

**Calendar No. 698**111<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION**S. 3480****[Report No. 111-368]**

To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

---

**IN THE SENATE OF THE UNITED STATES**

JUNE 10, 2010

Mr. LIEBERMAN (for himself, Ms. COLLINS, and Mr. CARPER) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 15, 2010

Reported by Mr. LIEBERMAN, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

---

**A BILL**

To amend the Homeland Security Act of 2002 and other laws 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Protecting Cyberspace  
3 as a National Asset Act of 2010”.

4 **SEC. 2. TABLE OF CONTENTS.**

5 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.
- Sec. 3. Definitions.

TITLE I—OFFICE OF CYBERSPACE POLICY

- Sec. 101. Establishment of the Office of Cyberspace Policy.
- Sec. 102. Appointment and responsibilities of the Director.
- Sec. 103. Prohibition on political campaigning.
- Sec. 104. Review of Federal agency budget requests relating to the National Strategy.
- Sec. 105. Access to intelligence.
- Sec. 106. Consultation.
- Sec. 107. Reports to Congress.

TITLE II—NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS

- Sec. 201. Cybersecurity.

TITLE III—FEDERAL INFORMATION SECURITY MANAGEMENT

- Sec. 301. Coordination of Federal information policy.

TITLE IV—RECRUITMENT AND PROFESSIONAL DEVELOPMENT

- Sec. 401. Definitions.
- Sec. 402. Assessment of cybersecurity workforce.
- Sec. 403. Strategic cybersecurity workforce planning.
- Sec. 404. Cybersecurity occupation classifications.
- Sec. 405. Measures of cybersecurity hiring effectiveness.
- Sec. 406. Training and education.
- Sec. 407. Cybersecurity incentives.
- Sec. 408. Recruitment and retention program for the National Center for Cybersecurity and Communications.

TITLE V—OTHER PROVISIONS

- Sec. 501. Consultation on cybersecurity matters.
- Sec. 502. Cybersecurity research and development.
- Sec. 503. Prioritized critical information infrastructure.
- Sec. 504. National Center for Cybersecurity and Communications acquisition authorities.
- Sec. 505. Technical and conforming amendments.

1 **SEC. 3. DEFINITIONS.**

2 In this Act:

3 (1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—

6 (A) the Committee on Homeland Security  
7 and Governmental Affairs of the Senate;

8 (B) the Committee on Homeland Security  
9 of the House of Representatives;

10 (C) the Committee on Oversight and Gov-  
11 ernment Reform of the House of Representa-  
12 tives; and

13 (D) any other congressional committee  
14 with jurisdiction over the particular matter.

15 (2) **CRITICAL INFRASTRUCTURE.**—The term  
16 “critical infrastructure” has the meaning given that  
17 term in section 1016(e) of the USA PATRIOT Act  
18 (42 U.S.C. 5195e(e)).

19 (3) **CYBERSPACE.**—The term “cyberspace”  
20 means the interdependent network of information in-  
21 frastructure, and includes the Internet, tele-  
22 communications networks, computer systems, and  
23 embedded processors and controllers in critical in-  
24 dustries.

1           (4) ~~DIRECTOR.~~—The term “Director” means  
2 the Director of Cyberspace Policy established under  
3 section 101.

4           (5) ~~FEDERAL AGENCY.~~—The term “Federal  
5 agency”—

6           (A) means any executive department, Gov-  
7 ernment corporation, Government controlled  
8 corporation, or other establishment in the exec-  
9 utive branch of the Government (including the  
10 Executive Office of the President), or any inde-  
11 pendent regulatory agency; and

12           (B) does not include the governments of  
13 the District of Columbia and of the territories  
14 and possessions of the United States and their  
15 various subdivisions.

16           (6) ~~FEDERAL INFORMATION INFRASTRUC-~~  
17 ~~TURE.~~—The term “Federal information infrastruc-  
18 ture”—

19           (A) means information infrastructure that  
20 is owned, operated, controlled, or licensed for  
21 use by, or on behalf of, any Federal agency, in-  
22 cluding information systems used or operated  
23 by another entity on behalf of a Federal agency;  
24 and

25           (B) does not include—

- 1 (i) a national security system; or  
2 (ii) information infrastructure that is  
3 owned, operated, controlled, or licensed for  
4 use by, or on behalf of, the Department of  
5 Defense, a military department, or another  
6 element of the intelligence community.

7 (7) INCIDENT.—The term “incident” means an  
8 occurrence that—

- 9 (A) actually or potentially jeopardizes—  
10 (i) the information security of infor-  
11 mation infrastructure; or  
12 (ii) the information that information  
13 infrastructure processes, stores, receives,  
14 or transmits; or  
15 (B) constitutes a violation or threat of vio-  
16 lation of security policies, security procedures,  
17 or acceptable use policies applicable to informa-  
18 tion infrastructure.

19 (8) INFORMATION INFRASTRUCTURE.—The  
20 term “information infrastructure” means the under-  
21 lying framework that information systems and assets  
22 rely on to process, transmit, receive, or store infor-  
23 mation electronically, including programmable elec-  
24 tronic devices and communications networks and any  
25 associated hardware, software, or data.

