

112TH CONGRESS  
2D SESSION

**S.** \_\_\_\_\_

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

---

## IN THE SENATE OF THE UNITED STATES

---

Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEIN-  
STEIN, and Mr. CARPER) introduced the following bill; which was read  
twice and referred to the Committee on \_\_\_\_\_

---

## A BILL

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

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

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

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

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

TITLE I—PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL  
INFRASTRUCTURE

## 2

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

## TITLE II—FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

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

## TITLE III—RESEARCH AND DEVELOPMENT

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

## TITLE IV—EDUCATION, WORKFORCE, AND AWARENESS

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

## TITLE V—FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

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

## TITLE VI—INTERNATIONAL COOPERATION

- Sec. 601. Definitions.
- Sec. 602. Findings.
- Sec. 603. Sense of Congress.

## 3

- Sec. 604. Coordination of international cyber issues within the United States Government.
- Sec. 605. Consideration of cybercrime in foreign policy and foreign assistance programs.

## TITLE VII—INFORMATION SHARING

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

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

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

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

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

15 (4) COUNCIL.—The term “Council” means the  
16 National Cybersecurity Council established under  
17 section 101.

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

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

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

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

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

1           (10) FEDERAL INFORMATION INFRASTRUC-  
2           TURE.—The term “Federal information infrastruc-  
3           ture”—

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

10                   (B) does not include—

11                           (i) a national security system; or

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

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

22           (12) INFORMATION INFRASTRUCTURE.—The  
23           term “information infrastructure” means the under-  
24           lying framework that information systems and assets  
25           rely on to process, transmit, receive, or store infor-

1        mation electronically, including programmable elec-  
2        tronic devices, communications networks, and indus-  
3        trial or supervisory control systems and any associ-  
4        ated hardware, software, or data.

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

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

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

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

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

1           (18) NATIONAL INFORMATION INFRASTRUC-  
2           TURE.—The term “national information infrastruc-  
3           ture” means information and information systems—

4                   (A) that are owned, operated, or con-  
5                   trolled, in whole or in part, within or from the  
6                   United States; and

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

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

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

17           (21) OWNER.—The term “owner”—

18                   (A) means an entity that owns critical in-  
19                   frastructure; and

20                   (B) does not include a company contracted  
21                   by the owner to manage, run, or operate that  
22                   critical infrastructure, or to provide a specific  
23                   information technology product or service that  
24                   is used or incorporated into that critical infra-  
25                   structure.

1 (22) OPERATOR.—The term “operator”—

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

5 (B) may include the owner of critical infra-  
6 structure.

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

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

13 (A) the exfiltration of data that is essential  
14 to the operation of critical cyber infrastructure;  
15 or

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

20 **TITLE I—PUBLIC-PRIVATE PART-**  
21 **NERSHIP TO PROTECT CRIT-**  
22 **ICAL INFRASTRUCTURE**

23 **SEC. 101. NATIONAL CYBERSECURITY COUNCIL.**

24 (a) IN GENERAL.—There is established a National  
25 Cybersecurity Council.

1 (b) RESPONSIBILITIES.—The Council shall—

2 (1) conduct sector-by-sector risk assessments in  
3 partnership with owners and operators, private sec-  
4 tor entities, relevant Federal agencies, and appro-  
5 priate non-governmental entities and institutions of  
6 higher education;

7 (2) identify categories of critical cyber infra-  
8 structure, in partnership with relevant Federal agen-  
9 cies, owners and operators, other appropriate private  
10 sector entities, and appropriate non-governmental  
11 entities and institutions of higher education;

12 (3) coordinate the adoption of private-sector  
13 recommended voluntary outcome-based cybersecurity  
14 practices with owners and operators, private sector  
15 entities, relevant Federal agencies, the Critical In-  
16 frastructure Partnership Advisory Council, institu-  
17 tions of higher education, and appropriate non-gov-  
18 ernmental cybersecurity experts, in accordance with  
19 this title;

20 (4) establish an incentives-based voluntary cy-  
21 bersecurity program for critical infrastructure to en-  
22 courage owners to adopt voluntary outcome-based  
23 cybersecurity practices under section 103;

1           (5) develop procedures to inform owners and  
2           operators of cyber threats, vulnerabilities, and con-  
3           sequences; and

4           (6) upon request and to the maximum extent  
5           possible, provide any technical guidance or assist-  
6           ance to owners and operators consistent with this  
7           title.

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

11           (1) prescribe the responsibilities of the Council  
12           and the member agencies;

13           (2) ensure the timely implementation of deci-  
14           sions of the Council;

15           (3) delegate authority to the Chairperson to  
16           take action to fulfill the responsibilities of the Coun-  
17           cil if—

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

20                   (B) necessary to prevent or mitigate an  
21                   imminent cybersecurity threat.

22          (d) MEMBERSHIP.—The Council shall be comprised  
23          of appropriate representatives appointed by the President  
24          from—

25           (1) the Department of Commerce;

- 1 (2) the Department of Defense;
- 2 (3) the Department of Justice;
- 3 (4) the intelligence community;
- 4 (5) sector-specific Federal agencies, as appropriate;
- 5
- 6 (6) Federal agencies with responsibility for regulating the security of critical cyber infrastructure,
- 7
- 8 as appropriate; and
- 9 (7) the Department.

10 (e) COORDINATION.—The Council shall coordinate  
11 the activities of the Council with—

- 12 (1) appropriate representatives of the private
- 13 sector; and
- 14 (2) owners and operators.

15 (f) CHAIRPERSON.—

16 (1) IN GENERAL.—The Secretary shall serve as  
17 Chairperson of the Council (referred to in this section as the “Chairperson”).

18

19 (2) RESPONSIBILITIES OF THE CHAIRPERSON.—The Chairperson shall—

20

21 (A) ensure the responsibilities of the Council are expeditiously fulfilled;

22

23 (B) provide expertise and support to the

24 Council; and

1 (C) provide recommendations to the Coun-  
2 cil.

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

12 (1) does not contradict any regulation or com-  
13 pulsory standard in effect before the adoption of the  
14 cybersecurity practice; and

15 (2) to the extent possible, complements or oth-  
16 erwise improves the regulation or compulsory stand-  
17 ard described in paragraph (1).

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

19 (a) RISK ASSESSMENTS.—

20 (1) IN GENERAL.—

21 (A) DESIGNATION OF MEMBER AGENCY.—

22 The Council shall designate a member agency  
23 to conduct top-level cybersecurity assessments  
24 of cyber risks to critical infrastructure with vol-

1           untary participation from private sector enti-  
2           ties.

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

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

16                   (A) not later than 180 days after the date  
17           of enactment of this Act, conduct a top-level as-  
18           sessment of the cybersecurity threats,  
19           vulnerabilities, and consequences and the prob-  
20           ability of a catastrophic incident and associated  
21           risk across all critical infrastructure sectors to  
22           determine which sectors pose the greatest im-  
23           mediate risk, in order to guide the allocation of  
24           resources for the implementation of this Act;  
25           and

1 (B) beginning with the highest priority sec-  
2 tors identified under subparagraph (A), con-  
3 duct, on an ongoing, sector-by-sector basis,  
4 cyber risk assessments of the threats to,  
5 vulnerabilities of, and consequences of a cyber  
6 attack on critical infrastructure.

7 (3) VOLUNTARY INPUT OF OWNERS AND OPER-  
8 ATORS.—The member agency designated under  
9 paragraph (1) shall—

10 (A) establish a process under which owners  
11 and operators and other relevant private sector  
12 experts may provide input into the risk assess-  
13 ments conducted under this section; and

14 (B) seek and incorporate private sector ex-  
15 pertise available through established public-pri-  
16 vate partnerships, including the Critical Infra-  
17 structure Partnership Advisory Council and ap-  
18 propriate Information Sharing and Analysis Or-  
19 ganizations.

20 (4) PROTECTION OF INFORMATION.—Any infor-  
21 mation submitted as part of the process established  
22 under paragraph (3) shall be protected in accord-  
23 ance with section 106.

24 (5) SUBMISSION OF RISK ASSESSMENTS.—The  
25 Council shall submit each risk assessment conducted

1 under this section, in a classified or unclassified  
2 form as necessary, to—

3 (A) the President;

4 (B) appropriate Federal agencies; and

5 (C) appropriate congressional committees.

6 (b) IDENTIFICATION OF CRITICAL CYBER INFRA-  
7 STRUCTURE CATEGORIES.—

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

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

19 (A) prioritize efforts based on the  
20 prioritization established under subsection (a);

21 (B) incorporate, to the extent practicable,  
22 the input of owners and operators, the Critical  
23 Infrastructure Partnership Advisory Council,  
24 appropriate Information Sharing and Analysis  
25 Organizations, and other appropriate represent-

1           atives of the private sector and State and local  
2           governments;

3           (C) develop a voluntary mechanism for  
4           owners to submit information to assist the  
5           Council in making determinations under this  
6           section;

7           (D) inform owners and operators of the  
8           criteria used to identify categories of critical  
9           cyber infrastructure;

10          (E) establish procedures for an owner of  
11          critical infrastructure identified as critical cyber  
12          infrastructure to challenge the identification;

13          (F) select a member agency to make rec-  
14          ommendations to the Council on the identifica-  
15          tion of categories of critical cyber infrastruc-  
16          ture; and

17          (G) periodically review and update identi-  
18          fications under this subsection.

19          (3) IDENTIFICATION REQUIREMENTS.—The  
20          Council shall—

21                (A) identify categories of critical cyber in-  
22                frastructure within each sector of critical infra-  
23                structure and identify owners of critical infra-  
24                structure within each category of critical cyber  
25                infrastructure;

1 (B) only identify a category of critical in-  
2 frastructure as critical cyber infrastructure if  
3 damage to or unauthorized access to such crit-  
4 ical infrastructure could reasonably result in—

5 (i) the interruption of life-sustaining  
6 services, including energy, water, transpor-  
7 tation, emergency services, or food, suffi-  
8 cient to cause—

9 (I) a mass casualty event; or

10 (II) mass evacuations;

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

13 (I) failure or substantial disrup-  
14 tion of a financial market of the  
15 United States;

16 (II) incapacitation or sustained  
17 disruption of a transportation system;  
18 or

19 (III) other systemic, long-term  
20 damage to the economy of the United  
21 States; or

22 (iii) severe degradation of national se-  
23 curity or national security capabilities, in-  
24 cluding intelligence and defense functions;  
25 and

1 (C) consider the sector-by-sector risk as-  
2 sessments developed in accordance with sub-  
3 section (a).

4 (4) INCIDENT REPORTING.—The Council shall  
5 establish procedures under which each owner of crit-  
6 ical cyber infrastructure shall report significant  
7 cyber incidents affecting critical cyber infrastruc-  
8 ture.

9 (5) LIMITATIONS.—The Council may not iden-  
10 tify as a category of critical cyber infrastructure  
11 under this section—

12 (A) critical infrastructure based solely on  
13 activities protected by the first amendment to  
14 the Constitution of the United States;

15 (B) an information technology product  
16 based solely on a finding that the product is ca-  
17 pable of, or is actually, being used in critical  
18 cyber infrastructure; or

19 (C) a commercial item that organizes or  
20 communicates information electronically.

21 (6) NOTIFICATION OF IDENTIFICATION OF CAT-  
22 EGORY OF CRITICAL CYBER INFRASTRUCTURE.—Not  
23 later than 10 days after the Council identifies a cat-  
24 egory of critical cyber infrastructure under this sec-

1       tion, the Council shall notify the relevant owners of  
2       the identified critical cyber infrastructure.

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

6       (c) CONGRESSIONAL NOTICE AND OPPORTUNITY FOR  
7       DISAPPROVAL.—

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

12                   (A) notify Congress of the identification;  
13                   and

14                   (B) submit to Congress a report explaining  
15                   the basis for the identification.

16           (2) OPPORTUNITY FOR CONGRESSIONAL RE-  
17      VIEW.—The identification of a category of critical  
18      infrastructure as critical cyber infrastructure shall  
19      not take effect for purposes of this title until the  
20      date that is 60 days after the date on which the  
21      Council notifies Congress under paragraph (1).

22   **SEC. 103. VOLUNTARY CYBERSECURITY PRACTICES.**

23           (a) PRIVATE SECTOR DEVELOPMENT OF CYBERSE-  
24      CURITY PRACTICES.—Not later than 180 days after the  
25      date of enactment of this Act, each sector coordinating

1 council shall propose to the Council voluntary outcome-  
2 based cybersecurity practices (referred to in this section  
3 as “cybersecurity practices”) sufficient to effectively reme-  
4 diate or mitigate cyber risks identified through an assess-  
5 ment conducted under section 102(a) comprised of—

6 (1) industry best practices, standards, and  
7 guidelines; or

8 (2) practices developed by the sector coordi-  
9 nating council in coordination with owners and oper-  
10 ators, voluntary consensus standards development  
11 organizations, representatives of State and local gov-  
12 ernments, the private sector, and appropriate infor-  
13 mation sharing and analysis organizations.

14 (b) REVIEW OF CYBERSECURITY PRACTICES.—

15 (1) IN GENERAL.—The Council shall, in con-  
16 sultation with owners and operators, the Critical In-  
17 frastructure Partnership Advisory Council, and ap-  
18 propriate information sharing and analysis organiza-  
19 tions, and in coordination with appropriate rep-  
20 resentatives from State and local governments—

21 (A) consult with relevant security experts  
22 and institutions of higher education, including  
23 university information security centers, appro-  
24 priate nongovernmental cybersecurity experts,  
25 and representatives from national laboratories;

1 (B) review relevant regulations or compul-  
2 sory standards or guidelines;

3 (C) review cybersecurity practices proposed  
4 under subsection (a); and

5 (D) consider any amendments to the cyber-  
6 security practices and any additional cybersecu-  
7 rity practices necessary to ensure adequate re-  
8 mediation or mitigation of the cyber risks iden-  
9 tified through an assessment conducted under  
10 section 102(a).

11 (2) ADOPTION.—

12 (A) IN GENERAL.—Not later than 1 year  
13 after the date of enactment of this Act, the  
14 Council shall—

15 (i) adopt any cybersecurity practices  
16 proposed under subsection (a) that ade-  
17 quately remediate or mitigate identified  
18 cyber risks and any associated con-  
19 sequences identified through an assessment  
20 conducted under section 102(a); and

21 (ii) adopt any amended or additional  
22 cybersecurity practices necessary to ensure  
23 the adequate remediation or mitigation of  
24 the cyber risks identified through an as-  
25 sessment conducted under section 102(a).

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

12 (c) FLEXIBILITY OF CYBERSECURITY PRACTICES.—  
13 Each sector coordinating council and the Council shall pe-  
14 riodically assess cybersecurity practices, but not less fre-  
15 quently than once every 3 years, and update or modify  
16 cybersecurity practices as necessary to ensure adequate re-  
17 mediation and mitigation of the cyber risks identified  
18 through an assessment conducted under section 102(a).

19 (d) PRIORITIZATION.—Based on the risk assessments  
20 performed under section 102(a), the Council shall  
21 prioritize the development of cybersecurity practices to en-  
22 sure the reduction or mitigation of the greatest cyber  
23 risks.

24 (e) PRIVATE SECTOR RECOMMENDED MEASURES.—  
25 Each sector coordinating council shall develop voluntary

1 recommended cybersecurity measures that provide owners  
2 reasonable and cost-effective methods of meeting any cy-  
3 bersecurity practice.

4 (f) TECHNOLOGY NEUTRALITY.—No cybersecurity  
5 practice shall require—

6 (1) the use of a specific commercial information  
7 technology product; or

8 (2) that a particular commercial information  
9 technology product be designed, developed, or manu-  
10 factured in a particular manner.

11 (g) RELATIONSHIP TO EXISTING REGULATIONS.—

12 (1) INCLUSION IN REGULATORY REGIMES.—

13 (A) IN GENERAL.—A Federal agency with  
14 responsibilities for regulating the security of  
15 critical infrastructure may adopt the cybersecu-  
16 rity practices as mandatory requirements.

17 (B) REPORTS.—If, as of the date that is  
18 1 year after the date of enactment of this Act,  
19 a Federal agency with responsibilities for regu-  
20 lating the security of critical infrastructure has  
21 not adopted the cybersecurity practices as man-  
22 datory requirements, the agency shall submit to  
23 the appropriate congressional committees a re-  
24 port on the reasons the agency did not do so,  
25 including a description of whether the critical

1 cyber infrastructure for which the Federal  
2 agency has responsibility is maintaining prac-  
3 tices sufficient to effectively remediate or miti-  
4 gate cyber risks identified through an assess-  
5 ment conducted under section 102(a).

6 (C) RULE OF CONSTRUCTION.—Nothing in  
7 this subsection shall be construed to provide a  
8 Federal agency with authority for regulating  
9 the security of critical cyber infrastructure in  
10 addition or to a greater extent than the author-  
11 ity the Federal agency has under other law.

12 (2) AVOIDANCE OF CONFLICT.—No cybersecu-  
13 rity practice shall—

14 (A) prevent an owner (including a certified  
15 owner) from complying with any law or regula-  
16 tion; or

17 (B) require an owner (including a certified  
18 owner) to implement cybersecurity measures  
19 that prevent the owner from complying with  
20 any law or regulation.

21 (3) AVOIDANCE OF DUPLICATION.—Where reg-  
22 ulations or compulsory standards regulate the secu-  
23 rity of critical cyber infrastructure, a cybersecurity  
24 practice shall, to the greatest extent possible, com-

1       plement or otherwise improve the regulations or  
2       compulsory standards.

3       (h) INDEPENDENT REVIEW.—

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

12          (2) CONSIDERATION BY COUNCIL.—The Council  
13      shall consider any review conducted under paragraph  
14      (1).

15      (i) VOLUNTARY TECHNICAL ASSISTANCE.—At the re-  
16      quest of an owner or operator of critical infrastructure,  
17      the Council shall provide guidance on the application of  
18      cybersecurity practices to the critical infrastructure.

19      **SEC. 104. VOLUNTARY CYBERSECURITY PROGRAM FOR**  
20                                      **CRITICAL INFRASTRUCTURE.**

21      (a) VOLUNTARY CYBERSECURITY PROGRAM FOR  
22      CRITICAL INFRASTRUCTURE.—

23          (1) IN GENERAL.—Not later than 1 year after  
24      the date of enactment of this Act, the Council, in  
25      consultation with owners and operators and the Crit-

1        ical Infrastructure Partnership Advisory Council,  
2        shall establish the Voluntary Cybersecurity Program  
3        for Critical Infrastructure in accordance with this  
4        section.

5            (2) ELIGIBILITY.—

6            (A) IN GENERAL.—An owner of critical  
7        cyber infrastructure may apply for certification  
8        under the Voluntary Cybersecurity Program for  
9        Critical Infrastructure.

10          (B) CRITERIA.—The Council shall estab-  
11        lish criteria for owners of critical infrastructure  
12        that is not critical cyber infrastructure to be eli-  
13        gible to apply for certification in the Voluntary  
14        Cybersecurity Program for Critical Infrastruc-  
15        ture.

16          (3) APPLICATION FOR CERTIFICATION.—An  
17        owner of critical cyber infrastructure or an owner of  
18        critical infrastructure that meets the criteria estab-  
19        lished under paragraph (2)(B) that applies for cer-  
20        tification under this subsection shall—

21            (A) select and implement cybersecurity  
22        measures of their choosing that satisfy the out-  
23        come-based cybersecurity practices established  
24        under section 103; and

1           (B)(i) certify in writing and under penalty  
2           of perjury to the Council that the owner has de-  
3           veloped and effectively implemented cybersecu-  
4           rity measures sufficient to satisfy the outcome-  
5           based cybersecurity practices established under  
6           section 103; or

7           (ii) submit to the Council an assessment  
8           verifying that the owner has developed and ef-  
9           fectively implemented cybersecurity measures  
10          sufficient to satisfy the outcome-based cyberse-  
11          curity practices established under section 103.

