by or on be-
8 half of the party to be protected or operated by a
9 private entity acting as a provider of electronic com-
10 munication services, remote computing services, or
11 cybersecurity services to the party to be protected.

12 (3) CYBERSECURITY EXCHANGE.—The term
13 “cybersecurity exchange” means any governmental
14 entity or private entity designated by the Secretary
15 as a cybersecurity exchange under section 703(a).

16 (4) CYBERSECURITY SERVICES.—The term “cy-
17 bersecurity services” means products, goods, or serv-
18 ices intended to detect, mitigate, or prevent cyberse-
19 curity threats.

20 (5) CYBERSECURITY THREAT.—The term “cy-
21 bersecurity threat” means any action that may re-
22 sult in unauthorized access to, exfiltration of, manip-
23 ulation of, or impairment to the integrity, confiden-
24 tiality, or availability of an information system or in-

1 formation that is stored on, processed by, or
2 transiting an information system.

3 (6) CYBERSECURITY THREAT INDICATOR.—The
4 term “cybersecurity threat indicator” means infor-
5 mation—

6 (A) that may be indicative of or describe—

7 (i) malicious reconnaissance, including
8 anomalous patterns of communications
9 that reasonably appear to be transmitted
10 for the purpose of gathering technical in-
11 formation related to a cybersecurity threat;

12 (ii) a method of defeating a technical
13 control;

14 (iii) a technical vulnerability;

15 (iv) a method of defeating an oper-
16 ational control;

17 (v) a method of causing a user with
18 legitimate access to an information system
19 or information that is stored on, processed
20 by, or transiting an information system to
21 unwittingly enable the defeat of a technical
22 control or an operational control;

23 (vi) malicious cyber command and
24 control;

1 (vii) the actual or potential harm
2 caused by an incident, including informa-
3 tion exfiltrated as a result of subverting a
4 technical control when it is necessary in
5 order to identify or describe a cybersecu-
6 rity threat;

7 (viii) any other attribute of a cyberse-
8 curity threat, if disclosure of such attribute
9 is not otherwise prohibited by law; or

10 (ix) any combination thereof; and

11 (B) from which reasonable efforts have
12 been made to remove information that can be
13 used to identify specific persons unrelated to
14 the cybersecurity threat.

15 (7) FEDERAL CYBERSECURITY CENTER.—The
16 term “Federal cybersecurity center” means the De-
17 partment of Defense Cyber Crime Center, the Intel-
18 ligence Community Incident Response Center, the
19 United States Cyber Command Joint Operations
20 Center, the National Cyber Investigative Joint Task
21 Force, the National Security Agency/Central Secu-
22 rity Service Threat Operations Center, or the United
23 States Computer Emergency Readiness Team, or
24 any successor to such a center.

1 (8) FEDERAL ENTITY.—The term “Federal en-
2 tity” means a Federal agency, or any component, of-
3 ficer, employee, or agent of a Federal agency.

4 (9) GOVERNMENTAL ENTITY.—The term “gov-
5 ernmental entity” means any Federal entity and
6 agency or department of a State, local, tribal, or ter-
7 ritorial government other than an educational insti-
8 tution, or any component, officer, employee, or agent
9 of such an agency or department.

10 (10) INFORMATION SYSTEM.—The term “infor-
11 mation system” means a discrete set of information
12 resources organized for the collection, processing,
13 maintenance, use, sharing, dissemination, or disposi-
14 tion of information, including communications with,
15 or commands to, specialized systems such as indus-
16 trial and process control systems, telephone switch-
17 ing and private branch exchange, and environmental
18 control systems.

19 (11) MALICIOUS CYBERCOMMAND AND CON-
20 TROL.—The term “malicious cyber command and
21 control” means a method for remote identification
22 of, access to, or use of, an information system or in-
23 formation that is stored on, processed by, or
24 transiting an information system associated with a
25 known or suspected cybersecurity threat.

1 (12) MALICIOUS RECONNAISSANCE.—The term
2 “malicious reconnaissance” means a method for ac-
3 tively probing or passively monitoring an information
4 system for the purpose of discerning technical
5 vulnerabilities of the information system, if such
6 method is associated with a known or suspected cy-
7 bersecurity threat.