1           (9) INFORMATION SECURITY.—The term “infor-  
2           mation security” means protecting information and  
3           information systems from disruption or unauthorized  
4           access, use, disclosure, modification, or destruction  
5           in order to provide—

6                   (A) integrity, by guarding against im-  
7                   proper information modification or destruction,  
8                   including by ensuring information nonrepudi-  
9                   ation and authenticity;

10                   (B) confidentiality, by preserving author-  
11                   ized restrictions on access and disclosure, in-  
12                   cluding means for protecting personal privacy  
13                   and proprietary information; and

14                   (C) availability, by ensuring timely and re-  
15                   liable access to and use of information.

16           (10) INFORMATION TECHNOLOGY.—The term  
17           “information technology” has the meaning given  
18           that term in section 11101 of title 40, United States  
19           Code.

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

24           (12) KEY RESOURCES.—The term “key re-  
25           sources” has the meaning given that term in section

1       2 of the Homeland Security Act of 2002 (6 U.S.C.  
2       101).

3           (13) NATIONAL CENTER FOR CYBERSECURITY  
4       AND COMMUNICATIONS.—The term “National Cen-  
5       ter for Cybersecurity and Communications” means  
6       the National Center for Cybersecurity and Commu-  
7       nications established under section 242(a) of the  
8       Homeland Security Act of 2002, as added by this  
9       Act.

10          (14) NATIONAL INFORMATION INFRASTRUC-  
11       TURE.—The term “national information infrastruc-  
12       ture” means information infrastructure—

13           (A)(i) that is owned, operated, or con-  
14       trolled within or from the United States; or

15           (ii) if located outside the United States,  
16       the disruption of which could result in national  
17       or regional catastrophic damage in the United  
18       States; and

19           (B) that is not owned, operated, controlled,  
20       or licensed for use by a Federal agency.

21          (15) NATIONAL SECURITY SYSTEM.—The term  
22       “national security system” has the meaning given  
23       that term in section 3551 of title 44, United States  
24       Code, as added by this Act.

1           (16) NATIONAL STRATEGY.—The term “Na-  
2           tional Strategy” means the national strategy to in-  
3           crease the security and resiliency of cyberspace de-  
4           veloped under section 101(a)(1).

5           (17) OFFICE.—The term “Office” means the  
6           Office of Cyberspace Policy established under section  
7           101.

8           (18) RISK.—The term “risk” means the poten-  
9           tial for an unwanted outcome resulting from an inci-  
10          dent, as determined by the likelihood of the occur-  
11          rence of the incident and the associated con-  
12          sequences, including potential for an adverse out-  
13          come assessed as a function of threats,  
14          vulnerabilities, and consequences associated with an  
15          incident.

16          (19) RISK-BASED SECURITY.—The term “risk-  
17          based security” has the meaning given that term in  
18          section 3551 of title 44, United States Code, as  
19          added by this Act.

**TITLE I—OFFICE OF  
CYBERSPACE POLICY**

**SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBER-  
SPACE POLICY.**

(a) ESTABLISHMENT OF OFFICE.—There is estab-  
lished in the Executive Office of the President an Office  
of Cyberspace Policy which shall—

(1) develop, not later than 1 year after the date  
of enactment of this Act, and update as needed, but  
not less frequently than once every 2 years, a na-  
tional strategy to increase the security and resiliency  
of cyberspace, that includes goals and objectives re-  
lating to—

(A) computer network operations, includ-  
ing offensive activities, defensive activities, and  
other activities;

(B) information assurance;

(C) protection of critical infrastructure and  
key resources;

(D) research and development priorities;

(E) law enforcement;

(F) diplomacy;

(G) homeland security; and

(H) military and intelligence activities;

1           (2) oversee, coordinate, and integrate all poli-  
2           cies and activities of the Federal Government across  
3           all instruments of national power relating to ensur-  
4           ing the security and resiliency of cyberspace, includ-  
5           ing—

6                   (A) diplomatic, economic, military, intel-  
7                   ligence, homeland security, and law enforcement  
8                   policies and activities within and among Federal  
9                   agencies; and

10                   (B) offensive activities, defensive activities,  
11                   and other policies and activities necessary to en-  
12                   sure effective capabilities to operate in cyber-  
13                   space;

14           (3) ensure that all Federal agencies comply  
15           with appropriate guidelines, policies, and directives  
16           from the Department of Homeland Security, other  
17           Federal agencies with responsibilities relating to  
18           cyberspace security or resiliency, and the National  
19           Center for Cybersecurity and Communications; and

20           (4) ensure that Federal agencies have access to,  
21           receive, and appropriately disseminate law enforc-  
22           ment information, intelligence information, terrorism  
23           information, and any other information (including  
24           information relating to incidents provided under sub-  
25           sections (a)(4) and (c) of section 246 of the Home-

land Security Act of 2002, as added by this Act) relevant to—

(A) the security of the Federal information infrastructure or the national information infrastructure; and

(B) the security of—

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

(ii) a national security system.

(b) DIRECTOR OF CYBERSPACE POLICY.—

(1) IN GENERAL.—There shall be a Director of Cyberspace Policy, who shall be the head of the Office.

(2) EXECUTIVE SCHEDULE POSITION.—Section 5312 of title 5, United States Code, is amended by adding at the end the following:

“Director of Cyberspace Policy.”.

**SEC. 102. APPOINTMENT AND RESPONSIBILITIES OF THE DIRECTOR.**

(a) APPOINTMENT.—

1           (1) IN GENERAL.—The Director shall be ap-  
2           pointed by the President, by and with the advice and  
3           consent of the Senate.