12          (4) CERTIFICATION.—Upon receipt of a self-  
13          certification under paragraph (3)(B)(i) or an assess-  
14          ment under paragraph (3)(B)(ii) the Council shall  
15          certify an owner.

16          (5) NONPERFORMANCE.—If the Council deter-  
17          mines that a certified owner is not in compliance  
18          with the cybersecurity practices established under  
19          section 103, the Council shall—

20                (A) notify the certified owner of such de-  
21                termination; and

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

24          (6) REVOCATION.—If a certified owner fails to  
25          remediate promptly any deficiencies identified by the

1 Council, the Council shall revoke the certification of  
2 the certified owner.

3 (7) REDRESS.—

4 (A) IN GENERAL.—If the Council revokes  
5 a certification under paragraph (6), the Council  
6 shall—

7 (i) notify the owner of such revoca-  
8 tion; and

9 (ii) provide the owner with specific cy-  
10 bersecurity measures that, if implemented,  
11 would remediate any deficiencies.

12 (B) RECERTIFICATION.—If the Council de-  
13 termines that an owner has remedied any defi-  
14 ciencies and is in compliance with the cyberse-  
15 curity practices, the Council may recertify the  
16 owner.

17 (b) ASSESSMENTS.—

18 (1) THIRD-PARTY ASSESSMENTS.—The Council,  
19 in consultation with owners and operators and the  
20 Critical Infrastructure Protection Advisory Council,  
21 shall enter into agreements with qualified third-  
22 party private entities, to conduct assessments that  
23 use reliable, repeatable, performance-based evalua-  
24 tions and metrics to assess whether an owner cer-

1       tified under subsection (a)(3)(B)(ii) is in compliance  
2       with all applicable cybersecurity practices.

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

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

13          (4) NOTIFICATION.—The Council shall provide  
14      copies of any assessments by the Federal Govern-  
15      ment to the certified owner.

16          (5) ACCESS TO INFORMATION.—

17            (A) IN GENERAL.—For the purposes of an  
18      assessment conducted under this subsection, a  
19      certified owner shall provide the Council, or a  
20      third party assessor, any reasonable access nec-  
21      essary to complete an assessment.

22            (B) PROTECTION OF INFORMATION.—In-  
23      formation provided to the Council, the Council's  
24      designee, or any assessor during the course of  
25      an assessment under this section shall be pro-

1           tected from disclosure in accordance with sec-  
2           tion 106.

3       (c) BENEFITS OF CERTIFICATION.—

4           (1) LIMITATIONS ON CIVIL LIABILITY.—

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

14            (B) LIMITATION.—Subaragraph (A) shall  
15          only apply to harm directly caused by the inci-  
16          dent related to the cyber risk and shall not  
17          apply to damages caused by any additional or  
18          intervening acts or omissions by the owner.

19           (2) EXPEDITED SECURITY CLEARANCE PROC-  
20          ESS.—The Council, in coordination with the Office  
21          of the Director of National Intelligence, shall estab-  
22          lish a procedure to expedite the provision of security  
23          clearances to appropriate personnel employed by a  
24          certified owner.

1           (3) PRIORITIZED TECHNICAL ASSISTANCE.—

2           The Council shall ensure that certified owners are  
3           eligible to receive prioritized technical assistance.

4           (4) PROVISION OF CYBER THREAT INFORMA-

5           TION.—The Council shall develop, in coordination  
6           with certified owners, a procedure for ensuring that  
7           certified owners are, to the maximum extent prac-  
8           ticable and consistent with the protection of sources  
9           and methods, informed of relevant real-time cyber  
10          threat information.

11          (5) PUBLIC RECOGNITION.—With the approval

12          of a certified owner, the Council may publicly recog-  
13          nize the certified owner if the Council determines  
14          such recognition does not pose a risk to the security  
15          of critical cyber infrastructure.

16          (6) STUDY TO EXAMINE BENEFITS OF PRO-  
17          CUREMENT PREFERENCE.—

18                 (A) IN GENERAL.—The Federal Acquisi-

19                 tion Regulatory Council, in coordination with  
20                 the Council and with input from relevant pri-  
21                 vate sector individuals and entities, shall con-  
22                 duct a study examining the potential benefits of  
23                 establishing a procurement preference for the  
24                 Federal Government for certified owners.

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

3 (i) potential persons and related prop-  
4 erty and services that could be eligible for  
5 preferential consideration in the procure-  
6 ment process;

7 (ii) development and management of  
8 an approved list of categories of property  
9 and services that could be eligible for pref-  
10 erential consideration in the procurement  
11 process;

12 (iii) appropriate mechanisms to imple-  
13 ment preferential consideration in the pro-  
14 curement process, including—

15 (I) establishing a policy encour-  
16 aging Federal agencies to conduct  
17 market research and industry out-  
18 reach to identify property and services  
19 that adhere to relevant cybersecurity  
20 practices;

21 (II) authorizing the use of a  
22 mark for the Voluntary Cybersecurity  
23 Program for Critical Infrastructure to  
24 be used for marketing property or  
25 services to the Federal Government;

1 (III) establishing a policy of en-  
2 couraging procurement of certain  
3 property and services from an ap-  
4 proved list;

5 (IV) authorizing the use of a  
6 preference by Federal agencies in the  
7 evaluation process; and

8 (V) authorizing a requirement in  
9 certain solicitations that the person  
10 providing the property or services be a  
11 certified owner; and

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

21 **SEC. 105. RULES OF CONSTRUCTION.**

22 Nothing in this title shall be construed to—

23 (1) limit the ability of a Federal agency with re-  
24 sponsibilities for regulating the security of critical

1 infrastructure from requiring that the cybersecurity  
2 practices developed under section 103 be met;

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

10 (3) limit or restrict the authority of the Depart-  
11 ment, or any other Federal agency, under any other  
12 provision of law; or

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

16 **SEC. 106. PROTECTION OF INFORMATION.**

17 (a) DEFINITIONS.—In this section—

18 (1) the term “covered information” means any  
19 information—

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

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

23 (C) required to be submitted by owners  
24 under section 102(b)(4);

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

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

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

15 (b) CRITICAL INFRASTRUCTURE INFORMATION.—

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

24 (2) SAVINGS CLAUSE FOR EXISTING WHISTLE-  
25 BLOWER PROTECTIONS.—With respect to covered in-

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

7       (c) CRITICAL INFRASTRUCTURE CYBER SECURITY  
8       TIP LINE.—

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

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

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

21               (i) a possible violation of any law,  
22       rule, regulation or guideline;

23               (ii) mismanagement;

24               (iii) risk to public health, safety, secu-  
25       rity, or privacy; or

1 (iv) other misfeasance or nonfeasance.

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

7 (A) disclosure of covered information; or

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

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

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

17 (B) shall not be provided initially to the  
18 Secretary; and

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

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

24 (1) limit or otherwise affect the right, ability,  
25 duty, or obligation of any entity to use or disclose

1 any information of that entity, including in the con-  
2 duct of any judicial or other proceeding;

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

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

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

22 (B) section 2409 of title 10, United States  
23 Code; or

24 (C) any other Federal, State, or local law,  
25 ordinance, or regulation that protects against

1           retaliation an individual who discloses informa-  
2           tion that the individual reasonably believes evi-  
3           dences a violation of any law, rule, or regula-  
4           tion, gross mismanagement, substantial and  
5           specific danger to public health, safety, or secu-  
6           rity, or other misfeasance or nonfeasance;

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

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

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

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

18          (e) AUDIT.—

19               (1) IN GENERAL.—Not later than 1 year after  
20          the date of enactment of this Act, the Inspector  
21          General of the Department shall conduct an audit of  
22          the management of covered information under this  
23          title and report the findings to appropriate congres-  
24          sional committees.

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

3           (A) whether the covered information is  
4           adequately safeguarded against inappropriate  
5           disclosure;

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

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

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

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

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

23          (G) any other factors at the discretion of  
24          the Inspector General of the Department.

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

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

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

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

14              (2) an analysis of—

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

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

22                   (C) whether Federal agencies with respon-  
23   sibilities for regulating the security of critical  
24   infrastructure are adequately adopting and en-  
25   forcing the cybersecurity practices adopted  
26   under section 103; and

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

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

8 **SEC. 108. INTERNATIONAL COOPERATION.**

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

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

23 (2) coordinate with the government of the coun-  
24 try in which such information infrastructure is lo-  
25 cated and, as appropriate, the owner or operator of

1 the information infrastructure regarding the imple-  
2 mentation of cybersecurity measures or other meas-  
3 ures to the information infrastructure to mitigate or  
4 remediate cyber risks.

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

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

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

14 **SEC. 110. DEFINITIONS.**

15 In this title:

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

20 (2) CYBER RISK.—The term “cyber risk”  
21 means any risk to information infrastructure, includ-  
22 ing physical or personnel risks and security  
23 vulnerabilities, that, if exploited or not mitigated,  
24 could pose a significant risk of disruption to the op-

1       eration of information infrastructure essential to the  
2       reliable operation of critical infrastructure.

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

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

17 **TITLE II—FEDERAL INFORMA-**  
18 **TION SECURITY MANAGE-**  
19 **MENT AND CONSOLIDATING**  
20 **RESOURCES**

21 **SEC. 201. FISMA REFORM.**

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

1 “SUBCHAPTER II—INFORMATION SECURITY

2 “§ 3551. Purposes

3 “The purposes of this subchapter are to—

4 “(1) provide a comprehensive framework for en-  
5 suring the effectiveness of information security con-  
6 trols over information resources that support Fed-  
7 eral operations and assets;

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

17 “(3) provide for development and maintenance  
18 of controls required to protect agency information  
19 and information systems and contribute to the over-  
20 all improvement of agency information security pos-  
21 ture; and

22 “(4) provide a mechanism to improve and con-  
23 tinuously monitor the security of agency information  
24 security programs and systems through a focus on  
25 continuous monitoring of agency information sys-

1       tems and streamlined reporting requirements rather  
2       than overly prescriptive manual reporting.

3   **“§ 3552. Definitions**

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

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

9           “(1) ADEQUATE SECURITY.—The term ‘ade-  
10   quate security’ means security commensurate with  
11   the risk and impact resulting from the unauthorized  
12   access to or loss, misuse, destruction, or modifica-  
13   tion of information.

14          “(2) CONTINUOUS MONITORING.—The term  
15   ‘continuous monitoring’ means the ongoing real time  
16   or near real-time process used to determine if the  
17   complete set of planned, required, and deployed se-  
18   curity controls within an information system con-  
19   tinue to be effective over time in light of rapidly  
20   changing information technology and threat develop-  
21   ment. To the maximum extent possible, this also re-  
22   quires automation of that process to enable cost ef-  
23   fective, efficient, and consistent monitoring and pro-  
24   vide a more dynamic view of the security state of  
25   those deployed controls.

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

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

16                 “(A) actually or imminently jeopardizes,  
17                 without lawful authority, the integrity, con-  
18                 fidentiality, or availability of information or an  
19                 information system; or

20                 “(B) constitutes a violation or imminent  
21                 threat of violation of law, security policies, secu-  
22                 rity procedures, or acceptable use policies.

23          “(5) INFORMATION SECURITY.—The term ‘in-  
24          formation security’ means protecting information  
25          and information systems from unauthorized access,

1 use, disclosure, disruption, modification, or destruc-  
2 tion in order to provide—

3 “(A) integrity, which means guarding  
4 against improper information modification or  
5 destruction, and includes ensuring nonrepudi-  
6 ation and authenticity;

7 “(B) confidentiality, which means pre-  
8 serving authorized restrictions on access and  
9 disclosure, including means for protecting per-  
10 sonal privacy and proprietary information; and

11 “(C) availability, which means ensuring  
12 timely and reliable access to and use of infor-  
13 mation.

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

17 “(7) NATIONAL SECURITY SYSTEM.—

18 “(A) IN GENERAL.—The term ‘national se-  
19 curity system’ means any information system  
20 (including any telecommunications system) used  
21 or operated by an agency or by a contractor of  
22 an agency, or other organization on behalf of an  
23 agency—

24 “(i) the function, operation, or use of  
25 which—

1 “(I) involves intelligence activi-  
2 ties;

3 “(II) involves cryptologic activi-  
4 ties related to national security;

5 “(III) involves command and  
6 control of military forces;

7 “(IV) involves equipment that is  
8 an integral part of a weapon or weap-  
9 ons system; or

10 “(V) subject to subparagraph  
11 (B), is critical to the direct fulfillment  
12 of military or intelligence missions; or

13 “(ii) that is protected at all times by  
14 procedures established for information that  
15 have been specifically authorized under cri-  
16 teria established by an Executive order or  
17 an Act of Congress to be kept classified in  
18 the interest of national defense or foreign  
19 policy.

20 “(B) EXCLUSION.—Subparagraph  
21 (A)(i)(V) does not include a system that is to  
22 be used for routine administrative and business  
23 applications (including payroll, finance, logis-  
24 tics, and personnel management applications).

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

3   **“§ 3553. Federal information security authority and**  
4           **coordination**

5           “(a) IN GENERAL.—Except as provided in sub-  
6           sections (f) and (g), the Secretary shall oversee agency in-  
7           formation security policies and practices, including the de-  
8           velopment and oversight of information security policies  
9           and directives and compliance with this subchapter.

10          “(b) DUTIES.—The Secretary shall—

11               “(1) develop, issue, and oversee the implemen-  
12               tation of information security policies and directives,  
13               which shall be compulsory and binding on agencies  
14               to the extent determined appropriate by the Sec-  
15               retary, including—

16                       “(A) policies and directives consistent with  
17                       the standards promulgated under section 11331  
18                       of title 40 to identify and provide information  
19                       security protections that are commensurate  
20                       with the risk and impact resulting from the un-  
21                       authorized access, use, disclosure, disruption,  
22                       modification, or destruction of—

23                               “(i) information collected, created,  
24                               processed, stored, disseminated, or other-

1 wise used or maintained by or on behalf of  
2 an agency; or

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

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

14 “(C) reporting requirements, consistent  
15 with relevant law, regarding information secu-  
16 rity incidents;

17 “(D) requirements for agencywide informa-  
18 tion security programs, including continuous  
19 monitoring of information security;

20 “(E) performance requirements and  
21 metrics for the security of agency information  
22 systems;

23 “(F) training requirements to ensure that  
24 agencies are able to fully and timely comply

1 with directions issued by the Secretary under  
2 this subchapter;

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

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

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

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

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

21 “(4) operate consolidated intrusion detection,  
22 prevention, or other protective capabilities and use  
23 associated countermeasures for the purpose of pro-  
24 tecting agency information and information systems  
25 from information security threats;

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

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

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

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

16                 “(A) standards and guidelines developed  
17                 for national security systems; and

18                 “(B) policies and directives issues by the  
19                 Secretary of Defense, Director of the Central  
20                 Intelligence Agency, and Director of National  
21                 Intelligence under subsection (g)(1); and

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

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

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

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

7                   “(D) significant deficiencies in agency in-  
8                   formation security practices as identified in the  
9                   reports, assessments, and evaluations referred  
10                  to in subparagraphs (A), (B), and (C), or other-  
11                  wise; and

12                  “(E) planned remedial action to address  
13                  any deficiencies identified under subparagraph  
14                  (D).

15           “(c) ISSUING POLICIES AND DIRECTIVES.—When  
16           issuing policies and directives under subsection (b), the  
17           Secretary shall consider any applicable standards or guide-  
18           lines developed by the National Institute of Standards and  
19           Technology and issued by the Secretary of Commerce  
20           under section 11331 of title 40. The Secretary shall con-  
21           sult with the Director of the National Institute of Stand-  
22           ards and Technology when such policies and directives im-  
23           plement standards or guidelines developed by National In-  
24           stitute of Standards and Technology. To the maximum ex-  
25           tent feasible, such standards and guidelines shall be com-

1 plementary with standards and guidelines developed for  
2 national security systems.

3 “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

4 “(1) IN GENERAL.—Notwithstanding any other  
5 provision of law, in carrying out the responsibilities  
6 under paragraphs (3) and (4) of subsection (b), if  
7 the Secretary makes a certification described in  
8 paragraph (2), the Secretary may acquire, intercept,  
9 retain, use, and disclose communications and other  
10 system traffic that are transiting to or from or  
11 stored on agency information systems and deploy  
12 countermeasures with regard to the communications  
13 and system traffic.

14 “(2) CERTIFICATION.—A certification described  
15 in this paragraph is a certification by the Secretary  
16 that—

17 “(A) the acquisitions, interceptions, and  
18 countermeasures are reasonably necessary for  
19 the purpose of protecting agency information  
20 systems from information security threats;

21 “(B) the content of communications will be  
22 collected and retained only when the commu-  
23 nication is associated with a known or reason-  
24 ably suspected information security threat, and  
25 communications and system traffic will not be

1 subject to the operation of a countermeasure  
2 unless associated with the threats;

3 “(C) information obtained under activities  
4 authorized under this subsection will only be re-  
5 tained, used, or disclosed to protect agency in-  
6 formation systems from information security  
7 threats, mitigate against such threats, or, with  
8 the approval of the Attorney General, for law  
9 enforcement purposes when—

10 “(i) the information is evidence of a  
11 crime that has been, is being, or is about  
12 to be committed; and

13 “(ii) disclosure of the information to a  
14 law enforcement agency is not otherwise  
15 prohibited by law;

16 “(D) notice has been provided to users of  
17 agency information systems concerning the po-  
18 tential for acquisition, interception, retention,  
19 use, and disclosure of communications and  
20 other system traffic; and

21 “(E) the activities are implemented pursu-  
22 ant to policies and procedures governing the ac-  
23 quisition, interception, retention, use, and dis-  
24 closure of communications and other system

1 traffic that have been reviewed and approved by  
2 the Attorney General.

3 “(3) PRIVATE ENTITIES.—The Secretary may  
4 enter into contracts or other agreements, or other-  
5 wise request and obtain the assistance of, private en-  
6 tities that provide electronic communication or infor-  
7 mation security services to acquire, intercept, retain,  
8 use, and disclose communications and other system  
9 traffic or to deploy countermeasures in accordance  
10 with this subsection.

11 “(e) DIRECTIONS TO AGENCIES.—

12 “(1) AUTHORITY.—

13 “(A) IN GENERAL.—Notwithstanding sec-  
14 tion 3554, and subject to subparagraph (B), in  
15 response to a known or reasonably suspected in-  
16 formation security threat, vulnerability, or inci-  
17 dent that represents a substantial threat to the  
18 information security of an agency, the Secretary  
19 may direct other agency heads to take any law-  
20 ful action with respect to the operation of the  
21 information systems, including those owned or  
22 operated by another entity on behalf of an  
23 agency, that collect, process, store, transmit,  
24 disseminate, or otherwise maintain agency in-  
25 formation, for the purpose of protecting the in-

1           formation system from or mitigating an infor-  
2           mation security threat.

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

7           “(2) PROCEDURES FOR USE OF AUTHORITY.—  
8           The Secretary shall—

9           “(A) in coordination with the Director of  
10          the Office of Management and Budget and, as  
11          appropriate, in consultation with operators of  
12          information systems, establish procedures gov-  
13          erning the circumstances under which a direc-  
14          tive may be issued under this subsection, which  
15          shall include—

16               “(i) thresholds and other criteria;

17               “(ii) privacy and civil liberties protec-  
18               tions; and

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

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

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

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

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

7                   “(D) notify the Director of the Office of  
8                   Management and Budget and head of any af-  
9                   fected agency immediately upon the issuance of  
10                  a directive under this subsection.