8 (13) MONITOR.—The term “monitor” means
9 the interception, acquisition, or collection of informa-
10 tion that is stored on, processed by, or transiting an
11 information system for the purpose of identifying cy-
12 bersecurity threats.

13 (14) NON-FEDERAL ENTITY.—The term “non-
14 Federal entity” means a private entity or a govern-
15 mental entity other than a Federal entity.

16 (15) OPERATIONAL CONTROL.—The term
17 “operational control” means a security control for
18 an information system that primarily is implemented
19 and executed by people.

20 (16) PRIVATE ENTITY.—The term “private en-
21 tity” has the meaning given the term “person” in
22 section 1 of title 1, United States Code, and does
23 not include a governmental entity.

24 (17) PROTECT.—The term “protect” means ac-
25 tions undertaken to secure, defend, or reduce the

1 vulnerabilities of an information system, mitigate cy-
2 bersecurity threats, or otherwise enhance informa-
3 tion security or the resiliency of information systems
4 or assets.

5 (18) PROTECTED ENTITY.—The term “pro-
6 tected entity” means an entity, other than an indi-
7 vidual, that contracts with a provider of cybersecu-
8 rity services for goods or services to be used for cy-
9 bersecurity purposes.

10 (19) SELF-PROTECTED ENTITY.—The term
11 “self-protected entity” means an entity, other than
12 an individual, that provides cybersecurity services to
13 itself.

14 (20) TECHNICAL CONTROL.—The term “tech-
15 nical control” means a hardware or software restric-
16 tion on, or audit of, access or use of an information
17 system or information that is stored on, processed
18 by, or transiting an information system that is in-
19 tended to ensure the confidentiality, integrity, or
20 availability of that system.

21 (21) TECHNICAL VULNERABILITY.—The term
22 “technical vulnerability” means any attribute of
23 hardware or software that could enable or facilitate
24 the defeat of a technical control.

1 (22) THIRD PARTY.—The term “third party”
2 includes Federal entities and non-Federal entities.

3 **TITLE VIII—PUBLIC AWARENESS**
4 **REPORTS**

5 **SEC. 801. FINDINGS.**

6 Congress finds the following:

7 (1) Information technology is central to the ef-
8 fectiveness, efficiency, and reliability of the industry
9 and commercial services, Armed Forces and national
10 security systems, and the critical infrastructure of
11 the United States.

12 (2) Cyber criminals, terrorists, and agents of
13 foreign powers have taken advantage of the
14 connectivity of the United States to inflict substan-
15 tial damage to the economic and national security
16 interests of the Nation.

17 (3) The cybersecurity threat is sophisticated,
18 relentless, and massive, exposing all consumers in
19 the United States to the risk of substantial harm.

20 (4) Businesses in the United States are bearing
21 enormous losses as a result of criminal cyber at-
22 tacks, depriving businesses of hard-earned profits
23 that could be reinvested in further job-producing in-
24 novation.

1 (5) Hackers continuously probe the networks of
2 Federal and State agencies, the Armed Forces, and
3 the commercial industrial base of the Armed Forces,
4 and already have caused substantial damage and
5 compromised sensitive and classified information.

6 (6) Severe cybersecurity threats will continue,
7 and will likely grow, as the economy of the United
8 States grows more connected, criminals become in-
9 creasingly sophisticated in efforts to steal from con-
10 sumers, industries, and businesses in the United
11 States, and terrorists and foreign nations continue
12 to use cyberspace as a means of attack against the
13 national and economic security of the United States.

14 (7) Public awareness of cybersecurity threats is
15 essential to cybersecurity defense. Only a well-in-
16 formed public and Congress can make the decisions
17 necessary to protect consumers, industries, and the
18 national and economic security of the United States.

19 (8) As of 2012, the level of public awareness of
20 cybersecurity threats is unacceptably low. Only a
21 tiny portion of relevant cybersecurity information is
22 released to the public. Information about attacks on
23 Federal Government systems is usually classified.
24 Information about attacks on private systems is or-
25 dinarily kept confidential. Sufficient mechanisms do

1 not exist to provide meaningful threat reports to the
2 public in unclassified and anonymized form.