4           (2) QUALIFICATIONS.—The President shall ap-  
5           point the Director from among individuals who have  
6           demonstrated ability and knowledge in information  
7           technology, cybersecurity, and the operations, secu-  
8           rity, and resiliency of communications networks.

9           (3) PROHIBITION.—No person shall serve as  
10          Director while serving in any other position in the  
11          Federal Government.

12         (b) RESPONSIBILITIES.—The Director shall—

13                 (1) advise the President regarding the estab-  
14                 lishment of policies, goals, objectives, and priorities  
15                 for securing the information infrastructure of the  
16                 Nation;

17                 (2) advise the President and other entities with-  
18                 in the Executive Office of the President regarding  
19                 mechanisms to build, and improve the resiliency and  
20                 efficiency of, the information and communication in-  
21                 dustry of the Nation, in collaboration with the pri-  
22                 vate sector, while promoting national economic inter-  
23                 ests;

24                 (3) work with Federal agencies to—

1           (A) oversee, coordinate, and integrate the  
2 implementation of the National Strategy, in-  
3 cluding coordination with—

4           (i) the Department of Homeland Se-  
5 curity;

6           (ii) the Department of Defense;

7           (iii) the Department of Commerce;

8           (iv) the Department of State;

9           (v) the Department of Justice;

10          (vi) the Department of Energy;

11          (vii) through the Director of National  
12 Intelligence, the intelligence community;  
13 and

14          (viii) and any other Federal agency  
15 with responsibilities relating to the Na-  
16 tional Strategy; and

17          (B) resolve any disputes that arise between  
18 Federal agencies relating to the National Strat-  
19 egy or other matters within the responsibility of  
20 the Office;

21          (4) if the policies or activities of a Federal  
22 agency are not in compliance with the responsibil-  
23 ities of the Federal agency under the National Strat-  
24 egy—

25           (A) notify the Federal agency;

1           ~~(B)~~ transmit a copy of each notification  
2           under subparagraph ~~(A)~~ to the President and  
3           the appropriate congressional committees; and

4           ~~(C)~~ coordinate the efforts to bring the  
5           Federal agency into compliance;

6           ~~(5)~~ ensure the adequacy of protections for pri-  
7           vacy and civil liberties in carrying out the respon-  
8           sibilities of the Director under this title, including  
9           through consultation with the Privacy and Civil Lib-  
10          erties Oversight Board established under section  
11          1061 of the National Security Intelligence Reform  
12          Act of 2004 (42 U.S.C. 2000ee);

13          ~~(6)~~ upon reasonable request, appear before any  
14          duly constituted committees of the Senate or of the  
15          House of Representatives;

16          ~~(7)~~ recommend to the Office of Management  
17          and Budget or the head of a Federal agency actions  
18          (including requests to Congress relating to the re-  
19          programming of funds) that the Director determines  
20          are necessary to ensure risk-based security of—

21                  ~~(A)~~ the Federal information infrastructure;

22                  ~~(B)~~ information infrastructure that is  
23                  owned, operated, controlled, or licensed for use  
24                  by, or on behalf of, the Department of Defense;

1 a military department, or another element of  
2 the intelligence community; or

3 ~~(C)~~ a national security system;

4 ~~(8)~~ advise the Administrator of the Office of E-  
5 Government and Information Technology and the  
6 Administrator of the Office of Information and Reg-  
7 ulatory Affairs on the development, and oversee the  
8 implementation, of policies, principles, standards,  
9 guidelines, and budget priorities for information  
10 technology functions and activities of the Federal  
11 Government;

12 ~~(9)~~ coordinate and ensure, to the maximum ex-  
13 tent practicable, that the standards and guidelines  
14 developed for national security systems and the  
15 standards and guidelines under section 20 of the  
16 National Institute of Standards and Technology Act  
17 ~~(15 U.S.C. 278g-3)~~ are complementary and unified;

18 ~~(10)~~ in consultation with the Administrator of  
19 the Office of Information and Regulatory Affairs,  
20 coordinate efforts of Federal agencies relating to the  
21 development of regulations, rules, requirements, or  
22 other actions applicable to the national information  
23 infrastructure to ensure, to the maximum extent  
24 practicable, that the efforts are complementary;

1           (11) coordinate the activities of the Office of  
 2           Science and Technology Policy, the National Eco-  
 3           nomic Council, the Office of Management and Budg-  
 4           et, the National Security Council, the Homeland Se-  
 5           curity Council, and the United States Trade Rep-  
 6           resentative related to the National Strategy and  
 7           other matters within the purview of the Office; and

8           (12) as assigned by the President, other duties  
 9           relating to the security and resiliency of cyberspace.

10 **SEC. 103. PROHIBITION ON POLITICAL CAMPAIGNING.**

11           Section 7323(b)(2)(B) of title 5, United States Code,  
 12 is amended—

13           (1) in clause (i), by striking “or” at the end;

14           (2) in clause (ii), by striking the period at the  
 15           end and inserting “; or”; and

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

17                   “(iii) notwithstanding the exception  
 18                   under subparagraph (A) (relating to an ap-  
 19                   pointment made by the President, by and  
 20                   with the advice and consent of the Senate),  
 21                   the Director of Cyberspace Policy.”.