11               “(3) IMMINENT THREATS.—

12               “(A) IN GENERAL.—If the Secretary deter-  
13               mines that there is an imminent threat to agen-  
14               cy information systems and a directive under  
15               this subsection is not reasonably likely to result  
16               in a timely response to the threat, the Secretary  
17               may authorize the use of protective capabilities  
18               under the control of the Secretary for commu-  
19               nications or other system traffic transiting to or  
20               from or stored on an agency information system  
21               without prior consultation with the affected  
22               agency for the purpose of ensuring the security  
23               of the information or information system or  
24               other agency information systems.

1           “(B) LIMITATION ON DELEGATION.—The  
2 authority under this paragraph may not be del-  
3 egated to an official in a position lower than  
4 Assistant Secretary or Director of the National  
5 Cybersecurity and Communications Integration  
6 Center.

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

13               “(i) any action taken under this sub-  
14 section; and

15               “(ii) the reasons for and duration and  
16 nature of the action.

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

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

23               “(A) protect agency information from un-  
24 authorized access, use, disclosure, disruption,  
25 modification, or destruction; or

1                   “(B) require the remediation of or protect  
2                   against identified information security risks  
3                   with respect to—

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

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

10                  “(f) NATIONAL SECURITY SYSTEMS.—

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

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

20                  “(g) DELEGATION OF AUTHORITIES.—

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

24                  “(A) the Secretary of Defense in the case  
25                  of systems described in paragraph (2);

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

4                   “(C) the Director of National Intelligence  
5                   in the case of systems described in paragraph  
6                   (4).

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

16                  “(3) CENTRAL INTELLIGENCE AGENCY.—The  
17                  systems described in this paragraph are systems  
18                  that are operated by the Central Intelligence Agen-  
19                  cy, a contractor of the Central Intelligence Agency,  
20                  or another entity on behalf of the Central Intel-  
21                  ligence Agency that process any information the un-  
22                  authorized access, use, disclosure, disruption, modi-  
23                  fication, or destruction of which would have a debili-  
24                  tating impact on the mission of the Central Intel-  
25                  ligence Agency.

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

13           “(5) INTEGRATION OF INFORMATION.—The  
14 Secretary of Defense, the Director of the Central In-  
15 telligence Agency, and the Director of National In-  
16 telligence shall carry out their responsibilities under  
17 this subsection in coordination with the Secretary  
18 and share relevant information in a timely manner  
19 with the Secretary relating to the security of agency  
20 information and information systems, including sys-  
21 tems described in paragraphs (2), (3), and (4), to  
22 enable the Secretary to carry out the responsibilities  
23 set forth in this section and to maintain comprehen-  
24 sive situational awareness regarding information se-  
25 curity incidents, threats, and vulnerabilities affecting

1       agency information systems, consistent with stand-  
2       ards and guidelines for national security systems,  
3       issued in accordance with law and as directed by the  
4       President.

5       **“§ 3554. Agency responsibilities**

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

7               “(1) be responsible for—

8                       “(A) providing information security protec-  
9                       tions commensurate with the risk resulting  
10                      from unauthorized access, use, disclosure, dis-  
11                      ruption, modification, or destruction of—

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

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

21               “(B) complying with this subchapter, in-  
22       cluding—

23                      “(i) the policies and directives issued  
24                      under section 3553, including any direc-  
25                      tions under section 3553(e); and

1                   “(ii) information security policies, di-  
2                   rectives, standards, and guidelines for na-  
3                   tional security systems issued in accord-  
4                   ance with law and as directed by the Presi-  
5                   dent;

6                   “(C) complying with the requirements of  
7                   the information security standards prescribed  
8                   under section 11331 of title 40, including any  
9                   required security configuration checklists; and

10                  “(D) ensuring that information security  
11                  management processes are integrated with  
12                  agency strategic and operational planning proc-  
13                  esses;

14                  “(2) ensure that senior agency officials provide  
15                  information security for the information and infor-  
16                  mation systems that support the operations and as-  
17                  sets under the control of the officials, including  
18                  through—

19                         “(A) assessing, with a frequency commen-  
20                         surate with risk, the risk and impact that could  
21                         result from the unauthorized access, use, disclo-  
22                         sure, disruption, modification, or destruction of  
23                         the information or information systems;

24                         “(B) determining the levels of information  
25                         security appropriate to protect the information

1 and information systems in accordance with the  
2 policies and directives issued under section  
3 3553(b) and standards prescribed under section  
4 11331 of title 40;

5 “(C) implementing policies, procedures,  
6 and capabilities to reduce risks to an acceptable  
7 level in a cost-effective manner;

8 “(D) security testing and evaluation, in-  
9 cluding continuously monitoring the effective  
10 implementation of information security controls  
11 and techniques, threats, vulnerabilities, assets,  
12 and other aspects of information security as ap-  
13 propriate; and

14 “(E) reporting information about informa-  
15 tion security incidents, threats, and  
16 vulnerabilities in a timely manner as required  
17 under policies and procedures established under  
18 subsection (b)(7);

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

22 “(4) delegate to the chief information officer or  
23 equivalent official (or to a senior agency official who  
24 reports to the chief information officer or equivalent  
25 official) the authority to ensure and primary respon-

1       sibility for ensuring compliance with this subchapter,  
2       including—

3               “(A) overseeing the establishment and  
4       maintenance of an agencywide security oper-  
5       ations capability that on a continuous basis  
6       can—

7               “(i) detect, report, respond to, con-  
8       tain, and mitigate information security in-  
9       cidents that impair adequate security of  
10      the agency information and information  
11      systems in a timely manner and in accord-  
12      ance with the policies and directives issued  
13      under section 3553(b); and

14              “(ii) report any information security  
15      incident described under clause (i) to the  
16      entity designated under section 3553(b)(6);

17              “(B) developing, maintaining, and over-  
18      seeing an agencywide information security pro-  
19      gram as required under subsection (b);

20              “(C) developing, maintaining, and over-  
21      seeing information security policies, procedures,  
22      and control techniques to address all applicable  
23      requirements, including those issued under sec-  
24      tion 3553 and section 11331 of title 40;

1           “(D) training and overseeing employees  
2           and contractors of the agency with significant  
3           responsibilities for information security with re-  
4           spect to such responsibilities; and

5           “(E) assisting senior agency officials con-  
6           cerning their responsibilities under paragraph  
7           (2);

8           “(5) the agency has trained and obtained secu-  
9           rity clearances for an adequate number of employees  
10          to assist the agency in complying with this sub-  
11          chapter, including the policies and directives issued  
12          under section 3553(b);

13          “(6) ensure that the chief information officer  
14          (or other senior agency official designated under  
15          paragraph (4)), in coordination with other senior  
16          agency officials, reports to the head of the agency on  
17          the effectiveness of the agency information security  
18          program, including the progress of remedial actions;

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

22                 “(A) possesses the necessary qualifications  
23                 to administer the duties of the official under  
24                 this subchapter; and

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

“(8) ensure that senior agency officials (including component chief information officers or equivalent officials) carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (4).

8 “(b) AGENCY PROGRAM.—The head of each agency  
9 shall develop, document, and implement an agencywide in-  
10 formation security program, which shall be reviewed under  
11 section 3553(b)(2), to provide information security for the  
12 information and information systems that support the op-  
13 erations and assets of the agency, including those provided  
14 or managed by another agency, contractor, or other  
15 source, which shall include—

“(1) the development, execution, and maintenance of a risk management strategy for information security that—

19                   “(A)     considers     information     security  
20                   threats, vulnerabilities, and consequences;

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

24 “(2) policies and procedures that—

1           “(A) are based on the risk management  
2           strategy and assessment results required under  
3           paragraph (1);

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

6           “(C) ensure that cost-effective and ade-  
7           quate information security is addressed  
8           throughout the life cycle of each agency infor-  
9           mation system; and

10          “(D) ensure compliance with—

11               “(i) this subchapter;

12               “(ii) the information security policies  
13              and directives issued under section  
14              3553(b); and

15               “(iii) any other applicable require-  
16              ments;

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

20          “(4) security awareness training developed in  
21          accordance with the requirements issued under sec-  
22          tion 3553(b) to inform individuals with access to  
23          agency information systems, including information  
24          security employees, contractors, and other users of

1 information systems that support the operations and  
2 assets of the agency, of—

3 “(A) information security risks associated  
4 with their activities;

5 “(B) their responsibilities in complying  
6 with agency policies and procedures designed to  
7 reduce those risks;

8 “(C) requirements for fulfilling privacy,  
9 civil rights, civil liberties, and other information  
10 oversight responsibilities; and

11 “(D) methods for individuals to report  
12 risks and incidents to relevant Offices of In-  
13 spectors General and the Secretary under sec-  
14 tion 106 of the Cybersecurity Act of 2012;

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

17 “(A) risk-based continuous monitoring of  
18 the operational status and security of agency  
19 information systems to enable evaluation of the  
20 effectiveness of and compliance with informa-  
21 tion security policies, procedures, and practices,  
22 including a relevant and appropriate selection of  
23 management, operational, and technical controls  
24 of information systems identified in the inven-  
25 tory required under section 3505(c);

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

6           “(C) vulnerability scanning, intrusion de-  
7           tection and prevention, and penetration testing,  
8           in accordance with the requirements issued  
9           under section 3553(b); and

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

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

19          “(7) policies and procedures to ensure detec-  
20          tion, mitigation, reporting, and responses to infor-  
21          mation security incidents, in accordance with the  
22          policies and directives issued under section 3553(b),  
23          including—

24                 “(A) ensuring timely internal reporting of  
25                 information security incidents;

1 “(B) establishing and maintaining appro-  
2 priate technical capabilities to detect and miti-  
3 gate risks associated with information security  
4 incidents;

5 “(C) notifying and consulting with the en-  
6 tity designated by the Secretary under section  
7 3553(b)(6); and

8 “(D) notifying and consulting with—

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

11 “(ii) relevant committees of Congress,  
12 as appropriate; and

13 “(iii) any other entity, in accordance  
14 with law and as directed by the President;  
15 and

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

19 “(c) ANNUAL AGENCY REPORTING.—The head of  
20 each agency shall—

21 “(1) report annually to the Committee on Gov-  
22 ernment Reform and the Committee on Science,  
23 Space, and Technology of the House of Representa-  
24 tives, the Committee on Homeland Security and  
25 Governmental Affairs and the Committee on Com-

1 merce, Science, and Transportation of the Senate,  
2 any other appropriate committees of Congress, and  
3 the Secretary on the adequacy and effectiveness of  
4 information security policies, procedures, and prac-  
5 tices, including—

6 “(A) a description of each major informa-  
7 tion security incident, or set of related inci-  
8 dents, resulting in significant compromise of in-  
9 formation security, including a summary of—

10 “(i) the threats, vulnerabilities, and  
11 impact of the incident;

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

15 “(iii) the detection and response ac-  
16 tions taken;

17 “(B) the number of information security  
18 incidents within the agency resulting in signifi-  
19 cant compromise of information security, pre-  
20 sented by system impact level, type of incident,  
21 and location;

22 “(C) the total number of information secu-  
23 rity incidents within the agency, presented by  
24 system impact level, type of incident, and loca-  
25 tion;

1                   “(D) an identification and analysis of, in-  
2                   cluding actions and plans to address, any sig-  
3                   nificant deficiencies identified in such policies,  
4                   procedures and practices;

5                   “(E) any information or evaluation re-  
6                   quired under the reporting requirements issued  
7                   under section 3553(b); and

8                   “(2) address the adequacy and effectiveness of  
9                   the information security policies, procedures, and  
10                  practices of the agency as required for management  
11                  and budget plans and reports, as appropriate.

12               “(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—  
13               Notwithstanding any other provision of law, the head of  
14               each agency is authorized to allow the Secretary, or a pri-  
15               vate entity providing assistance to the Secretary under  
16               section 3553, to acquire, intercept, retain, use, and dis-  
17               close communications, system traffic, records, or other in-  
18               formation transiting to or from or stored on an agency  
19               information system for the purpose of protecting agency  
20               information and information systems from information se-  
21               curity threats or mitigating the threats in connection with  
22               the implementation of the information security capabilities  
23               authorized by paragraph (3) or (4) of section 3553(b).

1   **“§ 3555. Annual assessments**

2           “(a) IN GENERAL.—Except as provided in subsection  
3 (c), the Secretary shall conduct periodic assessments of  
4 the information security programs and practices of agen-  
5 cies based on the annual agency reports required under  
6 section 3554(c), the annual independent evaluations re-  
7 quired under section 3556, the results of any continuous  
8 monitoring, and other available information.

9           “(b) CONTENTS.—Each assessment conducted under  
10 subsection (a) shall—

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

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

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

19           “(c) CERTAIN INFORMATION SYSTEMS.—

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

24               “(2) SPECIFIC AGENCIES.—Periodic assess-  
25 ments conducted under subsection (a) shall be pre-

1       pared in accordance with governmentwide reporting  
2       requirements by—

3               “(A) the Secretary of Defense for informa-  
4               tion systems under the control of the Depart-  
5               ment of Defense;

6               “(B) the Director of the Central Intel-  
7               ligence Agency for information systems under  
8               the control of the Central Intelligence Agency;  
9               and

10              “(C) the Director of National Intelligence  
11              for information systems under the control of  
12              the Office of the Director of National Intel-  
13              ligence.

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

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

24       “(f) REPORT TO CONGRESS.—The Secretary, in co-  
25       ordination with the Secretary of Defense, the Director of

1 the Central Intelligence Agency, and the Director of Na-  
2 tional Intelligence, shall evaluate and submit to Congress  
3 an annual report on the adequacy and effectiveness of the  
4 information security programs and practices assessed  
5 under this section.

6 **“§ 3556. Independent evaluations**

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

11 “(b) CONTENTS.—Each evaluation performed under  
12 subsection (a) shall include—

13 “(1) testing of the effectiveness of information  
14 security policies, procedures, and practices of a rep-  
15 resentative subset of the information systems of the  
16 agency; and

17 “(2) an assessment of the effectiveness of the  
18 information security policies, procedures, and prac-  
19 tices of the agency.

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

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

24 “(2) at the discretion of the Inspector General  
25 of the agency, an independent entity entering a con-

1       tract with the Inspector General to perform the eval-  
2       uation; or

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

6       “(d) PREVIOUSLY CONDUCTED EVALUATIONS.—The  
7       evaluation required by this section may be based in whole  
8       or in part on a previously conducted audit, evaluation, or  
9       report relating to programs or practices of the applicable  
10      agency.

11      “(e) REPORTS.—The official or entity performing an  
12      evaluation of an agency under subsection (a) shall submit  
13      to Congress, the agency, and the Comptroller General of  
14      the United States a report regarding the evaluation. The  
15      head of the agency shall provide to the Secretary a report  
16      received under this subsection.

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

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

23               “(1) the adequacy and effectiveness of the in-  
24      formation security policies and practices of agencies;  
25      and

1 “(2) implementation of this subchapter.

2 **“§ 3557. National security systems**

3 “The head of each agency operating or exercising  
4 control of a national security system shall be responsible  
5 for ensuring that the agency—

6 “(1) provides information security protections  
7 commensurate with the risk and magnitude of the  
8 harm resulting from the unauthorized use, disclo-  
9 sure, disruption, modification, or destruction of the  
10 information contained in the national security sys-  
11 tem;

12 “(2) implements information security policies  
13 and practices as required by standards and guide-  
14 lines for national security systems issued in accord-  
15 ance with law and as directed by the President; and

16 “(3) complies with this subchapter.

17 **“§ 3558. Effect on existing law**

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

21 (b) TECHNICAL AND CONFORMING AMENDMENT.—

22 The table of sections for chapter 35 of title 44 is amended  
23 by striking the matter relating to subchapters II and III  
24 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-

1       graphs (2) and (3) of section 20(a) of the National  
2       Institute of Standards and Technology Act (15  
3       U.S.C. 278g–3(a)), the Secretary of Commerce, in  
4       consultation with the Secretary of Homeland Secu-  
5       rity, shall prescribe standards and guidelines relat-  
6       ing to Federal information systems.

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

12             “(c) MANDATORY REQUIREMENTS.—

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

20               “(2) REQUIRED MANDATORY STANDARDS.—

21                   “(A) IN GENERAL.—The Secretary of  
22       Commerce shall require executive agencies to  
23       comply with the standards described in sub-  
24       paragraph (B).

1                   “(B) CONTENTS.—The standards de-  
2                   scribed in this subparagraph are information  
3                   security standards that—

4                   “(i) provide minimum information se-  
5                   curity requirements as determined under  
6                   section 20(b) of the National Institute of  
7                   Standards and Technology Act (15 U.S.C.  
8                   278g–3(b)); and

9                   “(ii) are otherwise necessary to im-  
10                  prove the security of Federal information  
11                  and Federal information systems.

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

1       “(e) EXERCISE OF AUTHORITY.—To ensure fiscal  
2 and policy consistency, the Secretary of Commerce shall  
3 exercise the authority under this section subject to direc-  
4 tion by the President and in coordination with the Direc-  
5 tor of the Office of Management and Budget.

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

13               “(1) contain any standards with which the Sec-  
14 retary of Commerce has required the agency to com-  
15 ply; and

16               “(2) are otherwise consistent with the policies  
17 and directives issued under section 3553(b) of title  
18 44.

19       “(g) DECISIONS ON PROMULGATION OF STAND-  
20 ARDS.—The decision by the Secretary of Commerce re-  
21 garding the promulgation of any standard under this sec-  
22 tion shall occur not later than 6 months after the submis-  
23 sion of the proposed standard to the Secretary of Com-  
24 merce by the National Institute of Standards and Tech-  
25 nology, as provided under section 20 of the National Insti-

1 tute of Standards and Technology Act (15 U.S.C. 278g–  
2 3).”.

3 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

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

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

10 (A) in section 20(a)(2) (15 U.S.C. 278g–  
11 3(a)(2)), by striking “section 3532(b)(2)” and  
12 inserting “section 3552(b)”; and

13 (B) in section 21(b) (15 U.S.C. 278g–  
14 4(b))—

15 (i) in paragraph (2), by inserting “,  
16 the Secretary of Homeland Security,” after  
17 “the Institute”; and

18 (ii) in paragraph (3), by inserting  
19 “the Secretary of Homeland Security,”  
20 after “the Secretary of Commerce,”.

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

1 (4) Part IV of title 10, United States Code, is  
2 amended—

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

6 (B) in section 2223(c)(3), by striking “sec-  
7 tion 3542(b)(2)” and inserting “section  
8 3552(b)”;

9 (C) in section 2315, by striking “section  
10 3542(b)(2)” and inserting “section 3552(b)”.

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

15 **SEC. 203. SAVINGS PROVISIONS.**

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

24 (b) OTHER STANDARDS AND GUIDELINES.—Stand-  
25 ards and guidelines issued by the Secretary of Commerce

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

8 **SEC. 204. CONSOLIDATION OF EXISTING DEPARTMENTAL**  
9 **CYBER RESOURCES AND AUTHORITIES.**

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

13 **“Subtitle E—Cybersecurity**

14 **“SEC. 241. DEFINITIONS.**

15 “In this subtitle:

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

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

23 “(3) DAMAGE.—The term ‘damage’ has the  
24 meaning given that term in section 1030(e) of title  
25 18, United States Code.