3 **SEC. 802. REPORT ON CYBER INCIDENTS AGAINST GOVERN-**
4 **MENT NETWORKS.**

5 (a) DEPARTMENT OF HOMELAND SECURITY.—Not
6 later than 180 days after the date of enactment of this
7 Act, and annually thereafter, the Secretary shall submit
8 to Congress a report that—

9 (1) summarizes major cyber incidents involving
10 networks of Executive agencies (as defined in section
11 105 of title 5, United States Code), except for the
12 Department of Defense;

13 (2) provides aggregate statistics on the number
14 of breaches of networks of Executive agencies, the
15 volume of data exfiltrated, and the estimated cost of
16 remedying the breaches; and

17 (3) discusses the risk of cyber sabotage.

18 (b) DEPARTMENT OF DEFENSE.—Not later than 180
19 days after the date of enactment of this Act, and annually
20 thereafter, the Secretary of Defense shall submit to Con-
21 gress a report that—

22 (1) summarizes major cyber incidents against
23 networks of the Department of Defense and the
24 military departments;

1 (2) provides aggregate statistics on the number
2 of breaches against networks of the Department of
3 Defense and the military departments, the volume of
4 data exfiltrated, and the estimated cost of remedying
5 the breaches; and

6 (3) discusses the risk of cyber sabotage.

7 (c) FORM OF REPORTS.—Each report submitted
8 under this section shall be in unclassified form, but may
9 include a classified annex as necessary to protect sources,
10 methods, and national security.

11 **SEC. 803. REPORTS ON PROSECUTION FOR CYBERCRIME.**

12 (a) IN GENERAL.—Not later than 180 days after the
13 date of enactment of this Act, the Attorney General and
14 the Director of the Federal Bureau of Investigation shall
15 submit to Congress reports—

16 (1) describing investigations and prosecutions
17 by the Department of Justice relating to cyber in-
18 trusions or other cybercrimes the preceding year, in-
19 cluding—

20 (A) the number of investigations initiated
21 relating to such crimes;

22 (B) the number of arrests relating to such
23 crimes;

24 (C) the number and description of in-
25 stances in which investigations or prosecutions

1 relating to such crimes have been delayed or
2 prevented because of an inability to extradite a
3 criminal defendant in a timely manner; and

4 (D) the number of prosecutions for such
5 crimes, including—

6 (i) the number of defendants pros-
7 ecuted;

8 (ii) whether the prosecutions resulted
9 in a conviction;

10 (iii) the sentence imposed and the
11 statutory maximum for each such crime
12 for which a defendant was convicted; and

13 (iv) the average sentence imposed for
14 a conviction of such crimes;

15 (2) identifying the number of employees, finan-
16 cial resources, and other resources (such as tech-
17 nology and training) devoted to the enforcement, in-
18 vestigation, and prosecution of cyber intrusions or
19 other cybercrimes, including the number of inves-
20 tigators, prosecutors, and forensic specialists dedi-
21 cated to investigating and prosecuting cyber intru-
22 sions or other cybercrimes; and

23 (3) discussing any impediments under the laws
24 of the United States or international law to prosecu-
25 tions for cyber intrusions or other cybercrimes.

1 (b) UPDATES.—The Attorney General and the Direc-
2 tor of the Federal Bureau of Investigation shall annually
3 submit to Congress reports updating the reports sub-
4 mitted under subsection (a) at the same time the Attorney
5 General and Director submit annual reports under section
6 404 of the Prioritizing Resources and Organization for In-
7 tellectual Property Act of 2008 (42 U.S.C. 3713d).

8 **SEC. 804. REPORT ON RESEARCH RELATING TO SECURE**
9 **DOMAIN.**

10 (a) IN GENERAL.—The Secretary shall enter into a
11 contract with the National Research Council, or another
12 federally funded research and development corporation,
13 under which the Council or corporation shall submit to
14 Congress reports on available technical options, consistent
15 with constitutional and statutory privacy rights, for en-
16 hancing the security of the information networks of enti-
17 ties that own or manage critical infrastructure through—

18 (1) technical improvements, including devel-
19 oping a secure domain; or

20 (2) increased notice of and consent to the use
21 of technologies to scan for, detect, and defeat cyber
22 security threats, such as technologies used in a se-
23 cure domain.