1 **SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET RE-**  
2 **QUESTS RELATING TO THE NATIONAL STRAT-**  
3 **EGY.**

4 (a) **IN GENERAL.**—For each fiscal year, the head of  
5 each Federal agency shall transmit to the Director a copy  
6 of any portion of the budget of the Federal agency in-  
7 tended to implement the National Strategy at the same  
8 time as that budget request is submitted to the Office of  
9 Management and Budget in the preparation of the budget  
10 of the President submitted to Congress under section  
11 1105 (a) of title 31, United States Code.

12 (b) **TIMELY SUBMISSIONS.**—The head of each Fed-  
13 eral agency shall ensure the timely development and sub-  
14 mission to the Director of each proposed budget under this  
15 section, in such format as may be designated by the Direc-  
16 tor with the concurrence of the Director of the Office of  
17 Management and Budget.

18 (c) **ADEQUACY OF THE PROPOSED BUDGET RE-**  
19 **QUESTS.**—With the assistance of, and in coordination  
20 with, the Office of E-Government and Information Tech-  
21 nology and the National Center for Cybersecurity and  
22 Communications, the Director shall review each budget  
23 submission to assess the adequacy of the proposed request  
24 with regard to implementation of the National Strategy.

25 (d) **INADEQUATE BUDGET REQUESTS.**—If the Direc-  
26 tor concludes that a budget request submitted under sub-

1 section (a) is inadequate, in whole or in part, to implement  
2 the objectives of the National Strategy, the Director shall  
3 submit to the Director of the Office of Management and  
4 Budget and the head of the Federal agency submitting  
5 the budget request a written description of funding levels  
6 and specific initiatives that would, in the determination  
7 of the Director, make the request adequate.

8 **SEC. 105. ACCESS TO INTELLIGENCE.**

9       The Director shall have access to law enforcement in-  
10 formation, intelligence information, terrorism information,  
11 and any other information (including information relating  
12 to incidents provided under subsections (a)(4) and (c) of  
13 section 246 of the Homeland Security Act of 2002, as  
14 added by this Act) that is obtained by, or in the possession  
15 of, any Federal agency that the Director determines rel-  
16 evant to the security of—

- 17           (1) the Federal information infrastructure;
- 18           (2) information infrastructure that is owned,  
19           operated, controlled, or licensed for use by, or on be-  
20           half of, the Department of Defense, a military de-  
21           partment, or another element of the intelligence  
22           community;
- 23           (3) a national security system; or
- 24           (4) national information infrastructure.

1 **SEC. 106. CONSULTATION.**

2 (a) **IN GENERAL.**—The Director may consult and ob-  
3 tain recommendations from, as needed, such Presidential  
4 and other advisory entities as the Director determines will  
5 assist in carrying out the mission of the Office, includ-  
6 ing—

7 (1) the National Security Telecommunications  
8 Advisory Committee;

9 (2) the National Infrastructure Advisory Coun-  
10 cil;

11 (3) the Privacy and Civil Liberties Oversight  
12 Board;

13 (4) the President's Intelligence Advisory Board;

14 (5) the Critical Infrastructure Partnership Ad-  
15 visory Council; and

16 (6) the National Cybersecurity Advisory Council  
17 established under section 239 of the Homeland Se-  
18 curity Act of 2002, as added by this Act.

19 (b) **NATIONAL STRATEGY.**—In developing and updat-  
20 ing the National Strategy the Director shall consult with  
21 the National Cybersecurity Advisory Council and, as ap-  
22 propriate, State and local governments and private enti-  
23 ties.

24 **SEC. 107. REPORTS TO CONGRESS.**

25 (a) **IN GENERAL.**—The Director shall submit an an-  
26 nual report to the appropriate congressional committees

1 describing the activities, ongoing projects, and plans of the  
 2 Federal Government designed to meet the goals and objec-  
 3 tives of the National Strategy.

4 (b) **CLASSIFIED ANNEX.**—A report submitted under  
 5 this section shall be submitted in an unclassified form, but  
 6 may include a classified annex, if necessary.

7 (c) **PUBLIC REPORT.**—An unclassified version of  
 8 each report submitted under this section shall be made  
 9 available to the public.

10 **TITLE H—NATIONAL CENTER**  
 11 **FOR CYBERSECURITY AND**  
 12 **COMMUNICATIONS**

13 **SEC. 201. CYBERSECURITY.**

14 Title H of the Homeland Security Act of 2002 (6  
 15 U.S.C. 121 et seq.) is amended by adding at the end the  
 16 following:

17 **“Subtitle E—Cybersecurity**

18 **“SEC. 241. DEFINITIONS.**

19 “In this subtitle—

20 “(1) the term ‘agency information infrastruc-  
 21 ture’ means the Federal information infrastructure  
 22 of a particular Federal agency;

23 “(2) the term ‘appropriate committees of Con-  
 24 gress’ means the Committee on Homeland Security  
 25 and Governmental Affairs of the Senate and the

1 Committee on Homeland Security of the House of  
2 Representatives;

3 “(3) the term ‘Center’ means the National Cen-  
4 ter for Cybersecurity and Communications estab-  
5 lished under section 242(a);

6 “(4) the term ‘covered critical infrastructure’  
7 means a system or asset—

8 “(A) that is on the prioritized critical in-  
9 frastructure list established by the Secretary  
10 under section 210E(a)(2); and

11 “(B)(i) that is a component of the national  
12 information infrastructure; or