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

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

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

11          “(7) FEDERAL INFORMATION INFRASTRUC-  
12          TURE.—The term ‘Federal information infrastruc-  
13          ture’—

14               “(A) means information and information  
15               systems that are owned, operated, controlled, or  
16               licensed solely for use by, or on behalf of, any  
17               Federal agency, including information systems  
18               used or operated by another entity on behalf of  
19               a Federal agency; and

20               “(B) does not include—

21                       “(i) a national security system; or

22                       “(ii) information and information sys-  
23                       tems that are owned, operated, controlled,  
24                       or licensed for use solely by, or on behalf  
25                       of, the Department of Defense, a military

1 department, or another element of the in-  
2 telligence community.

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

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

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

12 “(11) INTELLIGENCE COMMUNITY.—The term  
13 ‘intelligence community’ has the meaning given that  
14 term in section 3(4) of the National Security Act of  
15 1947 (50 U.S.C. 401a(4)).

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

1       lating to national security and emergency prepared-  
2       ness communications functions.

3               “(13) NATIONAL INFORMATION INFRASTRUC-  
4       TURE.—The term ‘national information infrastruc-  
5       ture’ means information and information systems—

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

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

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

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

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

19              “(a) ESTABLISHMENT.—There is established within  
20      the Department a National Center for Cybersecurity and  
21      Communications.

22              “(b) TRANSFER OF FUNCTIONS.—There are trans-  
23      ferred to the Center the National Cyber Security Division,  
24      the Office of Emergency Communications, and the Na-  
25      tional Communications System, including all the func-

1 tions, personnel, assets, authorities, and liabilities of the  
2 National Cyber Security Division, the Office of Emergency  
3 Communications, and the National Communications Sys-  
4 tem.

5 “(c) DIRECTOR.—The Center shall be headed by a  
6 Director, who shall be appointed by the President, by and  
7 with the advice and consent of the Senate, and who shall  
8 report directly to the Secretary.

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

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

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

20 “(3) prioritize the efforts of the Center to ad-  
21 dress the most significant risks and incidents that  
22 have caused or are likely to cause damage to the  
23 Federal information infrastructure, the national in-  
24 formation infrastructure, and national security and

1 emergency preparedness communications infrastruc-  
2 ture of the United States;

3 “(4) ensure, in coordination with the privacy of-  
4 ficer designated under subsection (j), the privacy of-  
5 ficer appointed under section 222, and the Director  
6 of the Office of Civil Rights and Civil Liberties ap-  
7 pointed under section 705, that the activities of the  
8 Center comply with all policies, regulations, and laws  
9 protecting the privacy and civil liberties of United  
10 States persons; and

11 “(5) perform such other duties as the Secretary  
12 may require relating to the security and resiliency of  
13 the Federal information infrastructure, national in-  
14 formation infrastructure, and the national security  
15 and emergency preparedness communications infra-  
16 structure of the United States.

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

19 “(1) engage in activities and otherwise coordi-  
20 nate Federal efforts to identify, protect against, re-  
21 mediate, and mitigate, respond to, and recover from  
22 cybersecurity threats, consequences, vulnerabilities  
23 and incidents impacting the Federal information in-  
24 frastructure and the national information infrastruc-  
25 ture, including by providing support to entities that

1 own or operate national information infrastructure,  
2 at their request;

3 “(2) conduct risk-based assessments of the Fed-  
4 eral information infrastructure, and risk assessments  
5 of critical infrastructure;

6 “(3) develop, oversee the implementation of,  
7 and enforce policies, principles, and guidelines on in-  
8 formation security for the Federal information infra-  
9 structure, including exercise of the authorities under  
10 the Federal Information Security Management Act  
11 of 2002 (title III of Public Law 107–347; 116 Stat.  
12 2946);

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

20 “(5) oversee the responsibilities related to na-  
21 tional security and emergency preparedness commu-  
22 nications infrastructure, including the functions of  
23 the Office of Emergency Communications and the  
24 National Communications System;

1           “(6)(A) maintain comprehensive situational  
2 awareness of the security of the Federal information  
3 infrastructure and the national information infra-  
4 structure for the purpose of enabling and supporting  
5 activities under subparagraph (e)(1); and

6           “(B) receive and distribute classified and un-  
7 classified information from and to entities that own  
8 or operate national information infrastructure to  
9 support efforts by such entities to secure such infra-  
10 structure and for enhancing overall situational  
11 awareness;

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

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

24           “(9) consult, in coordination with the Secretary  
25 of State, with appropriate international partners to

1       enhance the security of the Federal information in-  
2       frastructure, national information infrastructure,  
3       and information infrastructure located outside the  
4       United States the disruption of which could result in  
5       national or regional catastrophic damage in the  
6       United States;

7               “(10) coordinate the activities undertaken by  
8       Federal agencies to—

9               “(A) protect Federal information infra-  
10       structure and national information infrastruc-  
11       ture; and

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

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

21       “(f) USE OF EXISTING MECHANISMS FOR COLLABO-  
22       RATION.—To avoid unnecessary duplication or waste, in  
23       carrying out the authorities and responsibilities of the  
24       Center under this subtitle, to the maximum extent prac-  
25       ticable, the Director of the Center shall make use of exist-

1 ing mechanisms for collaboration and information sharing,  
2 including mechanisms relating to the identification and  
3 communication of cybersecurity threats, vulnerabilities,  
4 and associated consequences, established by other compo-  
5 nents of the Department or other Federal agencies and  
6 the information sharing mechanisms established under  
7 title VII of the Cybersecurity Act of 2012.

8 “(g) DEPUTY DIRECTORS.—

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

11 “(A) have expertise in infrastructure pro-  
12 tection; and

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

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

1 Center and the Director of National Intelligence,  
2 and, while serving as Deputy Director, shall report  
3 directly to the Director of the Center.

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

9 “(i) LIAISON OFFICERS.—

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

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

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

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

4       “(k) SUFFICIENCY OF RESOURCES PLAN.—

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

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

21       “(l) NO RIGHT OR BENEFIT.—The provision of as-  
22 sistance or information under this section to governmental  
23 or private entities that own or operate critical infrastruc-  
24 ture shall be at the discretion of the Secretary. The provi-  
25 sion of certain assistance or information to a governmental

1 or private entity pursuant to this section shall not create  
2 a right or benefit, substantive or procedural, to similar  
3 assistance or information for any other governmental or  
4 private entity.

5 **“SEC. 243. DEPARTMENT OF HOMELAND SECURITY INFOR-**  
6 **MATION SHARING.**

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

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

21 “(2) expand and enhance the sharing of timely  
22 and actionable cybersecurity threat and vulnerability  
23 information by the Federal Government with owners  
24 and operators of the national information infrastruc-  
25 ture;

1           “(3) establish a method of accessing classified  
2           or unclassified information, as appropriate and in  
3           accordance with applicable laws protecting trade se-  
4           crets, that will provide situational awareness of the  
5           security of the Federal information infrastructure  
6           and the national information infrastructure relating  
7           to cybersecurity threats, and vulnerabilities, includ-  
8           ing traffic, trends, incidents, damage, and other  
9           anomalous activities affecting the Federal informa-  
10          tion infrastructure or the national information infra-  
11          structure;

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

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

21          “(b) VOLUNTARILY SHARED INFORMATION.—

22           “(1) IN GENERAL.—The Director of the Center  
23          shall ensure that information submitted in accord-  
24          ance with this section by States and units of local  
25          governments, private entities, and international part-

1       ners of the United States regarding threats,  
2       vulnerabilities, incidents, and anomalous activities  
3       affecting the national information infrastructure,  
4       Federal information infrastructure, or information  
5       infrastructure that is owned, operated, controlled, or  
6       licensed solely for use by, or on behalf of, the De-  
7       partment of Defense, a military department, or an-  
8       other element of the intelligence community is treat-  
9       ed as voluntarily shared critical infrastructure infor-  
10      mation under section 214 as requested by submit-  
11      ting entities.

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

14                   “(A) conceal violations of law, inefficiency,  
15                   or administrative error;

16                   “(B) prevent embarrassment to a person,  
17                   organization, or agency; or

18                   “(C) interfere with competition in the pri-  
19                   vate sector.

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

1 “(d) FEDERAL AGENCIES.—

2 “(1) INFORMATION SHARING PROGRAM.—The  
3 Director of the Center, in consultation with the  
4 members of the Chief Information Officers Council  
5 established under section 3603 of title 44, United  
6 States Code, shall establish a program for sharing  
7 information with and between the Center and other  
8 Federal agencies that includes processes and proce-  
9 dures—

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

23 “(B) under which Federal agencies provide  
24 the Director of the Center, upon request, with  
25 information concerning the security of the Fed-

1           eral information infrastructure, information in-  
2           frastructure that is owned, operated, controlled,  
3           or licensed for use by, or on behalf of, the De-  
4           partment of Defense, a military department, or  
5           another element of the intelligence community,  
6           or the national information infrastructure nec-  
7           essary to carry out the duties of the Director of  
8           the Center under this subtitle or any other pro-  
9           vision of law.

10          “(2) ACCESS TO INFORMATION.—

11               “(A) IN GENERAL.—The Director of the  
12          Center shall ensure—

13                   “(i) that the head of each Federal  
14                   agency has timely access to data, including  
15                   appropriate raw and processed data, re-  
16                   garding the information infrastructure of  
17                   the Federal agency; and

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

1           “(B) COMPLIANCE.—The head of a Fed-  
2           eral agency shall comply with all processes and  
3           procedures established under this subsection re-  
4           garding notification to the Director of the Cen-  
5           ter relating to incidents.

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

13   **“SEC. 244. PROHIBITED CONDUCT.**

14          “None of the authorities provided under this subtitle  
15   shall authorize the Director of the Center, the Center, the  
16   Department, or any other Federal entity to—

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

20          “(2) intercept a wire, oral, or electronic commu-  
21          nication (as those terms are defined in section 2510  
22          of title 18, United States Code), access a stored  
23          electronic or wire communication, install or use a  
24          pen register or trap and trace device, or conduct  
25          electronic surveillance (as defined in section 101 of

1 the Foreign Intelligence Surveillance Act of 1978  
2 (50 U.S.C.1801)) relating to an incident unless oth-  
3 erwise authorized under chapter 119, chapter 121,  
4 or chapter 206 of title 18, United States Code, or  
5 the Foreign Intelligence Surveillance Act of 1978  
6 (50 U.S.C. 1801 et seq.).”.

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

“Subtitle E—Cybersecurity

“Sec. 241. Definitions.

“Sec. 242. Consolidation of existing resources.

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

“Sec. 244. Prohibited conduct.”.

## 12 **TITLE III—RESEARCH AND** 13 **DEVELOPMENT**

### 14 **SEC. 301. FEDERAL CYBERSECURITY RESEARCH AND DE-** 15 **VELOPMENT.**

16 (a) FUNDAMENTAL CYBERSECURITY RESEARCH.—  
17 The Director of the Office of Science and Technology Pol-  
18 icy (referred to in this section as the “Director”), in co-  
19 ordination with the Secretary and the head of any relevant  
20 Federal agency, shall build upon programs and plans in  
21 effect as of the date of enactment of this Act to develop

1 a national cybersecurity research and development plan,  
2 which shall be updated biennially.

3 (b) REQUIREMENTS.—The plan required to be devel-  
4 oped under subsection (a) shall encourage computer and  
5 information science and engineering research to meet chal-  
6 lenges in cybersecurity, including—

7 (1) how to design and build complex software-  
8 intensive systems that are secure and reliable when  
9 first deployed;

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

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

16 (4) how to guarantee the privacy of the iden-  
17 tity, information, or lawful transactions of an indi-  
18 vidual when stored in distributed systems or trans-  
19 mitted over networks;

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

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

1           (7) how to support privacy in conjunction with  
2           improved security;

3           (8) how to address the growing problem of in-  
4           sider threat;

5           (9) how improved consumer education and dig-  
6           ital literacy initiatives can address human factors  
7           that contribute to cybersecurity;

8           (10) how to protect information stored through  
9           cloud computing or transmitted through wireless  
10          services;

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

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

17          (c) CYBERSECURITY PRACTICES RESEARCH.—The  
18          Director of the National Science Foundation shall support  
19          research—

20               (1) that develops, evaluates, disseminates, and  
21               integrates new cybersecurity practices and concepts  
22               into the core curriculum of computer science pro-  
23               grams and of other programs where graduates of  
24               such programs have a substantial probability of de-  
25               veloping software after graduation, including new

1 practices and concepts relating to secure coding edu-  
2 cation and improvement programs; and

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

6 (d) CYBERSECURITY MODELING AND TEST BEDS.—

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

12 (2) ESTABLISHMENT OF PROGRAM.—

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

22 (B) REQUIREMENT.—The test beds estab-  
23 lished under subparagraph (A) shall be suffi-  
24 ciently large in order to model the scale and

1 complexity of real world networks and environ-  
2 ments.

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

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

15 (1) the National Institute of Standards and  
16 Technology;

17 (2) the Department;

18 (3) other Federal agencies;

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

23 (5) international partners of the United States.

24 (f) 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;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5               “(B) the National Science Foundation;

6               “(C) the National Academy of Sciences;

7               “(D) other Federal agencies;

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

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

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

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

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

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

“(5) shall submit a report to the appropriate committees of Congress on a review of the cybersecurity activities, and the capacity, of the national laboratories and other research entities available to the Department to determine if the establishment of a national laboratory dedicated to cybersecurity research and development is necessary.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—

The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.), as amended by section 204, is amended by inserting after the item relating to section 237 the following:

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

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

(a) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director of the National Science Foundation, in coordination with the Secretary, shall establish cybersecurity research centers based at institutions of higher education and other entities that meet the criteria described in subsection (b) to develop solutions and strategies that support the efforts of the Federal government under this Act in—

(1) improving the security and resilience of information infrastructure;

24 (2) reducing cyber vulnerabilities; and

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

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

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

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

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

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

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

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

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

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

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

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

17 **SEC. 401. DEFINITIONS.**

18 In this title:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 (d) COLLABORATIVE EDUCATION AND TRAINING.—

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

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

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

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

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

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

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

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

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

9 (a) TALENT COMPETITION AND CHALLENGE.—

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

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

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

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

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

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

9 (E) veterans; and

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

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

19 (A) Federal agencies;

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

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

24 (D) other private sector organizations.

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

4                   (A) ethical hacking;

5                   (B) penetration testing;

6                   (C) vulnerability assessment;

7                   (D) continuity of system operations;

8                   (E) cyber forensics;

9                   (F) offensive and defensive cyber oper-  
10       ations; and

11                   (G) other areas to fulfill the cybersecurity  
12       mission as the Secretary determines appro-  
13       priate.

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

21       (b) NATIONAL RESEARCH AND DEVELOPMENT COM-  
22       PETITION AND CHALLENGE.—

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

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

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

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

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

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

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

20 (E) veterans; and

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

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

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

6                   (B) may empanel advisory committees.

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

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

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

1 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

2 The program established under subsection (a) shall—

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

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

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

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

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

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

7 (c) HIRING AUTHORITY.—

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

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

16 (B) exempt from competitive service.

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

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

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

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

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

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

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

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

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

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

5 (b) STRATEGY.—

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

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

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

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

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

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

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

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

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

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

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

22 (b) TRAINING.—

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

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

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

12 (A) role-based security awareness training;

13 (B) recommended cybersecurity practices;

14 (C) cybersecurity recommendations for  
15 traveling abroad;

16 (D) unclassified counterintelligence infor-  
17 mation;

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

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

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

24 (H) identity management information;

1 (I) information regarding supply chain se-  
2 curity;

3 (J) information security risks associated  
4 with the activities of Federal employees and  
5 contractors; and

6 (K) the responsibilities of Federal employ-  
7 ees and contractors in complying with policies  
8 and procedures designed to reduce information  
9 security risks identified under subparagraph  
10 (J).

11 (3) FEDERAL CYBERSECURITY PROFES-  
12 SIONALS.—The Director of the Office of Personnel  
13 Management in conjunction with the Secretary, the  
14 Director of National Intelligence, the Secretary of  
15 Defense, the Director of the Office of Management  
16 and Budget, and, as appropriate, colleges, univer-  
17 sities, and nonprofit organizations with cybersecurity  
18 training expertise, shall develop a program to pro-  
19 vide training to improve and enhance the skills and  
20 capabilities of Federal employees engaged in the cy-  
21 bersecurity mission, including training specific to the  
22 acquisition workforce.

23 (4) HEADS OF FEDERAL AGENCIES.—Not later  
24 than 30 days after the date on which an individual  
25 is appointed to a position at level I or II of the Ex-

1       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) RECRUITMENT.—The Director of the Office of  
12      Personnel Management, in coordination with the Director  
13      of the National Center for Cybersecurity and Communica-  
14      tions, shall develop strategies and programs to recruit stu-  
15      dents enrolled in institutions of higher education and stu-  
16      dents enrolled in career and technical institutions in the  
17      United States to serve as Federal employees engaged in  
18      cybersecurity missions.

19      (d) LEADERSHIP IN CYBERSECURITY.—The head of  
20      each Federal agency shall adopt best practices, developed  
21      by the Office of Personnel Management, regarding effec-  
22      tive ways to educate and motivate employees of the Fed-  
23      eral Government to demonstrate leadership in cybersecu-  
24      rity, including—

1           (1) promotions and other nonmonetary awards;  
2       and

3           (2) publicizing information sharing accomplish-  
4       ments by individual employees and, if appropriate,  
5       the tangible benefits that resulted.

6   **SEC. 408. NATIONAL CENTER FOR CYBERSECURITY AND**  
7                   **COMMUNICATIONS ACQUISITION AUTHORI-**  
8                   **TIES.**

9       (a) IN GENERAL.—Subtitle E of title II of the Home-  
10   land Security Act of 2002, as added by section 204, is  
11   amended by adding at the end the following:

12   **“SEC. 245. NATIONAL CENTER FOR CYBERSECURITY AND**  
13                   **COMMUNICATIONS ACQUISITION AUTHORI-**  
14                   **TIES.**

15       “(a) IN GENERAL.—The National Center for Cyber-  
16   security and Communications is authorized to use the au-  
17   thorities under subsections (c)(1) and (d)(1)(B) of section  
18   2304 of title 10, United States Code, instead of the au-  
19   thorities under subsections (a)(1) and (b)(2) of section  
20   3304 of title 41, United States Code, subject to all other  
21   requirements of sections 3301 and 3304 of title 41, United  
22   States Code.

23       “(b) GUIDELINES.—Not later than 90 days after the  
24   date of enactment of the Cybersecurity Act of 2012, the

1 chief procurement officer of the Department shall issue  
2 guidelines for use of the authority under subsection (a).

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

7 “(d) REPORTING.—

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

11 “(A) the Committee on Homeland Security  
12 and Governmental Affairs of the Senate; and

13 “(B) the Committee on Homeland Security  
14 of the House of Representatives.

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

17 “(A) the number of contract actions taken  
18 under the authority under subsection (a) during  
19 the period covered by the report; and

20 “(B) for each contract action described in  
21 subparagraph (A)—

22 “(i) the total dollar value of the con-  
23 tract action;

24 “(ii) a summary of the market re-  
25 search conducted by the National Center

1 for Cybersecurity and Communications, in-  
2 cluding a list of all offerors who were con-  
3 sidered and those who actually submitted  
4 bids, in order to determine that use of the  
5 authority was appropriate; and

6 “(iii) a copy of the justification and  
7 approval documents required by section  
8 3304(e) of title 41, United States Code.