1 (b) TIMING.—The contract entered into under sub-
2 section (a) shall require that the report described in sub-
3 section (a) be submitted—

4 (1) not later than 180 days after the date of
5 enactment of this Act;

6 (2) annually, after the first report submitted
7 under subsection (a), for 3 years; and

8 (3) more frequently, as determined appropriate
9 by the Secretary in response to new risks or tech-
10 nologies that emerge.

11 **SEC. 805. REPORT ON PREPAREDNESS OF FEDERAL**
12 **COURTS TO PROMOTE CYBERSECURITY.**

13 Not later than 180 days after the date of enactment
14 of this Act, the Attorney General, in coordination with the
15 Administrative Office of the United States Courts, shall
16 submit to Congress a report—

17 (1) on whether Federal courts have granted
18 timely relief in matters relating to botnets and other
19 cybercrime and cyber security threats; and

20 (2) that includes, as appropriate, recommenda-
21 tions on changes or improvements to—

22 (A) the Federal Rules of Civil Procedure
23 or the Federal Rules of Criminal Procedure;

24 (B) the training and other resources avail-
25 able to support the Federal judiciary;

1 (C) the capabilities and specialization of
2 courts to which such cases may be assigned;
3 and

4 (D) Federal civil and criminal laws.

5 **SEC. 806. REPORT ON IMPEDIMENTS TO PUBLIC AWARE-**
6 **NESS.**

7 Not later than 180 days after the date of enactment
8 of this Act, and annually thereafter for 3 years (or more
9 frequently if determined appropriate by the Secretary) the
10 Secretary shall submit to Congress a report on—

11 (1) legal or other impediments to appropriate
12 public awareness of—

13 (A) the nature of, methods of propagation
14 of, and damage caused by common cyber secu-
15 rity threats such as computer viruses, phishing
16 techniques, and malware;

17 (B) the minimal standards of computer se-
18 curity necessary for responsible Internet use;
19 and

20 (C) the availability of commercial off the
21 shelf technology that allows consumers to meet
22 such levels of computer security;

23 (2) a summary of the plans of the Secretary to
24 enhance public awareness of common cyber security
25 threats, including a description of the metrics used

1 by the Department for evaluating the efficacy of
2 public awareness campaigns; and

3 (3) recommendations for congressional actions
4 to address these impediments to appropriate public
5 awareness of common cyber security threats.

6 **SEC. 807. REPORT ON PROTECTING THE ELECTRICAL GRID**
7 **OF THE UNITED STATES.**

8 Not later than 180 days after the date of enactment
9 of this Act, the Secretary, in consultation with the Sec-
10 retary of Defense and the Director of National Intel-
11 ligence, shall submit to Congress a report on—

12 (1) the threat of a cyber attack disrupting the
13 electrical grid of the United States;

14 (2) the implications for the national security of
15 the United States if the electrical grid is disrupted;

16 (3) the options available to the United States
17 and private sector entities to quickly reconstitute
18 electrical service to provide for the national security
19 of the United States, and, within a reasonable time
20 frame, the reconstitution of all electrical service
21 within the United States; and

22 (4) a plan to prevent disruption of the electric
23 grid of the United States caused by a cyber attack.

1 **TITLE IX—INTERNATIONAL**
2 **COOPERATION**

3 **SEC. 901. DEFINITIONS.**

4 In this title:

5 (1) **COMPUTER SYSTEM; COMPUTER DATA.**—

6 The terms “computer system” and “computer data”
7 have the meanings given those terms in chapter I of
8 the Convention on Cybercrime.

9 (2) **CONVENTION ON CYBERCRIME.**—The term

10 “Convention on Cybercrime” means the Council of
11 Europe’s Convention on Cybercrime, done at Buda-
12 pest November 23, 2001 as ratified by the United
13 States Senate on August 3, 2006 (Treaty 108–11)
14 with any relevant reservations of declarations.

15 (3) **CYBER ISSUES.**—The term “cyber issues”

16 means the full range of international policies de-
17 signed to ensure an open, interoperable, secure, and
18 reliable global information and communications in-
19 frastructure.