13 “(ii) for which the national information in-  
14 frastructure is essential to the reliable operation  
15 of the system or asset;

16 “(5) the term ‘cyber vulnerability’ means any  
17 security vulnerability that, if exploited, could pose a  
18 significant risk of disruption to the operation of in-  
19 formation infrastructure essential to the reliable op-  
20 eration of covered critical infrastructure;

21 “(6) the term ‘Director’ means the Director of  
22 the Center appointed under section 242(b)(1);

23 “(7) the term ‘Federal agency’—

24 “(A) means any executive department,  
25 military department, Government corporation,

1 Government controlled corporation, or other es-  
2 tablishment in the executive branch of the Gov-  
3 ernment (including the Executive Office of the  
4 President); or any independent regulatory agen-  
5 ey; and

6 “(B) does not include the governments of  
7 the District of Columbia and of the territories  
8 and possessions of the United States and their  
9 various subdivisions;

10 “(8) the term ‘Federal information infrastruc-  
11 ture’—

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

18 “(B) does not include—

19 “(i) a national security system; or

20 “(ii) information infrastructure that is  
21 owned, operated, controlled, or licensed for  
22 use by, or on behalf of, the Department of  
23 Defense, a military department, or another  
24 element of the intelligence community;

1           “(9) the term ‘incident’ means an occurrence  
2 that—

3           “(A) actually or potentially jeopardizes—

4           “(i) the information security of infor-  
5 mation infrastructure; or

6           “(ii) the information that information  
7 infrastructure processes, stores, receives,  
8 or transmits; or

9           “(B) constitutes a violation or threat of  
10 violation of security policies, security proce-  
11 dures, or acceptable use policies applicable to  
12 information infrastructure.

13           “(10) the term ‘information infrastructure’  
14 means the underlying framework that information  
15 systems and assets rely on to process, transmit, re-  
16 ceive, or store information electronically, including—

17           “(A) programmable electronic devices and  
18 communications networks; and

19           “(B) any associated hardware, software, or  
20 data;

21           “(11) the term ‘information security’ means  
22 protecting information and information systems  
23 from disruption or unauthorized access, use, disclo-  
24 sure, modification, or destruction in order to pro-  
25 vide—

1           “(A) integrity, by guarding against im-  
2           proper information modification or destruction,  
3           including by ensuring information nonrepudi-  
4           ation and authenticity;

5           “(B) confidentiality, by preserving author-  
6           ized restrictions on access and disclosure, in-  
7           cluding means for protecting personal privacy  
8           and proprietary information; and

9           “(C) availability, by ensuring timely and  
10          reliable access to and use of information;

11          “(12) the term ‘information sharing and anal-  
12          ysis center’ means a self-governed forum whose  
13          members work together within a specific sector of  
14          critical infrastructure to identify, analyze, and share  
15          with other members and the Federal Government  
16          critical information relating to threats,  
17          vulnerabilities, or incidents to the security and resil-  
18          iency of the critical infrastructure that comprises the  
19          specific sector;

20          “(13) the term ‘information system’ has the  
21          meaning given that term in section 3502 of title 44,  
22          United States Code;

23          “(14) the term ‘intelligence community’ has the  
24          meaning given that term in section 3(4) of the Na-  
25          tional Security Act of 1947 (50 U.S.C. 401a(4));

1           “(15) the term ‘management controls’ means  
2 safeguards or countermeasures for an information  
3 system that focus on the management of risk and  
4 the management of information system security;

5           “(16) the term ‘National Cybersecurity Advi-  
6 sory Council’ means the National Cybersecurity Ad-  
7 visory Council established under section 239;

8           “(17) the term ‘national cyber emergency’  
9 means an actual or imminent action by any indi-  
10 vidual or entity to exploit a cyber vulnerability in a  
11 manner that disrupts, attempts to disrupt, or poses  
12 a significant risk of disruption to the operation of  
13 the information infrastructure essential to the reli-  
14 able operation of covered critical infrastructure;

15           “(18) the term ‘national information infrastruc-  
16 ture’ means information infrastructure—

17           “(A)(i) that is owned, operated, or con-  
18 trolled within or from the United States; or

19           “(ii) if located outside the United States,  
20 the disruption of which could result in national  
21 or regional catastrophic damage in the United  
22 States; and

23           “(B) that is not owned, operated, con-  
24 trolled, or licensed for use by a Federal agency;

1           “(19) the term ‘national security system’ has  
2 the same meaning given that term in section 3551  
3 of title 44, United States Code;

4           “(20) the term ‘operational controls’ means the  
5 safeguards and countermeasures for an information  
6 system that are primarily implemented and executed  
7 by individuals not systems;

8           “(21) the term ‘sector-specific agency’ means  
9 the relevant Federal agency responsible for infra-  
10 structure protection activities in a designated critical  
11 infrastructure sector or key resources category under  
12 the National Infrastructure Protection Plan, or any  
13 other appropriate Federal agency identified by the  
14 President after the date of enactment of this sub-  
15 title;

16           “(22) the term ‘sector coordinating councils’  
17 means self-governed councils that are composed of  
18 representatives of key stakeholders within a specific  
19 sector of critical infrastructure that serve as the  
20 principal private sector policy coordination and plan-  
21 ning entities with the Federal Government relating  
22 to the security and resiliency of the critical infra-  
23 structure that comprise that sector;