9 “(3) CLASSIFIED ANNEX.—A report submitted  
10 under this subsection shall be submitted in an un-  
11 classified form, but may include a classified annex,  
12 if necessary.

13 **“SEC. 246. RECRUITMENT AND RETENTION PROGRAM FOR**  
14 **THE NATIONAL CENTER FOR CYBERSECU-**  
15 **RITY AND COMMUNICATIONS.**

16 “(a) DEFINITIONS.—In this section:

17 “(1) COLLECTIVE BARGAINING AGREEMENT.—  
18 The term ‘collective bargaining agreement’ has the  
19 meaning given that term in section 7103(a)(8) of  
20 title 5, United States Code.

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

25 “(b) GENERAL AUTHORITY.—

1           “(1) ESTABLISH POSITIONS, APPOINT PER-  
2       SONNEL, AND FIX RATES OF PAY.—The Secretary  
3       may exercise with respect to qualified employees of  
4       the Department the same authority of that the Sec-  
5       retary of Defense has with respect to civilian intel-  
6       ligence personnel under sections 1601, 1602, and  
7       1603 of title 10, United States Code, to establish as  
8       positions in the excepted service, to appoint individ-  
9       uals to those positions, and fix pay. Such authority  
10      shall be exercised subject to the same conditions and  
11      limitations applicable to the Secretary of Defense  
12      with respect to civilian intelligence personnel of the  
13      Department of Defense.

14          “(2) SCHOLARSHIP PROGRAM.—The Secretary  
15      may exercise with respect to qualified employees of  
16      the Department the same authority of the Secretary  
17      of Defense has with respect to civilian personnel  
18      under section 2200a of title 10, United States Code,  
19      to the same extent, and subject to the same condi-  
20      tions and limitations, that the Secretary of Defense  
21      may exercise such authority with respect to civilian  
22      personnel of the Department of Defense.

23          “(3) PLAN FOR EXECUTION OF AUTHORI-  
24      TIES.—Not later than 120 days after the date of en-  
25      actment of this subtitle, the Secretary shall submit

1 a report to the appropriate committees of Congress  
2 with a plan for the use of the authorities provided  
3 under this subsection.

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

12 “(5) REQUIRED REGULATIONS.—The Secretary,  
13 in coordination with the Director of the Center and  
14 the Director of the Office of Personnel Management,  
15 shall prescribe regulations for the administration of  
16 this section.

17 “(c) MERIT SYSTEM PRINCIPLES AND CIVIL SERVICE  
18 PROTECTIONS: APPLICABILITY.—

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

24 “(2) CIVIL SERVICE PROTECTIONS.—Section  
25 1221, section 2302, and chapter 75 of title 5,

1 United States Code, shall apply to the positions es-  
2 tablished under subsection (b)(1).

3 “(d) REQUIREMENTS.—Before the initial exercise of  
4 any authority authorized under subsection (b)(1) the Sec-  
5 retary shall—

6 “(1) seek input from affected employees, and  
7 the union representatives of affected employees as  
8 applicable, and Federal manager and professional  
9 associations into the design and implementation of a  
10 fair, credible, and transparent system for exercising  
11 any authority under subsection (b)(1);

12 “(2) make a good faith attempt to resolve any  
13 employee concerns regarding proposed changes in  
14 conditions of employment through discussions with  
15 the groups described in paragraph (1);

16 “(3) develop a program to provide training to  
17 supervisors of cybersecurity employees at the De-  
18 partment on the use of the new authorities, includ-  
19 ing actions, options, and strategies a supervisor may  
20 use in—

21 “(A) developing and discussing relevant  
22 goals and objectives with the employee, commu-  
23 nicating and discussing progress relative to per-  
24 formance goals and objectives, and conducting  
25 performance appraisals;

1           “(B) mentoring and motivating employees,  
2           and improving employee performance and pro-  
3           ductivity;

4           “(C) fostering a work environment charac-  
5           terized by fairness, respect, equal opportunity,  
6           and attention to the quality of work of the em-  
7           ployees;

8           “(D) effectively managing employees with  
9           unacceptable performance;

10           “(E) addressing reports of a hostile work  
11           environment, reprisal, or harassment of or by  
12           another supervisor or employee; and

13           “(F) otherwise carrying out the duties and  
14           responsibilities of a supervisor;

15           “(4) develop a program to provide training to  
16           supervisors of cybersecurity employees at the De-  
17           partment on the prohibited personnel practices  
18           under section 2302 of title 5, United States Code,  
19           (particularly with respect to the practices described  
20           in paragraphs (1) and (8) of section 2302(b) of title  
21           5, United States Code), employee collective bar-  
22           gaining and union participation rights, and the pro-  
23           cedures and processes used to enforce employee  
24           rights; and

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

3           “(A) sharing knowledge and advice in  
4           areas such as communication, critical thinking,  
5           responsibility, flexibility, motivating employees,  
6           teamwork, leadership, and professional develop-  
7           ment; and

8           “(B) pointing out strengths and areas for  
9           development.

10          “(e) SUPERVISOR REQUIREMENT.—

11           “(1) IN GENERAL.—Except as provided in para-  
12           graph (2), not later than 1 year after the date of en-  
13           actment of the Cybersecurity Act of 2012 and every  
14           3 years thereafter, every supervisor of cybersecurity  
15           employees at the Department shall complete the pro-  
16           grams established under paragraphs (3) and (4) of  
17           subsection (d).

18           “(2) EXCEPTION.—A supervisor of cybersecu-  
19           rity employees at the Department who is appointed  
20           after the date of enactment of the Cybersecurity Act  
21           of 2012 shall complete the programs established  
22           under paragraphs (3) and (4) of subsection (d) not  
23           later than 1 year after the date on which the super-  
24           visor is appointed to the position, and every 3 years  
25           thereafter.

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

5           “(f) CONVERSION TO COMPETITIVE SERVICE.—In  
6       consultation with the Director of the Center, the Secretary  
7       may grant competitive civil service status to a qualified  
8       employee appointed to the excepted service under sub-  
9       section (b) if that employee is employed in the Center or  
10      is transferring to the Center.

11          “(g) ANNUAL REPORT.—Not later than 1 year after  
12      the date of enactment of this subtitle, and every year  
13      thereafter for 4 years, the Secretary shall submit to the  
14      appropriate committees of Congress a detailed report  
15      that—

16           “(1) discusses the process used by the Sec-  
17      retary in accepting applications, assessing can-  
18      didates, ensuring adherence to veterans’ preference,  
19      and selecting applicants for vacancies to be filled by  
20      a qualified employee;

21           “(2) describes—

22           “(A) how the Secretary plans to fulfill the  
23      critical need of the Department to recruit and  
24      retain qualified employees;

1 “(B) the measures that will be used to  
2 measure progress; and

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

5 “(3) discusses how the planning and actions  
6 taken under paragraph (2) are integrated into the  
7 strategic workforce planning of the Department;

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

10 “(A) the number of qualified employees  
11 hired by occupation and grade and level or pay  
12 band;

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

14 “(C) the number of separations of qualified  
15 employees by occupation and grade and level or  
16 pay band;

17 “(D) the number of retirements of quali-  
18 fied employees by occupation and grade and  
19 level or pay band; and

20 “(E) the number and amounts of recruit-  
21 ment, relocation, and retention incentives paid  
22 to qualified employees by occupation and grade  
23 and level or pay band.”.

24 (b) TECHNICAL AND CONFORMING AMENDMENT.—

25 The table of contents in section 1(b) of the Homeland Se-

1   curity Act of 2002 (6 U.S.C. 101 et seq.), as amended  
2   by section 204, is amended by inserting after the item re-  
3   lating to section 244 the following:

“Sec. 245. National Center for Cybersecurity and Communications acquisition  
authorities.

“Sec. 246. Recruitment and retention program for the national center for cy-  
bersecurity and communications.”.

4   **SEC. 409. REPORTS ON CYBER INCIDENTS AGAINST GOV-**  
5                   **ERNMENT NETWORKS.**

6           (a) DEPARTMENT OF HOMELAND SECURITY.—Not  
7   later than 180 days after the date of enactment of this  
8   Act, and annually thereafter, the Secretary shall submit  
9   to Congress a report that—

10           (1) summarizes major cyber incidents involving  
11   networks of Executive agencies (as defined in section  
12   105 of title 5, United States Code), except for the  
13   Department of Defense;

14           (2) provides aggregate statistics on the number  
15   of breaches of networks of Executive agencies, the  
16   volume of data exfiltrated, and the estimated cost of  
17   remedying the breaches; and

18           (3) discusses the risk of cyber sabotage.

19           (b) DEPARTMENT OF DEFENSE.—Not later than 180  
20   days after the date of enactment of this Act, and annually  
21   thereafter, the Secretary of Defense shall submit to Con-  
22   gress a report that—

1           (1) summarizes major cyber incidents against  
2       networks of the Department of Defense and the  
3       military departments;

4           (2) provides aggregate statistics on the number  
5       of breaches against networks of the Department of  
6       Defense and the military departments, the volume of  
7       data exfiltrated, and the estimated cost of remedying  
8       the breaches; and

9           (3) discusses the risk of cyber sabotage.

10       (c) FORM OF REPORTS.—Each report submitted  
11   under this section shall be in unclassified form, but may  
12   include a classified annex as necessary to protect sources,  
13   methods, and national security.

14       (d) CONTENTS OF REPORTS.—Each report submitted  
15   under this section may be based in whole or in part on  
16   the reporting requirements under section 3553 of chapter  
17   35 of title 44, United States Code, as amended by this  
18   Act.

19   **SEC. 410. REPORTS ON PROSECUTION FOR CYBERCRIME.**

20       (a) IN GENERAL.—Not later than 180 days after the  
21   date of enactment of this Act, the Attorney General and  
22   the Directors of the Federal Bureau of Investigation and  
23   the United States Secret Service shall submit to Congress  
24   reports—

1           (1) describing investigations and prosecutions  
2 relating to cyber intrusions or other cybercrimes the  
3 preceding year, including—

4               (A) the number of investigations initiated  
5 relating to such crimes;

6               (B) the number of arrests relating to such  
7 crimes;

8               (C) the number and description of in-  
9 stances in which investigations or prosecutions  
10 relating to such crimes have been delayed or  
11 prevented because of an inability to extradite a  
12 criminal defendant in a timely manner; and

13               (D) the number of prosecutions for such  
14 crimes, including—

15                   (i) the number of defendants pros-  
16 ecuted;

17                   (ii) whether the prosecutions resulted  
18 in a conviction;

19                   (iii) the sentence imposed and the  
20 statutory maximum for each such crime  
21 for which a defendant was convicted; and

22                   (iv) the average sentence imposed for  
23 a conviction of such crimes;

24           (2) identifying the number of employees, finan-  
25 cial resources, and other resources (such as tech-

1 nology and training) devoted to the enforcement, in-  
2 vestigation, and prosecution of cyber intrusions or  
3 other cybercrimes, including the number of inves-  
4 tigators, prosecutors, and forensic specialists dedi-  
5 cated to investigating and prosecuting cyber intru-  
6 sions or other cybercrimes; and

7 (3) discussing any impediments under the laws  
8 of the United States or international law to prosecu-  
9 tions for cyber intrusions or other cybercrimes.

10 (b) UPDATES.—The Attorney General and the Direc-  
11 tors of the Federal Bureau of Investigation and the  
12 United States Secret Service shall annually submit to Con-  
13 gress reports updating the reports submitted under sub-  
14 section (a) at the same time the Attorney General and  
15 the Directors submit annual reports under section 404 of  
16 the Prioritizing Resources and Organization for Intellect-  
17 ual Property Act of 2008 (42 U.S.C. 3713d).

18 **SEC. 411. REPORT ON RESEARCH RELATING TO SECURE**  
19 **DOMAIN.**

20 (a) IN GENERAL.—The Secretary shall enter into a  
21 contract with the National Research Council, or another  
22 federally funded research and development corporation,  
23 under which the Council or corporation shall submit to  
24 Congress reports on available technical options, consistent  
25 with constitutional and statutory privacy rights, for en-

1 hancing the security of the information networks of enti-  
2 ties that own or manage critical infrastructure through—

3 (1) technical improvements, including devel-  
4 oping a secure domain; or

5 (2) increased notice of and consent to the use  
6 of technologies to scan for, detect, and defeat cyber  
7 security threats, such as technologies used in a se-  
8 cure domain.

9 (b) **TIMING.**—The contract entered into under sub-  
10 section (a) shall require that the report described in sub-  
11 section (a) be submitted—

12 (1) not later than 180 days after the date of  
13 enactment of this Act;

14 (2) annually, after the first report submitted  
15 under subsection (a), for 3 years; and

16 (3) more frequently, as determined appropriate  
17 by the Secretary in response to new risks or tech-  
18 nologies that emerge.

19 **SEC. 412. REPORT ON PREPAREDNESS OF FEDERAL**  
20 **COURTS TO PROMOTE CYBERSECURITY.**

21 Not later than 180 days after the date of enactment  
22 of this Act, the Attorney General, in coordination with the  
23 Administrative Office of the United States Courts, shall  
24 submit to Congress a report—

1           (1) on whether Federal courts have granted  
2           timely relief in matters relating to botnets and other  
3           cybercrime and cyber security threats; and

4           (2) that includes, as appropriate, recommenda-  
5           tions on changes or improvements to—

6                   (A) the Federal Rules of Civil Procedure  
7                   or the Federal Rules of Criminal Procedure;

8                   (B) the training and other resources avail-  
9                   able to support the Federal judiciary;

10                  (C) the capabilities and specialization of  
11                  courts to which such cases may be assigned;  
12                  and

13                  (D) Federal civil and criminal laws.

14 **SEC. 413. REPORT ON IMPEDIMENTS TO PUBLIC AWARE-**  
15 **NESS.**

16           Not later than 180 days after the date of enactment  
17 of this Act, and annually thereafter for 3 years (or more  
18 frequently if determined appropriate by the Secretary) the  
19 Secretary shall submit to Congress a report on—

20           (1) legal or other impediments to appropriate  
21           public awareness of—

22                   (A) the nature of, methods of propagation  
23                   of, and damage caused by common cyber secu-  
24                   rity threats such as computer viruses, phishing  
25                   techniques, and malware;

1 (B) the minimal standards of computer se-  
2 curity necessary for responsible Internet use;  
3 and

4 (C) the availability of commercial off the  
5 shelf technology that allows consumers to meet  
6 such levels of computer security;

7 (2) a summary of the plans of the Secretary to  
8 enhance public awareness of common cyber security  
9 threats, including a description of the metrics used  
10 by the Department for evaluating the efficacy of  
11 public awareness campaigns; and

12 (3) recommendations for congressional actions  
13 to address these impediments to appropriate public  
14 awareness of common cyber security threats.

15 **SEC. 414. REPORT ON PROTECTING THE ELECTRICAL GRID**  
16 **OF THE UNITED STATES.**

17 Not later than 180 days after the date of enactment  
18 of this Act, the Secretary, in consultation with the Sec-  
19 retary of Defense and the Director of National Intel-  
20 ligence, shall submit to Congress a report on—

21 (1) the threat of a cyber attack disrupting the  
22 electrical grid of the United States;

23 (2) the implications for the national security of  
24 the United States if the electrical grid is disrupted;

1           (3) the options available to the United States  
2           and private sector entities to quickly reconstitute  
3           electrical service to provide for the national security  
4           of the United States, and, within a reasonable time  
5           frame, the reconstitution of all electrical service  
6           within the United States; and

7           (4) a plan to prevent disruption of the electric  
8           grid of the United States caused by a cyber attack.

9   **SEC. 415. MARKETPLACE INFORMATION.**

10          (a) SENSE OF CONGRESS.—It is the sense of Con-  
11          gress that—

12               (1) registrants that file reports with the Securi-  
13               ties and Exchange Commission have an obligation to  
14               disclose material risks to investors; and

15               (2) as with longstanding rules regarding other  
16               material risks, information security risks and related  
17               events that are material to investors should be dis-  
18               closed on a regular basis to provide quality informa-  
19               tion to the marketplace and enable informed investor  
20               decisions.

21          (b) DEFINITION OF INFORMATION SECURITY RISK.—

22          In this section, the term “information security risk and  
23          related events” means the risk to a registrant’s business  
24          operations, assets, financial condition, strategy, competi-  
25          tive positioning, and reputation, due to the potential for

1 unauthorized access, use, disclosure, disruption, modifica-  
2 tion, or destruction of registrant information, information  
3 of third parties collected by the registrant, or information  
4 systems of the registrant.

5 (c) GUIDANCE.—Not later than 1 year after the date  
6 of enactment of this Act, the Securities and Exchange  
7 Commission (referred to in this section as the “Commis-  
8 sion”) shall evaluate existing guidance to registrants re-  
9 lated to disclosures by registrants of information security  
10 risks and related events (including Securities and Ex-  
11 change Commission Division of Corporation Finance, CF  
12 Disclosure Guidance: Topic No. 2, Cybersecurity) to deter-  
13 mine whether such guidance, in light of the evaluation,  
14 should be—

15 (1) updated by the Division of Corporation Fi-  
16 nance; or

17 (2) issued as Commission interpretive guidance.

18 (d) ANNUAL REPORTS.—For 5 years following the  
19 evaluation under subsection (b), the Commission shall sub-  
20 mit to Congress, on an annual basis, a report that re-  
21 views—

22 (1) the types of information security risks and  
23 related events that registrants disclosed in the pre-  
24 vious year;

1           (2) whether the staff of the Commission has re-  
2           requested registrants to provide additional information  
3           on the disclosures under paragraph (1);

4           (3) any awareness or education activities for  
5           registrants or investors, on the subject of informa-  
6           tion security risks and related events disclosure re-  
7           quirements, sponsored by the Commission or at-  
8           tended by a Commissioner or staff of the Commis-  
9           sion; and

10          (4) any public actions commenced by the Com-  
11          mission relating to the enforcement of disclosure re-  
12          quirements pertaining to the information security  
13          risks and related events.

14   **TITLE    V—FEDERAL   ACQUI-**  
15   **TION    RISK   MANAGEMENT**  
16   **STRATEGY**

17   **SEC. 501. FEDERAL ACQUISITION RISK MANAGEMENT**  
18   **STRATEGY.**

19          (a) IN GENERAL.—The Secretary, in coordination  
20          with relevant private sector and academic experts and each  
21          Federal entity described in paragraphs (1) through (9) of  
22          subsection (b), shall develop and periodically update an ac-  
23          quisition risk management strategy designed to ensure,  
24          based on mission criticality and cost effectiveness, the se-  
25          curity of the Federal information infrastructure.

1 (b) COORDINATION.—In developing the acquisition  
2 risk management strategy required under subsection (a),  
3 the Secretary shall coordinate with—

4 (1) the Secretary of Defense;

5 (2) the Secretary of Commerce;

6 (3) the Secretary of State;

7 (4) the Director of National Intelligence;

8 (5) the Administrator of General Services;

9 (6) the Administrator for Federal Procurement  
10 Policy;

11 (7) the members of the Chief Information Offi-  
12 cers Council established under section 3603 of title  
13 44, United States Code;

14 (8) the Chief Acquisition Officers Council estab-  
15 lished under section 1311 of title 41, United States  
16 Code; and

17 (9) the Chief Financial Officers Council estab-  
18 lished under section 302 of the Chief Financial Offi-  
19 cers Act of 1990 (31 U.S.C. 901 note).