20 (4) **CYBERCRIME.**—The term “cybercrime” re-

21 fers to criminal offenses relating to computer sys-
22 tems of computer data described in the Convention
23 of Cybercrime.

24 (5) **RELEVANT FEDERAL AGENCIES.**—The term

25 “relevant Federal agencies” means any Federal

1 agency that has responsibility for combating
2 cybercrime globally, including the Department of
3 Commerce, the Department of Homeland Security,
4 the Department of Justice, the Department of State,
5 the Department of the Treasury, and the Office of
6 the United States Trade Representative.

7 **SEC. 902. FINDINGS.**

8 Congress finds the following:

9 (1) On February 2, 2010, Admiral Dennis C.
10 Blair, the Director of National Intelligence, testified
11 before the Select Committee on Intelligence of the
12 Senate regarding the Annual Threat Assessment of
13 the U.S. Intelligence Community, stating “The na-
14 tional security of the United States, our economic
15 prosperity, and the daily functioning of our govern-
16 ment are dependent on a dynamic public and private
17 information infrastructure, which includes tele-com-
18 munications, computer networks and systems, and
19 the information residing within. This critical infra-
20 structure is severely threatened. . . . We cannot pro-
21 tect cyberspace without a coordinated and collabo-
22 rative effort that incorporates both the US private
23 sector and our international partners.”

24 (2) In a January 2010 speech on Internet free-
25 dom, Secretary of State Hillary Clinton stated:

1 “Those who disrupt the free flow of information in
2 our society, or any other, pose a threat to our econ-
3 omy, our government, and our civil society. Coun-
4 tries or individuals that engage in cyber attacks
5 should face consequences and international con-
6 demnation. In an Internet-connected world, an at-
7 tack on one nation’s networks can be an attack on
8 all. And by reinforcing that message, we can create
9 norms of behavior among states and encourage re-
10 spect for the global networked commons.”

11 (3) November 2011 marked the tenth anniver-
12 sary of the Convention on Cybercrime, the only mul-
13 tilateral agreement on cybercrime, to which the Sen-
14 ate provided advice and consent on August 3, 2006,
15 and is currently ratified by over 30 countries.

16 (4) The May 2009 White House Cyberspace
17 Policy Review asserts “[t]he Nation also needs a
18 strategy for cybersecurity designed to shape the
19 international environment and bring like-minded na-
20 tions together on a host of issues, such as technical
21 standards and acceptable legal norms regarding ter-
22 ritorial jurisdiction, sovereign responsibility, and use
23 of force. International norms are critical to estab-
24 lishing a secure and thriving digital infrastructure.”

1 **SEC. 903. SENSE OF CONGRESS.**

2 It is the sense of Congress that—

3 (1) engagement with other countries to advance
4 the cyberspace objectives of the United States should
5 be an integral part of the conduct of United States
6 foreign relations and diplomacy;

7 (2) the cyberspace objectives of the United
8 States include the full range of cyber issues, includ-
9 ing issues related to governance, standards, cyberse-
10 curity, cybercrime, international security, human
11 rights, and the free flow of information;

12 (3) it is in the interest of the United States to
13 work with other countries to build consensus on
14 principles and standards of conduct that protect
15 computer systems and users that rely on them, pre-
16 vent and punish acts of cybercrime, and promote the
17 free flow of information;

18 (4) a comprehensive national cyberspace strat-
19 egy must include tools for addressing threats to
20 computer systems and acts of cybercrime from
21 sources and by persons outside the United States;

22 (5) developing effective solutions to inter-
23 national cyberspace threats requires engagement
24 with foreign countries on a bilateral basis and
25 through relevant regional and multilateral fora;

1 (6) it is in the interest of the United States to
2 encourage the development of effective frameworks
3 for international cooperation to combat cyberthreats,
4 and the development of foreign government capabili-
5 ties to combat cyberthreats; and

6 (7) the Secretary of State, in consultation with
7 other relevant Federal agencies, should develop and
8 lead Federal Government efforts to engage with
9 other countries to advance the cyberspace objectives
10 of the United States, including efforts to bolster an
11 international framework of cyber norms, governance
12 and deterrence.