24           “(23) the term ‘security controls’ means the  
25 management, operational, and technical controls pre-

1 scribed for an information system to protect the in-  
2 formation security of the system;

3 “(24) the term ‘small business concern’ has the  
4 meaning given that term under section 3 of the  
5 Small Business Act (15 U.S.C. 632);

6 “(25) the term ‘technical controls’ means the  
7 safeguards or countermeasures for an information  
8 system that are primarily implemented and executed  
9 by the information system through mechanisms con-  
10 tained in the hardware, software, or firmware com-  
11 ponents of the system;

12 “(26) the term ‘terrorism information’ has the  
13 meaning given that term in section 1016 of the In-  
14 telligence Reform and Terrorism Prevention Act of  
15 2004 (6 U.S.C. 485);

16 “(27) the term ‘United States person’ has the  
17 meaning given that term in section 101 of the For-  
18 eign Intelligence Surveillance Act of 1978 (50  
19 U.S.C. 1801); and

20 “(28) the term ‘US-CERT’ means the United  
21 States Computer Readiness Team established under  
22 section 244.

23 **“SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND**  
24 **COMMUNICATIONS.**

25 “(a) ESTABLISHMENT.—

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

4           “(2) OPERATIONAL ENTITY.—The Center  
5 may—

6           “(A) enter into contracts for the procure-  
7 ment of property and services for the Center;  
8 and

9           “(B) appoint employees of the Center in  
10 accordance with the civil service laws of the  
11 United States.

12          “(b) DIRECTOR.—

13           “(1) IN GENERAL.—The Center shall be headed  
14 by a Director, who shall be appointed by the Presi-  
15 dent, by and with the advice and consent of the Sen-  
16 ate.

17           “(2) REPORTING TO SECRETARY.—The Direc-  
18 tor shall report directly to the Secretary and serve  
19 as the principal advisor to the Secretary on cyberse-  
20 curity and the operations, security, and resiliency of  
21 the communications infrastructure of the United  
22 States.

23           “(3) PRESIDENTIAL ADVICE.—The Director  
24 shall regularly advise the President on the exercise  
25 of the authorities provided under this subtitle or any

1 other provision of law relating to the security of the  
2 Federal information infrastructure or an agency in-  
3 formation infrastructure.

4 “(4) QUALIFICATIONS.—The Director shall be  
5 appointed from among individuals who have—

6 “(A) a demonstrated ability in and knowl-  
7 edge of information technology, cybersecurity,  
8 and the operations, security and resiliency of  
9 communications networks; and

10 “(B) significant executive leadership and  
11 management experience in the public or private  
12 sector.

13 “(5) LIMITATION ON SERVICE.—

14 “(A) IN GENERAL.—Subject to subpara-  
15 graph (B), the individual serving as the Direc-  
16 tor may not, while so serving, serve in any  
17 other capacity in the Federal Government, ex-  
18 cept to the extent that the individual serving as  
19 Director is doing so in an acting capacity.

20 “(B) EXCEPTION.—The Director may  
21 serve on any commission, board, council, or  
22 similar entity with responsibilities or duties re-  
23 lating to cybersecurity or the operations, secu-  
24 rity, and resiliency of the communications infra-  
25 structure of the United States at the direction

1 of the President or as otherwise provided by  
2 law.

3 ~~“(c) DEPUTY DIRECTORS.—~~

4 ~~“(1) IN GENERAL.—~~There shall be not less  
5 than 2 Deputy Directors for the Center, who shall  
6 report to the Director.

7 ~~“(2) INFRASTRUCTURE PROTECTION.—~~

8 ~~“(A) APPOINTMENT.—~~There shall be a  
9 Deputy Director appointed by the Secretary,  
10 who shall have expertise in infrastructure pro-  
11 tection.

12 ~~“(B) RESPONSIBILITIES.—~~The Deputy Di-  
13 rector appointed under subparagraph (A)  
14 shall—

15 ~~“(i) assist the Director and the As-~~  
16 ~~stant Secretary for Infrastructure Protec-~~  
17 ~~tion in coordinating, managing, and direct-~~  
18 ~~ing the information, communications, and~~  
19 ~~physical infrastructure protection respon-~~  
20 ~~sibilities and activities of the Department,~~  
21 ~~including activities under Homeland Secu-~~  
22 ~~rity Presidential Directive 7, or any suc-~~  
23 ~~cessor thereto, and the National Infra-~~  
24 ~~structure Protection Plan, or any successor~~  
25 ~~thereto;~~

1           “(ii) review the budget for the Center  
2           and the Office of Infrastructure Protection  
3           before submission of the budget to the Sec-  
4           retary to ensure that activities are appro-  
5           priately coordinated;

6           “(iii) develop, update periodically, and  
7           submit to the appropriate committees of  
8           Congress a strategic plan detailing how  
9           critical infrastructure protection activities  
10          will be coordinated between the Center, the  
11          Office of Infrastructure Protection, and  
12          the private sector;

13          “(iv) subject to the direction of the  
14          Director resolve conflicts between the Cen-  
15          ter and the Office of Infrastructure Protec-  
16          tion relating to the information, commu-  
17          nications, and physical infrastructure pro-  
18          tection responsibilities of the Center and  
19          the Office of Infrastructure Protection;  
20          and

21          “(v) perform such other duties as the  
22          Director may assign.