20 (c) ELEMENTS.—The risk management strategy de-  
21 veloped under subsection (a) shall—

22 (1) address risks in the acquisition of any part  
23 of the Federal information infrastructure; and

24 (2) include developing processes that—

1 (A) incorporate all-source intelligence anal-  
2 ysis into assessments of the integrity of the  
3 supply chain for the Federal information infra-  
4 structure;

5 (B) incorporate internationally recognized  
6 standards, guidelines, and best practices, in-  
7 cluding those developed by the private sector,  
8 for supply chain integrity;

9 (C) enhance capabilities to test and evalu-  
10 ate software and hardware within or for use in  
11 the Federal information infrastructure, and,  
12 where appropriate, make the capabilities avail-  
13 able for use by the private sector;

14 (D) protect the intellectual property and  
15 trade secrets of suppliers of information and  
16 communications technology products and serv-  
17 ices;

18 (E) share with the private sector, to the  
19 fullest extent possible, the risks identified in the  
20 supply chain and working with the private sec-  
21 tor to mitigate those threats as identified;

22 (F) identify specific acquisition practices of  
23 Federal agencies that increase risks to the sup-  
24 ply chain and develop a process to provide rec-

1           ommendations for revisions to those processes;  
2           and

3                   (G) to the maximum extent practicable,  
4           promote the ability of Federal agencies to pro-  
5           cure authentic commercial off-the-shelf informa-  
6           tion and communications technology products  
7           and services from a diverse pool of suppliers,  
8           consistent with the preferences for the acquisi-  
9           tion of commercial items under section 2377 of  
10          title 10, United States Code, and section 3307  
11          of title 41, United States Code.

12 **SEC. 502. AMENDMENTS TO CLINGER-COHEN PROVISIONS**  
13                   **TO ENHANCE AGENCY PLANNING FOR INFOR-**  
14                   **MATION SECURITY NEEDS.**

15          Chapter 113 of title 40, United States Code, is  
16          amended—

17               (1) in section 11302—

18                   (A) in subsection (f), by striking “tech-  
19           nology.” and inserting “technology, including  
20           information technology or network information  
21           security requirements.”;

22                   (B) in subsection (i)—

23                           (i) by inserting “, including informa-  
24           tion security requirements,” after “infor-  
25           mation resources management”; and

1                   (ii) by adding at the end the fol-  
2                   lowing: “The Administrator for Federal  
3                   Procurement Policy, in coordination with  
4                   the Chief Information Officers Council and  
5                   the Federal Acquisition Institute, shall en-  
6                   sure that contracting officers and the indi-  
7                   viduals preparing descriptions of the Gov-  
8                   ernment requirements and statements of  
9                   work have adequate training in informa-  
10                  tion security requirements, including in in-  
11                  formation technology security contracts.”;

12                (C) in subsection (j), by adding at the end  
13                the following: “The Director shall review and  
14                report on possible impediments in the acquisi-  
15                tion process or elsewhere that are acting to slow  
16                agency uptake of the newest, most secure tech-  
17                nologies.”; and

18                (D) by adding at the end the following:

19                “(l) MULTIPLE AWARD SCHEDULE FOR INFORMA-  
20                TION SECURITY.—The Administrator of General Services  
21                shall develop a special item number under Schedule 70  
22                for information security products and services and consoli-  
23                date those products and services under that special item  
24                number to promote acquisition.

1 “(m) REDUCING THE USE OF COUNTERFEIT PROD-  
2 UCTS.—Not later than 180 days after the date of enact-  
3 ment of the Cybersecurity Act of 2012, the Director shall  
4 issue guidance requiring, to the extent practicable, Federal  
5 agencies to purchase information technology products only  
6 through the authorized channels or distributors of a sup-  
7 plier.”; and

8 (2) in section 11312(b)(3), by inserting “, in-  
9 formation security improvement,” after “risk-ad-  
10 justed return on investment”.

## 11 **TITLE VI—INTERNATIONAL** 12 **COOPERATION**

### 13 **SEC. 601. DEFINITIONS.**

14 In this title:

15 (1) COMPUTER SYSTEM; COMPUTER DATA.—  
16 The terms “computer system” and “computer data”  
17 have the meanings given those terms in chapter I of  
18 the Convention on Cybercrime.

19 (2) CONVENTION ON CYBERCRIME.—The term  
20 “Convention on Cybercrime” means the Council of  
21 Europe’s Convention on Cybercrime, done at Buda-  
22 pest November 23, 2001 as ratified by the United  
23 States Senate on August 3, 2006 (Treaty 108–11)  
24 with any relevant reservations or declarations.

1           (3) CYBER ISSUES.—The term “cyber issues”  
2       means the full range of international policies de-  
3       signed to ensure an open, interoperable, secure, and  
4       reliable global information and communications in-  
5       frastructure.

6           (4) CYBERCRIME.—The term “cybercrime” re-  
7       fers to criminal offenses relating to computer sys-  
8       tems of computer data described in the Convention  
9       of Cybercrime.

10          (5) RELEVANT FEDERAL AGENCIES.—The term  
11       “relevant Federal agencies” means any Federal  
12       agency that has responsibility for combating  
13       cybercrime globally, including the Department of  
14       Commerce, the Department of Homeland Security,  
15       the Department of Justice, the Department of State,  
16       the Department of the Treasury, and the Office of  
17       the United States Trade Representative.

18   **SEC. 602. FINDINGS.**

19       Congress finds the following:

20          (1) On February 2, 2010, Admiral Dennis C.  
21       Blair, the Director of National Intelligence, testified  
22       before the Select Committee on Intelligence of the  
23       Senate regarding the Annual Threat Assessment of  
24       the U.S. Intelligence Community, stating “The na-  
25       tional security of the United States, our economic

1 prosperity, and the daily functioning of our govern-  
2 ment are dependent on a dynamic public and private  
3 information infrastructure, which includes tele-com-  
4 munications, computer networks and systems, and  
5 the information residing within. This critical infra-  
6 structure is severely threatened. . . . We cannot pro-  
7 tect cyberspace without a coordinated and collabo-  
8 rative effort that incorporates both the US private  
9 sector and our international partners.”

10 (2) In a January 2010 speech on Internet free-  
11 dom, Secretary of State Hillary Clinton stated:  
12 “Those who disrupt the free flow of information in  
13 our society, or any other, pose a threat to our econ-  
14 omy, our government, and our civil society. Coun-  
15 tries or individuals that engage in cyber attacks  
16 should face consequences and international con-  
17 demnation. In an Internet-connected world, an at-  
18 tack on one nation’s networks can be an attack on  
19 all. And by reinforcing that message, we can create  
20 norms of behavior among states and encourage re-  
21 spect for the global networked commons.”

22 (3) November 2011 marked the tenth anniver-  
23 sary of the Convention on Cybercrime, the only mul-  
24 tilateral agreement on cybercrime, to which the Sen-

1        ate provided advice and consent on August 3, 2006,  
2        and is currently ratified by over 30 countries.

3            (4) The May 2009 White House Cyberspace  
4        Policy Review asserts “[t]he Nation also needs a  
5        strategy for cybersecurity designed to shape the  
6        international environment and bring like-minded na-  
7        tions together on a host of issues, such as technical  
8        standards and acceptable legal norms regarding ter-  
9        ritorial jurisdiction, sovereign responsibility, and use  
10       of force. International norms are critical to estab-  
11       lishing a secure and thriving digital infrastructure.”

12   **SEC. 603. SENSE OF CONGRESS.**

13        It is the sense of Congress that—

14            (1) engagement with other countries to advance  
15        the cyberspace objectives of the United States should  
16        be an integral part of the conduct of United States  
17        foreign relations and diplomacy;

18            (2) the cyberspace objectives of the United  
19        States include the full range of cyber issues, includ-  
20        ing issues related to governance, standards, cyberse-  
21        curity, cybercrime, international security, human  
22        rights, and the free flow of information;

23            (3) it is in the interest of the United States to  
24        work with other countries to build consensus on  
25        principles and standards of conduct that protect

1 computer systems and users that rely on them, pre-  
2 vent and punish acts of cybercrime, and promote the  
3 free flow of information;

4 (4) a comprehensive national cyberspace strat-  
5 egy must include tools for addressing threats to  
6 computer systems and acts of cybercrime from  
7 sources and by persons outside the United States;

8 (5) developing effective solutions to inter-  
9 national cyberspace threats requires engagement  
10 with foreign countries on a bilateral basis and  
11 through relevant regional and multilateral fora;

12 (6) it is in the interest of the United States to  
13 encourage the development of effective frameworks  
14 for international cooperation to combat cyberthreats,  
15 and the development of foreign government capabili-  
16 ties to combat cyberthreats; and

17 (7) the Secretary of State, in consultation with  
18 other relevant Federal agencies, should develop and  
19 lead Federal Government efforts to engage with  
20 other countries to advance the cyberspace objectives  
21 of the United States, including efforts to bolster an  
22 international framework of cyber norms, governance  
23 and deterrence.

1 **SEC. 604. COORDINATION OF INTERNATIONAL CYBER**  
2 **ISSUES WITHIN THE UNITED STATES GOV-**  
3 **ERNMENT.**

4 The Secretary of State is authorized to designate a  
5 senior level official at the Department of State, to carry  
6 out the Secretary's responsibilities to—

7 (1) coordinate the United States global diplo-  
8 matic engagement on the full range of international  
9 cyber issues, including building multilateral coopera-  
10 tion and developing international norms, common  
11 policies, and responses to secure the integrity of  
12 cyberspace;

13 (2) provide strategic direction and coordination  
14 for United States Government policy and programs  
15 aimed at addressing and responding to cyber issues  
16 overseas, especially in relation to issues that affect  
17 United States foreign policy and related national se-  
18 curity concerns;

19 (3) coordinate with relevant Federal agencies,  
20 including the Department, the Department of De-  
21 fense, the Department of the Treasury, the Depart-  
22 ment of Justice, the Department of Commerce, and  
23 the intelligence community to develop interagency  
24 plans regarding international cyberspace, cybersecu-  
25 rity, and cybercrime issues; and

1           (4) ensure that cyber issues, including cyberse-  
2           curity and cybercrime, are included in the respon-  
3           sibilities of overseas Embassies and consulates of the  
4           United States, as appropriate.

5   **SEC. 605. CONSIDERATION OF CYBERCRIME IN FOREIGN**  
6                   **POLICY AND FOREIGN ASSISTANCE PRO-**  
7                   **GRAMS.**

8           (a) BRIEFING.—

9           (1) IN GENERAL.—Not later than 1 year after  
10          the date of enactment of this Act, the Secretary of  
11          State, after consultation with the heads of the rel-  
12          evant Federal agencies, shall provide a comprehen-  
13          sive briefing to relevant congressional committees—

14                (A) assessing global issues, trends, and ac-  
15                tors considered to be significant with respect to  
16                cybercrime;

17                (B) assessing, after consultation with pri-  
18                vate industry groups, civil society organizations,  
19                and other relevant domestic or multilateral or-  
20                ganizations, which shall be selected by the  
21                President based on an interest in combating  
22                cybercrime, means of enhancing multilateral or  
23                bilateral efforts in areas of significance—

24                       (i) to prevent and investigate  
25                       cybercrime;

1 (ii) to develop and share best prac-  
2 tices with respect to directly or indirectly  
3 combating cybercrime; and

4 (iii) to cooperate and take action with  
5 respect to the prevention, investigation,  
6 and prosecution of cybercrime; and

7 (C) describing the steps taken by the  
8 United States to promote the multilateral or bi-  
9 lateral efforts described in subparagraph (B).

10 (2) CONTRIBUTIONS FROM RELEVANT FEDERAL  
11 AGENCIES.—Not later than 30 days before the date  
12 on which the briefing is to be provided under para-  
13 graph (1), the head of each relevant Federal agency  
14 shall consult with and provide to the Secretary of  
15 State relevant information appropriate for the brief-  
16 ing.

17 (b) PERIODIC UPDATES.—The Secretary of State  
18 shall provide updated information highlighting significant  
19 developments relating to the issues described in subsection  
20 (a), through periodic briefings to Congress.

21 (c) USE OF FOREIGN ASSISTANCE PROGRAMS.—

22 (1) FOREIGN ASSISTANCE PROGRAMS TO COM-  
23 BAT CYBERCRIME.—The Secretary of State is au-  
24 thorized to accord priority in foreign assistance to  
25 programs designed to combat cybercrime in a region

1 or program of significance in order to better combat  
2 cybercrime by, among other things, improving the  
3 effectiveness and capacity of the legal and judicial  
4 systems and the capabilities of law enforcement  
5 agencies with respect to cybercrime.

6 (2) SENSE OF THE CONGRESS WITH RESPECT  
7 TO BILATERAL AND MULTILATERAL ASSISTANCE.—

8 It is the sense of Congress that the Secretary of  
9 State should include programs designed to combat  
10 cybercrime in relevant bilateral or multilateral as-  
11 sistance programs administered or supported by the  
12 United States Government.

13 **TITLE VII—INFORMATION**  
14 **SHARING**

15 **SEC. 701. AFFIRMATIVE AUTHORITY TO MONITOR AND DE-**  
16 **FEND AGAINST CYBERSECURITY THREATS.**

17 (a) IN GENERAL.—Notwithstanding chapter 119,  
18 121, or 206 of title 18, United States Code, the Foreign  
19 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et  
20 seq.), and sections 222 and 705 of the Communications  
21 Act of 1934 (47 U.S.C. 222 and 605), any private entity  
22 may—

23 (1) monitor its information systems and infor-  
24 mation that is stored on, processed by, or transiting  
25 such information systems for—

1 (A) malicious reconnaissance;

2 (B) efforts to defeat a technical control or  
3 an operational control;

4 (C) technical vulnerabilities;

5 (D) efforts to cause a user with legitimate  
6 access to an information system or information  
7 that is stored on, processed by, or transiting an  
8 information system to unwittingly enable the  
9 defeat of a technical control or an operational  
10 control;

11 (E) malicious cyber command and control;

12 (F) information exfiltrated as a result of  
13 defeating a technical control or an operational  
14 control;

15 (G) any other attribute of a cybersecurity  
16 threat, if monitoring for such attribute is not  
17 otherwise prohibited by law; or

18 (H) any combination of subparagraphs (A)  
19 through (G);

20 (2) operate countermeasures on its information  
21 systems to protect its rights or property from cyber-  
22 security threats;

23 (3) consent to another private entity monitoring  
24 or operating countermeasures on its information sys-  
25 tems and information that is stored on, processed

1 by, or transiting such information systems in accord-  
2 ance with this section;

3 (4) monitor a third party's information systems  
4 and information that is stored on, processed by, or  
5 transiting such information systems for the informa-  
6 tion listed in subparagraphs (A) through (H) of  
7 paragraph (1), if—

8 (A) the third party provides express prior  
9 consent to such monitoring; and

10 (B) such monitoring would be lawful under  
11 paragraph (1) or under any other provision of  
12 law if the third party were to perform such  
13 monitoring of its own networks; and

14 (5) operate countermeasures on a third party's  
15 information systems to protect the third party's  
16 rights or property from cybersecurity threats, if—

17 (A) the third party provides express prior  
18 consent to such countermeasures; and

19 (B) operating such countermeasures would  
20 be lawful under paragraph (2) or under any  
21 other provision of law if the third party were to  
22 operate such countermeasures on its own infor-  
23 mation systems to protect its own rights or  
24 property.

1 (b) USE AND PROTECTION OF INFORMATION.—A pri-  
2 vate entity performing monitoring or operating counter-  
3 measures under subsection (a)—

4 (1) may use cybersecurity threat indicators ac-  
5 quired under this title, provided such use is solely  
6 for the purpose of protecting an information system  
7 or information that is stored on, processed by, or  
8 transiting an information system from cybersecurity  
9 threats or mitigating such threats;

10 (2) shall make reasonable efforts to safeguard  
11 communications, records, system traffic, or other in-  
12 formation that may be used to identify specific per-  
13 sons acquired in the course of such monitoring from  
14 unauthorized access or acquisition;

15 (3) shall comply with any lawful restrictions  
16 placed on the use of cybersecurity threat indicators,  
17 including, if requested, the removal or destruction of  
18 information that can be used to identify specific per-  
19 sons from such indicators;

20 (4) may not use cybersecurity threat indicators  
21 to gain an unfair competitive advantage to the det-  
22 riment of the entity that authorized such monitoring  
23 or operation of countermeasures; and

24 (5) may use information obtained under any  
25 other provision of law.

1 **SEC. 702. VOLUNTARY DISCLOSURE OF CYBERSECURITY**  
2 **THREAT INDICATORS AMONG PRIVATE ENTI-**  
3 **TIES.**

4 (a) **AUTHORITY TO DISCLOSE.**—Notwithstanding any  
5 other provision of law, any private entity may disclose law-  
6 fully obtained cybersecurity threat indicators to any other  
7 private entity in accordance with this section.

8 (b) **USE AND PROTECTION OF INFORMATION.**—A pri-  
9 vate entity disclosing or receiving cybersecurity threat in-  
10 dicators pursuant to subsection (a)—

11 (1) may use, retain, or further disclose such cy-  
12 bersecurity threat indicators solely for the purpose  
13 of protecting an information system or information  
14 that is stored on, processed by, or transiting an in-  
15 formation system from cybersecurity threats or miti-  
16 gating such threats;

17 (2) shall make reasonable efforts to safeguard  
18 communications, records, system traffic, or other in-  
19 formation that can be used to identify specific per-  
20 sons from unauthorized access or acquisition;

21 (3) shall comply with any lawful restrictions  
22 placed on the disclosure or use of cybersecurity  
23 threat indicators, including, if requested, the re-  
24 moval of information that may be used to identify  
25 specific persons from such indicators; and

1           (4) may not use the cybersecurity threat indica-  
2           tors to gain an unfair competitive advantage to the  
3           detriment of the entity that authorized such sharing.

4           (c) TRANSFERS TO UNRELIABLE PRIVATE ENTITIES  
5   PROHIBITED.—A private entity may not disclose cyberse-  
6   curity threat indicators to another private entity that the  
7   disclosing entity knows—

8           (1) has intentionally or willfully violated the re-  
9           quirements of subsection (b); and

10          (2) is reasonably likely to violate such require-  
11          ments.

12   **SEC. 703. CYBERSECURITY EXCHANGES.**

13          (a) DESIGNATION OF CYBERSECURITY EX-  
14   CHANGES.—The Secretary of Homeland Security, in con-  
15   sultation with the Director of National Intelligence, the  
16   Attorney General, and the Secretary of Defense, shall es-  
17   tablish—

18          (1) a process for designating one or more ap-  
19          propriate civilian Federal entities or non-Federal en-  
20          tities to serve as cybersecurity exchanges to receive  
21          and distribute cybersecurity threat indicators;

22          (2) procedures to facilitate and ensure the shar-  
23          ing of classified and unclassified cybersecurity threat  
24          indicators in as close to real time as possible with

1 appropriate Federal entities and non-Federal entities  
2 in accordance with this title; and

3 (3) a process for identifying certified entities to  
4 receive classified cybersecurity threat indicators in  
5 accordance with paragraph (2).

6 (b) PURPOSE.—The purpose of a cybersecurity ex-  
7 change is to receive and distribute, in as close to real time  
8 as possible, cybersecurity threat indicators, and to thereby  
9 avoid unnecessary and duplicative Federal bureaucracy for  
10 information sharing as provided in this title.

11 (c) REQUIREMENT FOR A LEAD FEDERAL CIVILIAN  
12 CYBERSECURITY EXCHANGE.—

13 (1) IN GENERAL.—The Secretary, in consulta-  
14 tion with the Director of National Intelligence, the  
15 Attorney General, and the Secretary of Defense,  
16 shall designate a civilian Federal entity as the lead  
17 cybersecurity exchange to serve as a focal point  
18 within the Federal Government for cybersecurity in-  
19 formation sharing among Federal entities and with  
20 non-Federal entities.