13 **SEC. 904. COORDINATION OF INTERNATIONAL CYBER**
14 **ISSUES WITHIN THE UNITED STATES GOV-**
15 **ERNMENT.**

16 The Secretary of State is authorized to designate a
17 senior level official at the Department of State, to carry
18 out the Secretary's responsibilities to—

19 (1) coordinate the United States global diplo-
20 matic engagement on the full range of international
21 cyber issues, including building multilateral coopera-
22 tion and developing international norms, common
23 policies, and responses to secure the integrity of
24 cyberspace;

1 (2) provide strategic direction and coordination
2 for United States Government policy and programs
3 aimed at addressing and responding to cyber issues
4 overseas, especially in relation to issues that affect
5 United States foreign policy and related national se-
6 curity concerns;

7 (3) coordinate with relevant Federal agencies,
8 including the Department, the Department of De-
9 fense, the Department of the Treasury, the Depart-
10 ment of Justice, the Department of Commerce, and
11 the intelligence community to develop interagency
12 plans regarding international cyberspace, cybersecu-
13 rity, and cybercrime issues; and

14 (4) ensure that cyber issues, including cyberse-
15 curity and cybercrime, are included in the respon-
16 sibilities of overseas Embassies and consulates of the
17 United States, as appropriate.

18 **SEC. 905. CONSIDERATION OF CYBERCRIME IN FOREIGN**
19 **POLICY AND FOREIGN ASSISTANCE PRO-**
20 **GRAMS.**

21 (a) BRIEFING.—

22 (1) IN GENERAL.—Not later than 1 year after
23 the date of enactment of this Act, the Secretary of
24 State, after consultation with the heads of the rel-

1 evant Federal agencies, shall provide a comprehen-
2 sive briefing to relevant congressional committees—

3 (A) assessing global issues, trends, and ac-
4 tors considered to be significant with respect to
5 cybercrime;

6 (B) assessing, after consultation with pri-
7 vate industry groups, civil society organizations,
8 and other relevant domestic or multilateral or-
9 ganizations, which shall be selected by the
10 President based on an interest in combating
11 cybercrime, means of enhancing multilateral or
12 bilateral efforts in areas of significance—

13 (i) to prevent and investigate
14 cybercrime;

15 (ii) to develop and share best prac-
16 tices with respect to directly or indirectly
17 combating cybercrime; and

18 (iii) to cooperate and take action with
19 respect to the prevention, investigation,
20 and prosecution of cybercrime; and

21 (C) describing the steps taken by the
22 United States to promote the multilateral or bi-
23 lateral efforts described in subparagraph (B).

24 (2) CONTRIBUTIONS FROM RELEVANT FEDERAL
25 AGENCIES.—Not later than 30 days before the date

1 on which the briefing is to be provided under para-
2 graph (1), the head of each relevant Federal agency
3 shall consult with and provide to the Secretary of
4 State relevant information appropriate for the brief-
5 ing.

6 (b) PERIODIC UPDATES.—The Secretary of State
7 shall provide updated information highlighting significant
8 developments relating to the issues described in subsection
9 (a), through periodic briefings to Congress.

10 (c) USE OF FOREIGN ASSISTANCE PROGRAMS.—

11 (1) FOREIGN ASSISTANCE PROGRAMS TO COM-
12 BAT CYBERCRIME.—The Secretary of State is au-
13 thorized to accord priority in foreign assistance to
14 programs designed to combat cybercrime in a region
15 or program of significance in order to better combat
16 cybercrime by, among other things, improving the
17 effectiveness and capacity of the legal and judicial
18 systems and the capabilities of law enforcement
19 agencies with respect to cybercrime.

20 (2) SENSE OF THE CONGRESS WITH RESPECT
21 TO BILATERAL AND MULTILATERAL ASSISTANCE.—

22 It is the sense of Congress that the Secretary of
23 State should include programs designed to combat
24 cybercrime in relevant bilateral or multilateral as-

- 1 assistance programs administered or supported by the
- 2 United States Government.

Calendar No. 323

112TH CONGRESS
2^D SESSION

S. 2105

A BILL

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

FEBRUARY 15, 2012

Read the second time and placed on the calendar