23          “(C) ANNUAL EVALUATION.—The Assist-  
24          ant Secretary for Infrastructure Protection  
25          shall submit annually to the Director an evalua-

1           tion of the performance of the Deputy Director  
2           appointed under subparagraph (A).

3           “(3) INTELLIGENCE COMMUNITY.—The Direc-  
4           tor of National Intelligence shall identify an em-  
5           ployee of an element of the intelligence community  
6           to serve as a Deputy Director of the Center. The  
7           employee shall be detailed to the Center on a reim-  
8           bursable basis for such period as is agreed to by the  
9           Director and the Director of National Intelligence,  
10          and, while serving as Deputy Director, shall report  
11          directly to the Director of the Center.

12          “(d) LIAISON OFFICERS.—The Secretary of Defense,  
13          the Attorney General, the Secretary of Commerce, and the  
14          Director of National Intelligence shall detail personnel to  
15          the Center to act as full-time liaisons with the Department  
16          of Defense, the Department of Justice, the National Insti-  
17          tute of Standards and Technology, and elements of the  
18          intelligence community to assist in coordination between  
19          and among the Center, the Department of Defense, the  
20          Department of Justice, the National Institute of Stand-  
21          ards and Technology, and elements of the intelligence  
22          community.

23          “(e) PRIVACY OFFICER.—

1           “(1) IN GENERAL.—The Director, in consulta-  
2           tion with the Secretary, shall designate a full-time  
3           privacy officer, who shall report to the Director.

4           “(2) DUTIES.—The privacy officer designated  
5           under paragraph (1) shall have primary responsi-  
6           bility for implementation by the Center of the pri-  
7           vacy policy for the Department established by the  
8           Privacy Officer appointed under section 222.

9           “(f) DUTIES OF DIRECTOR.—

10           “(1) IN GENERAL.—The Director shall—

11           “(A) working cooperatively with the private  
12           sector, lead the Federal effort to secure, pro-  
13           tect, and ensure the resiliency of the Federal in-  
14           formation infrastructure and national informa-  
15           tion infrastructure of the United States, includ-  
16           ing communications networks;

17           “(B) assist in the identification, remedi-  
18           ation, and mitigation of vulnerabilities to the  
19           Federal information infrastructure and the na-  
20           tional information infrastructure;

21           “(C) provide dynamic, comprehensive, and  
22           continuous situational awareness of the security  
23           status of the Federal information infrastruc-  
24           ture, national information infrastructure, and  
25           information infrastructure that is owned, oper-

1           ated, controlled, or licensed for use by, or on  
2           behalf of, the Department of Defense, a mili-  
3           tary department, or another element of the in-  
4           telligence community by sharing and inte-  
5           grating classified and unclassified information,  
6           including information relating to threats,  
7           vulnerabilities, traffic, trends, incidents, and  
8           other anomalous activities affecting the infra-  
9           structure or systems, on a routine and contin-  
10          uous basis with—

11                   “(i) the National Threat Operations  
12                   Center of the National Security Agency;

13                   “(ii) the United States Cyber Com-  
14                   mand, including the Joint Task Force-  
15                   Global Network Operations;

16                   “(iii) the Cyber Crime Center of the  
17                   Department of Defense;

18                   “(iv) the National Cyber Investigative  
19                   Joint Task Force;

20                   “(v) the Intelligence Community Inci-  
21                   dent Response Center;

22                   “(vi) any other Federal agency, or  
23                   component thereof, identified by the Direc-  
24                   tor; and

1           “(vii) any non-Federal entity, includ-  
2           ing, where appropriate, information shar-  
3           ing and analysis centers, identified by the  
4           Director, with the concurrence of the  
5           owner or operator of that entity and con-  
6           sistent with applicable law;

7           “(D) work with the entities described in  
8           subparagraph (C) to establish policies and pro-  
9           cedures that enable information sharing be-  
10          tween and among the entities;

11          “(E) develop, in coordination with the As-  
12          sistant Secretary for Infrastructure Protection,  
13          other Federal agencies, the private sector, and  
14          State and local governments, a national incident  
15          response plan that details the roles of Federal  
16          agencies, State and local governments, and the  
17          private sector, including plans to be executed in  
18          response to a declaration of a national cyber  
19          emergency by the President under section 249;

20          “(F) conduct risk-based assessments of the  
21          Federal information infrastructure with respect  
22          to acts of terrorism, natural disasters, and  
23          other large-scale disruptions and provide the re-  
24          sults of the assessments to the Director of  
25          Cyberspace Policy;

1           “(G) develop, oversee the implementation  
2 of, and enforce policies, principles, and guide-  
3 lines on information security for the Federal in-  
4 formation infrastructure, including timely adop-  
5 tion of and compliance with standards devel-  
6 oped by the National Institute of Standards  
7 and Technology under section 20 of the Na-  
8 tional Institute of Standards and Technology  
9 Act (15 U.S.C. 278g-3);

10           “(H) provide assistance to the National In-  
11 stitute of Standards and Technology in devel-  
12 oping standards under section 20 of the Na-  
13 tional Institute of Standards and Technology  
14 Act (15 U.S.C. 278g-3);

15           “(I) provide to Federal agencies manda-  
16 tory security controls to mitigate and remediate  
17 vulnerabilities of and incidents affecting the  
18 Federal information infrastructure;