21 (2) RESPONSIBILITIES.—The lead Federal civil-  
22 ian cybersecurity exchange designated under para-  
23 graph (1) shall—

1 (A) receive and distribute, in as close to  
2 real time as possible, cybersecurity threat indi-  
3 cators in accordance with this title;

4 (B) facilitate information sharing, inter-  
5 action, and collaboration among and between—

6 (i) Federal entities;

7 (ii) State, local, tribal, and territorial  
8 governments;

9 (iii) private entities;

10 (iv) academia;

11 (v) international partners, in consulta-  
12 tion with the Secretary of State; and

13 (vi) other cybersecurity exchanges;

14 (C) disseminate timely and actionable cy-  
15 bersecurity threat, vulnerability, mitigation, and  
16 warning information lawfully obtained from any  
17 source, including alerts, advisories, indicators,  
18 signatures, and mitigation and response meas-  
19 ures, to appropriate Federal and non-Federal  
20 entities in as close to real time as possible, to  
21 improve the security and protection of informa-  
22 tion systems;

23 (D) coordinate with other Federal and  
24 non-Federal entities, as appropriate, to inte-  
25 grate information from Federal and non-Fed-

1           eral entities, including Federal cybersecurity  
2           centers, non-Federal network or security oper-  
3           ation centers, other cybersecurity exchanges,  
4           and non-Federal entities that disclose cyberse-  
5           curity threat indicators under section 704(a), in  
6           as close to real time as possible, to provide situ-  
7           ational awareness of the United States informa-  
8           tion security posture and foster information se-  
9           curity collaboration among information system  
10          owners and operators;

11                 (E) conduct, in consultation with private  
12           entities and relevant Federal and other govern-  
13           mental entities, regular assessments of existing  
14           and proposed information sharing models to  
15           eliminate bureaucratic obstacles to information  
16           sharing and identify best practices for such  
17           sharing; and

18                 (F) coordinate with other Federal entities,  
19           as appropriate, to compile and analyze informa-  
20           tion about risks and incidents that threaten in-  
21           formation systems, including information volun-  
22           tarily submitted in accordance with section  
23           704(a) or otherwise in accordance with applica-  
24           ble laws.

1           (3) SCHEDULE FOR DESIGNATION.—The des-  
2           ignation of a lead Federal civilian cybersecurity ex-  
3           change under paragraph (1) shall be made concur-  
4           rently with the issuance of the interim policies and  
5           procedures under section 704(g)(3)(D).

6           (d) ADDITIONAL CIVILIAN FEDERAL CYBERSECU-  
7           RITY EXCHANGES.—In accordance with the process and  
8           procedures established in subsection (a), the Secretary, in  
9           consultation with the Director of National Intelligence, the  
10          Attorney General, and the Secretary of Defense, may des-  
11          ignate additional civilian Federal entities to receive and  
12          distribute cybersecurity threat indicators, if such entities  
13          are subject to the requirements for use, retention, and dis-  
14          closure of information by a cybersecurity exchange under  
15          section 704(b) and the special requirements for Federal  
16          entities under section 704(g).

17          (e) REQUIREMENTS FOR NON-FEDERAL CYBERSECU-  
18          RITY EXCHANGES.—

19               (1) IN GENERAL.—In considering whether to  
20               designate a private entity or any other non-Federal  
21               entity as a cybersecurity exchange to receive and dis-  
22               tribute cybersecurity threat indicators under section  
23               704, and what entity to designate, the Secretary  
24               shall consider the following factors:

1 (A) The net effect that such designation  
2 would have on the overall cybersecurity of the  
3 United States.

4 (B) Whether such designation could sub-  
5 stantially improve such overall cybersecurity by  
6 serving as a hub for receiving and sharing cy-  
7 bersecurity threat indicators in as close to real  
8 time as possible, including the capacity of the  
9 non-Federal entity for performing those func-  
10 tions.

11 (C) The capacity of such non-Federal enti-  
12 ty to safeguard cybersecurity threat indicators  
13 from unauthorized disclosure and use.

14 (D) The adequacy of the policies and pro-  
15 cedures of such non-Federal entity to protect  
16 personally identifiable information from unau-  
17 thorized disclosure and use.

18 (E) The ability of the non-Federal entity  
19 to sustain operations using entirely non-Federal  
20 sources of funding.

21 (2) REGULATIONS.—The Secretary may pro-  
22 mulgate regulations as may be necessary to carry  
23 out this subsection.

24 (f) CONSTRUCTION WITH OTHER AUTHORITIES.—  
25 Nothing in this section may be construed to alter the au-

1   thorities of a Federal cybersecurity center, unless such cy-  
2   bersecurity center is acting in its capacity as a designated  
3   cybersecurity exchange.

4       (g) CONGRESSIONAL NOTIFICATION OF DESIGNA-  
5   TION OF CYBERSECURITY EXCHANGES.—

6           (1) IN GENERAL.—The Secretary, in coordina-  
7       tion with the Director of National Intelligence, the  
8       Attorney General, and the Secretary of Defense,  
9       shall promptly notify Congress, in writing, of any  
10      designation of a cybersecurity exchange under this  
11      title.

12          (2) REQUIREMENT.—Written notification under  
13      paragraph (1) shall include a description of the cri-  
14      teria and processes used to make the designation.

15   **SEC. 704. VOLUNTARY DISCLOSURE OF CYBERSECURITY**  
16                   **THREAT INDICATORS TO A CYBERSECURITY**  
17                   **EXCHANGE.**

18      (a) AUTHORITY TO DISCLOSE.—Notwithstanding any  
19   other provision of law, a non-Federal entity may disclose  
20   lawfully obtained cybersecurity threat indicators to a cy-  
21   bersecurity exchange in accordance with this section.

22      (b) USE, RETENTION, AND DISCLOSURE OF INFOR-  
23   MATION BY A CYBERSECURITY EXCHANGE.—A cybersecu-  
24   rity exchange may only use, retain, or further disclose in-  
25   formation provided pursuant to subsection (a)—

1           (1) in order to protect information systems  
2           from cybersecurity threats and to mitigate cyberse-  
3           curity threats; or

4           (2) to law enforcement pursuant to subsection  
5           (g)(2).

6           (c) USE AND PROTECTION OF INFORMATION RE-  
7           CEIVED FROM A CYBERSECURITY EXCHANGE.—A non-  
8           Federal entity receiving cybersecurity threat indicators  
9           from a cybersecurity exchange—

10           (1) may use, retain, or further disclose such cy-  
11           bersecurity threat indicators solely for the purpose  
12           of protecting an information system or information  
13           that is stored on, processed by, or transiting an in-  
14           formation system from cybersecurity threats or miti-  
15           gating such threats;

16           (2) shall make reasonable efforts to safeguard  
17           communications, records, system traffic, or other in-  
18           formation that can be used to identify specific per-  
19           sons from unauthorized access or acquisition;

20           (3) shall comply with any lawful restrictions  
21           placed on the disclosure or use of cybersecurity  
22           threat indicators by the cybersecurity exchange or a  
23           third party, if the cybersecurity exchange received  
24           such information from the third party, including, if  
25           requested, the removal of information that can be

1       used to identify specific persons from such indica-  
2       tors; and

3           (4) may not use the cybersecurity threat indica-  
4       tors to gain an unfair competitive advantage to the  
5       detriment of the third party that authorized such  
6       sharing.

7       (d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any  
8       cybersecurity threat indicator disclosed by a non-Federal  
9       entity to a cybersecurity exchange pursuant to subsection  
10      (a) shall be—

11           (1) exempt from disclosure under section  
12       552(b)(3) of title 5, United States Code, or any  
13       comparable State law; and

14           (2) treated as voluntarily shared information  
15       under section 552 of title 5, United States Code, or  
16       any comparable State law.

17       (e) EXEMPTION FROM EX PARTE LIMITATIONS.—  
18       Any cybersecurity threat indicator disclosed by a non-Fed-  
19       eral entity to a cybersecurity exchange pursuant to sub-  
20       section (a) shall not be subject to the rules of any govern-  
21       mental entity or judicial doctrine regarding ex parte com-  
22       munications with a decision making official.

23       (f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any  
24       cybersecurity threat indicator disclosed by a non-Federal  
25       entity to a cybersecurity exchange pursuant to subsection

1 (a) may not be construed to be a waiver of any applicable  
2 privilege or protection provided under Federal, State, trib-  
3 al, or territorial law, including any trade secret protection.

4 (g) SPECIAL REQUIREMENTS FOR FEDERAL AND  
5 LAW ENFORCEMENT ENTITIES.—

6 (1) RECEIPT, DISCLOSURE AND USE OF CYBER-  
7 SECURITY THREAT INDICATORS BY A FEDERAL EN-  
8 TITY.—

9 (A) AUTHORITY TO RECEIVE AND USE CY-  
10 BERSECURITY THREAT INDICATORS.—A Fed-  
11 eral entity that is not a cybersecurity exchange  
12 may receive, retain, and use cybersecurity  
13 threat indicators from a cybersecurity exchange  
14 in order—

15 (i) to protect information systems  
16 from cybersecurity threats and to mitigate  
17 cybersecurity threats; and

18 (ii) to disclose such cybersecurity  
19 threat indicators to law enforcement in ac-  
20 cordance with paragraph (2).

21 (B) AUTHORITY TO DISCLOSE CYBERSECU-  
22 RITY THREAT INDICATORS.—A Federal entity  
23 that is not a cybersecurity exchange shall en-  
24 sure that if disclosing cybersecurity threat indi-  
25 cators to a non-Federal entity under this sec-

tion, such non-Federal entity shall use or retain such cybersecurity threat indicators in a manner that is consistent with the requirements in—

(i) subsection (b) on the use and protection of information; and

(ii) paragraph (2).

(2) LAW ENFORCEMENT ACCESS AND USE OF CYBERSECURITY THREAT INDICATORS.—

(A) DISCLOSURE TO LAW ENFORCEMENT.—A Federal entity may disclose cybersecurity threat indicators received under this title to a law enforcement entity if—

(i) the disclosure is permitted under the procedures developed by the Secretary and approved by the Attorney General under paragraph (3); and

(ii) the information appears to pertain—

(I) to a cybersecurity crime which has been, is being, or is about to be committed;

(II) to an imminent threat of death or serious bodily harm; or

1 (III) to a serious threat to mi-  
2 nors, including sexual exploitation and  
3 threats to physical safety.

4 (B) USE BY LAW ENFORCEMENT.—A law  
5 enforcement entity may only use cybersecurity  
6 threat indicators received by a Federal entity  
7 under paragraph (A) in order—

8 (i) to protect information systems  
9 from a cybersecurity threat or investigate,  
10 prosecute, or disrupt a cybersecurity crime;

11 (ii) to protect individuals from an im-  
12 minent threat of death or serious bodily  
13 harm; or

14 (iii) to protect minors from any seri-  
15 ous threat, including sexual exploitation  
16 and threats to physical safety.

17 (3) PRIVACY AND CIVIL LIBERTIES.—

18 (A) REQUIREMENT FOR POLICIES AND  
19 PROCEDURES.—The Secretary, in consultation  
20 with privacy and civil liberties experts, the Di-  
21 rector of National Intelligence, and the Sec-  
22 retary of Defense, shall develop and periodically  
23 review policies and procedures governing the re-  
24 ceipt, retention, use, and disclosure of cyberse-  
25 curity threat indicators by a Federal entity ob-

1           tained in connection with activities authorized  
2           in this title. Such policies and procedures  
3           shall—

4                   (i) minimize the impact on privacy  
5                   and civil liberties, consistent with the need  
6                   to protect information systems from cyber-  
7                   security threats and mitigate cybersecurity  
8                   threats;

9                   (ii) reasonably limit the receipt, reten-  
10                  tion, use and disclosure of cybersecurity  
11                  threat indicators associated with specific  
12                  persons consistent with the need to carry  
13                  out the responsibilities of this title, includ-  
14                  ing establishing a process for the timely  
15                  destruction of cybersecurity threat indica-  
16                  tors that are received pursuant to this sec-  
17                  tion that do not reasonably appear to be  
18                  related to the purposes identified in para-  
19                  graph (1)(A);

20                  (iii) include requirements to safeguard  
21                  cybersecurity threat indicators that may be  
22                  used to identify specific persons from un-  
23                  authorized access or acquisition;

24                  (iv) include procedures for notifying  
25                  entities, as appropriate, if information re-

ceived pursuant to this section is not a cybersecurity threat indicator; and

(v) protect the confidentiality of cybersecurity threat indicators associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for the purposes identified in paragraph (1)(A).

(B) ADOPTION OF POLICIES AND PROCEDURES.—The head of an agency responsible for a Federal entity designated as a cybersecurity exchange under section 703 shall adopt and comply with the policies and procedures developed under this paragraph.

(C) REVIEW BY THE ATTORNEY GENERAL.—The policies and procedures developed under this subsection shall be provided to the Attorney General for review not later than 1 year after the date of the enactment of this title, and shall not be issued without the Attorney General's approval.

(D) REQUIREMENT FOR INTERIM POLICIES AND PROCEDURES.—The Secretary shall issue interim policies and procedures not later than

1           60 days after the date of the enactment of this  
2           title.

3           (E) PROVISION TO CONGRESS.—The poli-  
4           cies and procedures issued under this title and  
5           any amendments to such policies and proce-  
6           dures shall be provided to Congress in an un-  
7           classified form and be made public, but may in-  
8           clude a classified annex.

9           (4) OVERSIGHT.—

10          (A) REQUIREMENT FOR OVERSIGHT.—The  
11          Secretary and the Attorney General shall estab-  
12          lish a mandatory program to monitor and over-  
13          see compliance with the policies and procedures  
14          issued under this subsection.

15          (B) NOTIFICATION OF THE ATTORNEY  
16          GENERAL.—The head of each Federal entity  
17          that receives information under this title  
18          shall—

19               (i) comply with the policies and proce-  
20               dures developed by the Secretary and ap-  
21               proved by the Attorney General under  
22               paragraph (3);

23               (ii) promptly notify the Attorney Gen-  
24               eral of significant violations of such poli-  
25               cies and procedures; and

1 (iii) provide to the Attorney General  
2 any information relevant to the violation  
3 that the Attorney General requires.

4 (C) ANNUAL REPORT.—On an annual  
5 basis, the Chief Privacy and Civil Liberties Of-  
6 ficer of the Department of Justice and the  
7 Chief Privacy Officer of the Department, in  
8 consultation with the most senior privacy and  
9 civil liberties officer or officers of any appro-  
10 priate agencies, shall jointly submit to Congress  
11 a report assessing the privacy and civil liberties  
12 impact of the governmental activities conducted  
13 pursuant to this title.

14 (5) REPORTS ON INFORMATION SHARING.—

15 (A) PRIVACY AND CIVIL LIBERTIES OVER-  
16 SIGHT BOARD REPORT.—Not later than 2 years  
17 after the date of the enactment of this title, and  
18 every 2 years thereafter, the Privacy and Civil  
19 Liberties Oversight Board shall submit to Con-  
20 gress and the President a report providing—

21 (i) an analysis of the practices of pri-  
22 vate entities that are performing, moni-  
23 toring, operating countermeasures, or dis-  
24 closing cybersecurity threat indicators pur-  
25 suant to this title;

1 (ii) an assessment of the privacy and  
2 civil liberties impact of the activities car-  
3 ried out by the Federal entities under this  
4 title; and

5 (iii) recommendations for improve-  
6 ments to or modifications of the law and  
7 the policies and procedures established  
8 pursuant to paragraph (3) in order to ad-  
9 dress privacy and civil liberties concerns.

10 (B) INSPECTORS GENERAL ANNUAL RE-  
11 PORT.—The Inspector General of the Depart-  
12 ment, the Inspector General of the Intelligence  
13 Community, the Inspector General of the De-  
14 partment of Justice, and the Inspector General  
15 of the Department of Defense shall, on an an-  
16 nual basis, jointly submit to Congress a report  
17 on the receipt, use and disclosure of informa-  
18 tion shared with a Federal cybersecurity ex-  
19 change under this title, including—

20 (i) a review of the use by Federal en-  
21 tities of such information for a purpose  
22 other than to protect information systems  
23 from cybersecurity threats and to mitigate  
24 cybersecurity threats, including law en-

1           enforcement access and use pursuant to  
2           paragraph (2);

3                 (ii) a review of the type of information  
4           shared with a Federal cybersecurity ex-  
5           change;

6                 (iii) a review of the actions taken by  
7           Federal entities based on such information;

8                 (iv) appropriate metrics to determine  
9           the impact of the sharing of such informa-  
10          tion with a Federal cybersecurity exchange  
11          on privacy and civil liberties;

12                (v) a list of Federal entities receiving  
13          such information;

14                (vi) a review of the sharing of such in-  
15          formation among Federal entities to iden-  
16          tify inappropriate stovepiping of shared in-  
17          formation; and

18                (vii) any recommendations of the in-  
19          spectors general for improvements or modi-  
20          fications to the authorities under this title.

21                (C) FORM.—Each report required under  
22          this paragraph shall be submitted in unclassi-  
23          fied form, but may include a classified annex.

24                (6) SANCTIONS.—The head of each Federal en-  
25          tity that conducts activities under this title shall de-

1       velop and enforce appropriate sanctions for officers,  
2       employees, or agents of such entities who conducts  
3       such activities—

4               (A) outside the normal course of their  
5       specified duties;

6               (B) in a manner inconsistent with the dis-  
7       charge of the responsibilities of such entity; or

8               (C) in contravention of the requirements,  
9       policies, and procedures required by this sub-  
10      section.

11       (7) FEDERAL GOVERNMENT LIABILITY FOR  
12      VIOLATIONS OF THIS TITLE.—

13               (A) IN GENERAL.—If a Federal entity in-  
14      tentionally or willfully violates a provision of  
15      this title or a regulation promulgated under this  
16      title, the United States shall be liable to a per-  
17      son adversely affected by such violation in an  
18      amount equal to the sum of—

19                   (i) the actual damages sustained by  
20      the person as a result of the violation or  
21      \$1,000, whichever is greater; and

22                   (ii) the costs of the action together  
23      with reasonable attorney fees as deter-  
24      mined by the court.

1 (B) VENUE.—An action to enforce liability  
2 created under this subsection may be brought  
3 in the district court of the United States in—

4 (i) the district in which the complain-  
5 ant resides;

6 (ii) the district in which the principal  
7 place of business of the complainant is lo-  
8 cated;

9 (iii) the district in which the Federal  
10 entity that disclosed the information is lo-  
11 cated; or

12 (iv) the District of Columbia.

13 (C) STATUTE OF LIMITATIONS.—No action  
14 shall lie under this subsection unless such ac-  
15 tion is commenced not later than 2 years after  
16 the date of the violation that is the basis for the  
17 action.

18 (D) EXCLUSIVE CAUSE OF ACTION.—A  
19 cause of action under this subsection shall be  
20 the exclusive means available to a complainant  
21 seeking a remedy for a disclosure of informa-  
22 tion in violation of this title by a Federal entity.

1 **SEC. 705. SHARING OF CLASSIFIED CYBERSECURITY**  
2 **THREAT INDICATORS.**

3 (a) SHARING OF CLASSIFIED CYBERSECURITY  
4 THREAT INDICATORS.—The procedures established under  
5 section 703(a)(2) shall provide that classified cybersecu-  
6 rity threat indicators may only be—

7 (1) shared with certified entities;

8 (2) shared in a manner that is consistent with  
9 the need to protect the national security of the  
10 United States;

11 (3) shared with a person with an appropriate  
12 security clearance to receive such cybersecurity  
13 threat indicators; and

14 (4) used by a certified entity in a manner that  
15 protects such cybersecurity threat indicators from  
16 unauthorized disclosure.

17 (b) REQUIREMENT FOR GUIDELINES.—Not later  
18 than 60 days after the date of the enactment of this title,  
19 the Director of National Intelligence shall issue guidelines  
20 providing that appropriate Federal officials may, as the  
21 Director considers necessary to carry out this title—

22 (1) grant a security clearance on a temporary  
23 or permanent basis to an employee of a certified en-  
24 tity;

1           (2) grant a security clearance on a temporary  
2           or permanent basis to a certified entity and approval  
3           to use appropriate facilities; or

4           (3) expedite the security clearance process for  
5           such an employee or entity, if appropriate, in a man-  
6           ner consistent with the need to protect the national  
7           security of the United States.

8           (c) DISTRIBUTION OF PROCEDURES AND GUIDE-  
9           LINES.—Following the establishment of the procedures  
10          under section 703(a)(2) and the issuance of the guidelines  
11          under subsection (b), the Secretary and the Director of  
12          National Intelligence shall expeditiously distribute such  
13          procedures and guidelines to—

14               (1) appropriate governmental entities and pri-  
15               vate entities;

16               (2) the Committee on Armed Services, the  
17               Committee on Commerce, Science, and Transpor-  
18               tation, the Committee on Homeland Security and  
19               Governmental Affairs, the Committee on the Judici-  
20               ary, and the Select Committee on Intelligence of the  
21               Senate; and

22               (3) the Committee on Armed Services, the  
23               Committee on Energy and Commerce, the Com-  
24               mittee on Homeland Security, the Committee on the

1       Judiciary, and the Permanent Select Committee on  
2       Intelligence of the House of Representatives.

3       **SEC. 706. LIMITATION ON LIABILITY AND GOOD FAITH DE-**  
4       **FENSE FOR CYBERSECURITY ACTIVITIES.**

5       (a) IN GENERAL.—No civil or criminal cause of ac-  
6       tion shall lie or be maintained in any Federal or State  
7       court against any entity acting as authorized by this title,  
8       and any such action shall be dismissed promptly for activi-  
9       ties authorized by this title consisting of—

10           (1) the cybersecurity monitoring activities au-  
11           thorized by paragraph (1), (3) or (4) of section  
12           701(a); or

13           (2) the voluntary disclosure of a lawfully ob-  
14           tained cybersecurity threat indicator—

15                   (A) to a cybersecurity exchange pursuant  
16                   to section 704(a);

17                   (B) by a provider of cybersecurity services  
18                   to a customer of that provider;

19                   (C) to a private entity or governmental en-  
20                   tity that provides or manages critical infra-  
21                   structure (as that term is used in section 1016  
22                   of the Critical Infrastructures Protection Act of  
23                   2001 (42 U.S.C. 5195c)); or

24                   (D) to any other private entity under sec-  
25                   tion 702(a), if the cybersecurity threat indicator

1 is also disclosed within a reasonable time to a  
2 cybersecurity exchange.

3 (b) GOOD FAITH DEFENSE.—If a civil or criminal  
4 cause of action is not barred under subsection (a), a rea-  
5 sonable good faith reliance that this title permitted the  
6 conduct complained of is a complete defense against any  
7 civil or criminal action brought under this title or any  
8 other law.

9 (c) LIMITATION ON USE OF CYBERSECURITY  
10 THREAT INDICATORS FOR REGULATORY ENFORCEMENT  
11 ACTIONS.—No Federal entity may use a cybersecurity  
12 threat indicator received pursuant to this title as evidence  
13 in a regulatory enforcement action against the entity that  
14 lawfully shared the cybersecurity threat indicator with a  
15 cybersecurity exchange that is a Federal entity.

16 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW  
17 ENFORCEMENT, NATIONAL SECURITY, OR HOMELAND  
18 SECURITY PURPOSES.—No civil or criminal cause of ac-  
19 tion shall lie or be maintained in any Federal or State  
20 court against any entity, and any such action shall be dis-  
21 missed promptly, for a failure to disclose a cybersecurity  
22 threat indicator if—

23 (1) the Attorney General or the Secretary de-  
24 termines that disclosure of a cybersecurity threat in-  
25 dicator would impede a civil or criminal investigation

1       and submits a written request to delay notification  
2       for up to 30 days, except that the Attorney General  
3       or the Secretary may, by a subsequent written re-  
4       quest, revoke such delay or extend the period of time  
5       set forth in the original request made under this  
6       paragraph if further delay is necessary; or

7               (2) the Secretary, the Attorney General, or the  
8       Director of National Intelligence determines that  
9       disclosure of a cybersecurity threat indicator would  
10      threaten national or homeland security and submits  
11      a written request to delay notification, except that  
12      the Secretary, the Attorney General, or the Director,  
13      may, by a subsequent written request, revoke such  
14      delay or extend the period of time set forth in the  
15      original request made under this paragraph if fur-  
16      ther delay is necessary.

17      (e) LIMITATION ON LIABILITY FOR FAILURE TO  
18      ACT.—No civil or criminal cause of action shall lie or be  
19      maintained in any Federal or State court against any pri-  
20      vate entity, or any officer, employee, or agent of such an  
21      entity, and any such action shall be dismissed promptly,  
22      for the reasonable failure to act on information received  
23      under this title.

24      (f) DEFENSE FOR BREACH OF CONTRACT.—Compli-  
25      ance with lawful restrictions placed on the disclosure or

1 use of cybersecurity threat indicators is a complete defense  
2 to any tort or breach of contract claim originating in a  
3 failure to disclose cybersecurity threat indicators to a third  
4 party.

5 (g) LIMITATION ON LIABILITY PROTECTIONS.—Any  
6 person who, knowingly or acting in gross negligence, vio-  
7 lates a provision of this title or a regulation promulgated  
8 under this title shall—

9 (1) not receive the protections of this title; and

10 (2) be subject to any criminal or civil cause of  
11 action that may arise under any other State or Fed-  
12 eral law prohibiting the conduct in question.

13 **SEC. 707. CONSTRUCTION AND FEDERAL PREEMPTION.**

14 (a) CONSTRUCTION.—Nothing in this title may be  
15 construed—

16 (1) to limit any other existing authority or law-  
17 ful requirement to monitor information systems and  
18 information that is stored on, processed by, or  
19 transiting such information systems, operate coun-  
20 termeasures, and retain, use or disclose lawfully ob-  
21 tained information;

22 (2) to permit the unauthorized disclosure of—

23 (A) information that has been determined  
24 by the Federal Government pursuant to an Ex-  
25 ecutive order or statute to require protection

1           against unauthorized disclosure for reasons of  
2           national defense or foreign relations;

3                 (B) any restricted data (as that term is de-  
4           fined in paragraph (y) of section 11 of the  
5           Atomic Energy Act of 1954 (42 U.S.C. 2014));

6                 (C) information related to intelligence  
7           sources and methods; or

8                 (D) information that is specifically subject  
9           to a court order or a certification, directive, or  
10          other authorization by the Attorney General  
11          precluding such disclosure;

12                (3) to provide additional authority to, or modify  
13          an existing authority of, the Department of Defense  
14          or the National Security Agency or any other ele-  
15          ment of the intelligence community to control, mod-  
16          ify, require, or otherwise direct the cybersecurity ef-  
17          forts of a non-Federal entity or a Federal entity;

18                (4) to limit or modify an existing information  
19          sharing relationship;

20                (5) to prohibit a new information sharing rela-  
21          tionship;

22                (6) to require a new information sharing rela-  
23          tionship between a Federal entity and a private enti-  
24          ty;

1           (7) to limit the ability of a non-Federal entity  
2           or a Federal entity to receive data about its informa-  
3           tion systems, including lawfully obtained cybersecu-  
4           rity threat indicators;

5           (8) to authorize or prohibit any law enforce-  
6           ment, homeland security, or intelligence activities  
7           not otherwise authorized or prohibited under another  
8           provision of law;

9           (9) to permit price-fixing, allocating a market  
10          between competitors, monopolizing or attempting to  
11          monopolize a market, boycotting, or exchanges of  
12          price or cost information, customer lists, or informa-  
13          tion regarding future competitive planning;

14          (10) to authorize or limit liability for actions  
15          that would violate the regulations adopted by the  
16          Federal Communications Commission on preserving  
17          the open Internet, or any successor regulations  
18          thereto, nor to modify or alter the obligations of pri-  
19          vate entities under such regulations; or

20          (11) to prevent a governmental entity from  
21          using information not acquired through a cybersecu-  
22          rity exchange for regulatory purposes.

23          (b) FEDERAL PREEMPTION.—This title supersedes  
24          any law or requirement of a State or political subdivision  
25          of a State that restricts or otherwise expressly regulates

1 the provision of cybersecurity services or the acquisition,  
2 interception, retention, use or disclosure of communica-  
3 tions, records, or other information by private entities to  
4 the extent such law contains requirements inconsistent  
5 with this title.

6 (c) PRESERVATION OF OTHER STATE LAW.—Except  
7 as expressly provided, nothing in this title shall be con-  
8 strued to preempt the applicability of any other State law  
9 or requirement.

10 (d) NO CREATION OF A RIGHT TO INFORMATION.—  
11 The provision of information to a non-Federal entity  
12 under this title does not create a right or benefit to similar  
13 information by any other non-Federal entity.

14 (e) PROHIBITION ON REQUIREMENT TO PROVIDE IN-  
15 FORMATION TO THE FEDERAL GOVERNMENT.—Nothing  
16 in this title may be construed to permit a Federal entity—

17 (1) to require a non-Federal entity to share in-  
18 formation with the Federal Government;

19 (2) to condition the disclosure of unclassified or  
20 classified cybersecurity threat indicators pursuant to  
21 this title with a non-Federal entity on the provision  
22 of cybersecurity threat information to the Federal  
23 Government; or

24 (3) to condition the award of any Federal  
25 grant, contract or purchase on the provision of cy-

1       bersecurity threat indicators to a Federal entity, if  
2       the provision of such indicators does not reasonably  
3       relate to the nature of activities, goods, or services  
4       covered by the award.

5       (f) LIMITATION ON USE OF INFORMATION.—No cy-  
6       bersecurity threat indicators obtained pursuant to this  
7       title may be used, retained, or disclosed by a Federal enti-  
8       ty or non-Federal entity, except as authorized under this  
9       title.

10       (g) DECLASSIFICATION AND SHARING OF INFORMA-  
11       TION.—Consistent with the exemptions from public disclo-  
12       sure of section 704(d), the Director of National Intel-  
13       ligence, in consultation with the Secretary and the head  
14       of the Federal entity in possession of the information,  
15       shall facilitate the declassification and sharing of informa-  
16       tion in the possession of a Federal entity that is related  
17       to cybersecurity threats, as the Director deems appro-  
18       priate.

19       (h) REPORT ON IMPLEMENTATION.—Not later than  
20       2 years after the date of the enactment of this title, the  
21       Secretary, the Director of National Intelligence, the Attor-  
22       ney General, and the Secretary of Defense shall jointly  
23       submit to Congress a report that—

24               (1) describes the extent to which the authorities  
25       conferred by this title have enabled the Federal Gov-

1       ernment and the private sector to mitigate cyberse-  
2       curity threats;

3           (2) discloses any significant acts of noncompli-  
4       ance by a non-Federal entity with this title, with  
5       special emphasis on privacy and civil liberties, and  
6       any measures taken by the Federal Government to  
7       uncover such noncompliance;

8           (3) describes in general terms the nature and  
9       quantity of information disclosed and received by  
10      governmental entities and private entities under this  
11      title; and

12          (4) identifies the emergence of new threats or  
13      technologies that challenge the adequacy of the law,  
14      including the definitions, authorities and require-  
15      ments of this title, for keeping pace with the threat.

16      (i) REQUIREMENT FOR ANNUAL REPORT.—On an  
17      annual basis, the Director of National Intelligence shall  
18      provide a report to the Select Committee on Intelligence  
19      of the Senate and the Permanent Select Committee on In-  
20      telligence of the House of Representatives on the imple-  
21      mentation of section 705. Such report, which shall be sub-  
22      mitted in a classified and in an unclassified form, shall  
23      include a list of private entities that receive classified cy-  
24      bersecurity threat indicators under this title, except that  
25      the unclassified report shall not contain information that

1 may be used to identify specific private entities unless  
2 such private entities consent to such identification.

3 **SEC. 708. DEFINITIONS.**

4 In this title:

5 (1) CERTIFIED ENTITY.—The term “certified  
6 entity” means a protected entity, a self-protected en-  
7 tity, or a provider of cybersecurity services that—

8 (A) possesses or is eligible to obtain a se-  
9 curity clearance, as determined by the Director  
10 of National Intelligence; and

11 (B) is able to demonstrate to the Director  
12 of National Intelligence that such provider or  
13 such entity can appropriately protect and use  
14 classified cybersecurity threat indicators.

15 (2) COUNTERMEASURE.—The term “counter-  
16 measure” means automated or manual actions to  
17 modify, redirect, or block information that is stored  
18 on, processed by, or transiting an information sys-  
19 tem that is known or suspected to contain cybersecu-  
20 rity threat indicators for the purpose of protecting  
21 an information system from cybersecurity threats,  
22 conducted on an information system owned or oper-  
23 ated by or on behalf of the party to be protected or  
24 operated by a private entity acting as a provider of  
25 electronic communication services, remote computing

1 services, or cybersecurity services to the party to be  
2 protected.

3 (3) CYBERSECURITY CRIME.—The term “cyber-  
4 security crime” means the violation of a provision of  
5 State or Federal law relating to computer crimes, in-  
6 cluding a violation of any provision of title 18,  
7 United States Code, enacted or amended by the  
8 Computer Fraud and Abuse Act of 1986 (Public  
9 Law 99–474; 100 Stat. 1213).

10 (4) CYBERSECURITY EXCHANGE.—The term  
11 “cybersecurity exchange” means any governmental  
12 entity or private entity designated by the Secretary  
13 of Homeland Security, in consultation with the Di-  
14 rector of National Intelligence, the Attorney Gen-  
15 eral, and the Secretary of Defense, to receive and  
16 distribute cybersecurity threat indicators under sec-  
17 tion 703(a).

18 (5) CYBERSECURITY SERVICES.—The term “cy-  
19 bersecurity services” means products, goods, or serv-  
20 ices intended to detect, mitigate, or prevent cyberse-  
21 curity threats.

22 (6) CYBERSECURITY THREAT.—The term “cy-  
23 bersecurity threat” means any action that may re-  
24 sult in unauthorized access to, exfiltration of, manip-  
25 ulation of, harm of, or impairment to the integrity,

1 confidentiality, or availability of an information sys-  
2 tem or information that is stored on, processed by,  
3 or transiting an information system, except that  
4 none of the following shall be considered a cyberse-  
5 curity threat—

6 (A) actions protected by the first amend-  
7 ment to the Constitution of the United States;  
8 and

9 (B) exceeding authorized access of an in-  
10 formation system, if such access solely involves  
11 a violation of consumer terms of service or con-  
12 sumer licensing agreements.

13 (7) CYBERSECURITY THREAT INDICATOR.—The  
14 term “cybersecurity threat indicator” means infor-  
15 mation—

16 (A) that is reasonably necessary to de-  
17 scribe—

18 (i) malicious reconnaissance, including  
19 anomalous patterns of communications  
20 that reasonably appear to be transmitted  
21 for the purpose of gathering technical in-  
22 formation related to a cybersecurity threat;

23 (ii) a method of defeating a technical  
24 control;

25 (iii) a technical vulnerability;

1 (iv) a method of defeating an oper-  
2 ational control;

3 (v) a method of causing a user with  
4 legitimate access to an information system  
5 or information that is stored on, processed  
6 by, or transiting an information system to  
7 unwittingly enable the defeat of a technical  
8 control or an operational control;

9 (vi) malicious cyber command and  
10 control;

11 (vii) the actual or potential harm  
12 caused by an incident, including informa-  
13 tion exfiltrated as a result of defeating a  
14 technical control or an operational control  
15 when it is necessary in order to identify or  
16 describe a cybersecurity threat;

17 (viii) any other attribute of a cyberse-  
18 curity threat, if disclosure of such attribute  
19 is not otherwise prohibited by law; or

20 (ix) any combination thereof; and

21 (B) from which reasonable efforts have  
22 been made to remove information that can be  
23 used to identify specific persons unrelated to  
24 the cybersecurity threat.

1           (8) FEDERAL CYBERSECURITY CENTER.—The  
2       term “Federal cybersecurity center” means the De-  
3       partment of Defense Cyber Crime Center, the Intel-  
4       ligence Community Incident Response Center, the  
5       United States Cyber Command Joint Operations  
6       Center, the National Cyber Investigative Joint Task  
7       Force, the National Security Agency/Central Secu-  
8       rity Service Threat Operations Center, the United  
9       States Computer Emergency Readiness Team, or  
10      successors to such centers.

11          (9) FEDERAL ENTITY.—The term “Federal en-  
12      tity” means an agency or department of the United  
13      States, or any component, officer, employee, or  
14      agent of such an agency or department.

15          (10) GOVERNMENTAL ENTITY.—The term “gov-  
16      ernmental entity” means any Federal entity and  
17      agency or department of a State, local, tribal, or ter-  
18      ritorial government other than an educational insti-  
19      tution, or any component, officer, employee, or agent  
20      of such an agency or department.

21          (11) INFORMATION SYSTEM.—The term “infor-  
22      mation system” means a discrete set of information  
23      resources organized for the collection, processing,  
24      maintenance, use, sharing, dissemination, or disposi-  
25      tion of information, including communications with,

1 or commands to, specialized systems such as indus-  
2 trial and process control systems, telephone switch-  
3 ing and private branch exchanges, and environ-  
4 mental control systems.

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

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

19 (14) MONITOR.—The term “monitor” means  
20 the interception, acquisition, or collection of informa-  
21 tion that is stored on, processed by, or transiting an  
22 information system for the purpose of identifying cy-  
23 bersecurity threats.

1           (15) NON-FEDERAL ENTITY.—The term “non-  
2       Federal entity” means a private entity or a govern-  
3       mental entity other than a Federal entity.

4           (16) OPERATIONAL CONTROL.—The term  
5       “operational control” means a security control for  
6       an information system that primarily is implemented  
7       and executed by people.

8           (17) PRIVATE ENTITY.—The term “private en-  
9       tity” has the meaning given the term “person” in  
10      section 1 of title 1, United States Code, and does  
11      not include a governmental entity.

12          (18) PROTECT.—The term “protect” means ac-  
13      tions undertaken to secure, defend, or reduce the  
14      vulnerabilities of an information system, mitigate cy-  
15      bersecurity threats, or otherwise enhance informa-  
16      tion security or the resiliency of information systems  
17      or assets.

18          (19) TECHNICAL CONTROL.—The term “tech-  
19      nical control” means a hardware or software restric-  
20      tion on, or audit of, access or use of an information  
21      system or information that is stored on, processed  
22      by, or transiting an information system that is in-  
23      tended to ensure the confidentiality, integrity, or  
24      availability of that system.

- 1           (20) TECHNICAL VULNERABILITY.—The term  
2       “technical vulnerability” means any attribute of  
3       hardware or software that could enable or facilitate  
4       the defeat of a technical control.
- 5           (21) THIRD PARTY.—The term “third party”  
6       includes Federal entities and non-Federal entities.