19           “(J) subject to paragraph (2), and as  
20 needed, assist the Director of the Office of  
21 Management and Budget and the Director of  
22 Cyberspace Policy in conducting analysis and  
23 prioritization of budgets, relating to the secu-  
24 rity of the Federal information infrastructure;

1           “(K) in accordance with section 253, de-  
2           velop, periodically update, and implement a  
3           supply chain risk management strategy to en-  
4           hance, in a risk-based and cost-effective man-  
5           ner, the security of the communications and in-  
6           formation technology products and services pur-  
7           chased by the Federal Government;

8           “(L) notify the Director of Cyberspace  
9           Policy of any incident involving the Federal in-  
10          formation infrastructure, information infra-  
11          structure that is owned, operated, controlled, or  
12          licensed for use by, or on behalf of, the Depart-  
13          ment of Defense, a military department, or an-  
14          other element of the intelligence community, or  
15          the national information infrastructure that  
16          could compromise or significantly affect eco-  
17          nomic or national security;

18          “(M) consult, in coordination with the Di-  
19          rector of Cyberspace Policy, with appropriate  
20          international partners to enhance the security  
21          of the Federal information infrastructure and  
22          national information infrastructure;

23          “(N)(i) coordinate and integrate informa-  
24          tion to analyze the composite security state of  
25          the Federal information infrastructure and in-

1 formation infrastructure that is owned, oper-  
2 ated, controlled, or licensed for use by, or on  
3 behalf of, the Department of Defense, a mili-  
4 tary department, or another element of the in-  
5 telligence community;

6 “(ii) ensure the information required under  
7 clause (i) and section 3553(e)(1)(A) of title 44,  
8 United States Code, including the views of the  
9 Director on the adequacy and effectiveness of  
10 information security throughout the Federal in-  
11 formation infrastructure and information infra-  
12 structure that is owned, operated, controlled, or  
13 licensed for use by, or on behalf of, the Depart-  
14 ment of Defense, a military department, or an-  
15 other element of the intelligence community, is  
16 available on an automated and continuous basis  
17 through the system maintained under section  
18 3552(a)(3)(D) of title 44, United States Code;

19 “(iii) in conjunction with the quadrennial  
20 homeland security review required under section  
21 707, and at such other times determined appro-  
22 priate by the Director, analyze the composite  
23 security state of the national information infra-  
24 structure and submit to the President, Con-  
25 gress, and the Secretary a report regarding ac-

1 tions necessary to enhance the composite secu-  
2 rity state of the national information infrastruc-  
3 ture based on the analysis; and

4 “(iv) foster collaboration and serve as the  
5 primary contact between the Federal Govern-  
6 ment, State and local governments, and private  
7 entities on matters relating to the security of  
8 the Federal information infrastructure and the  
9 national information infrastructure;

10 “(O) oversee the development, implementa-  
11 tion, and management of security requirements  
12 for Federal agencies relating to the external ac-  
13 cess points to or from the Federal information  
14 infrastructure;

15 “(P) establish, develop, and oversee the ca-  
16 pabilities and operations within the US-CERT  
17 as required by section 244;

18 “(Q) oversee the operations of the National  
19 Communications System, as described in Execu-  
20 tive Order 12472 (49 Fed. Reg. 13471; relating  
21 to the assignment of national security and  
22 emergency preparedness telecommunications  
23 functions), as amended by Executive Order  
24 13286 (68 Fed. Reg. 10619) and Executive  
25 Order 13407 (71 Fed. Reg. 36975), or any suc-

1           cessor thereto, including planning for and pro-  
2           viding communications for the Federal Govern-  
3           ment under all circumstances, including crises,  
4           emergencies, attacks, recoveries, and reconstitu-  
5           tions;

6           “(R) ensure, in coordination with the pri-  
7           vacy officer designated under subsection (c), the  
8           Privacy Officer appointed under section 222,  
9           and the Director of the Office of Civil Rights  
10          and Civil Liberties appointed under section 705,  
11          that the activities of the Center comply with all  
12          policies, regulations, and laws protecting the  
13          privacy and civil liberties of United States per-  
14          sons;

15          “(S) subject to the availability of re-  
16          sources, and at the discretion of the Director,  
17          provide voluntary technical assistance—

18                 “(i) at the request of an owner or op-  
19                 erator of covered critical infrastructure, to  
20                 assist the owner or operator in complying  
21                 with sections 248 and 249, including im-  
22                 plementing required security or emergency  
23                 measures and developing response plans  
24                 for national cyber emergencies declared  
25                 under section 249; and

1           “(ii) at the request of the owner or  
2           operator of national information infra-  
3           structure that is not covered critical infra-  
4           structure, and based on risk, to assist the  
5           owner or operator in implementing best  
6           practices, and related standards and guide-  
7           lines, recommended under section 247 and  
8           other measures necessary to mitigate or re-  
9           mediate vulnerabilities of the information  
10          infrastructure and the consequences of ef-  
11          forts to exploit the vulnerabilities;

12          “(T)(i) conduct, in consultation with the  
13          National Cybersecurity Advisory Council, the  
14          head of appropriate sector-specific agencies, and  
15          any private sector entity determined appro-  
16          priate by the Director, risk-based assessments  
17          of national information infrastructure, on a sec-  
18          tor-by-sector basis, with respect to acts of ter-  
19          rorism, natural disasters, and other large-scale  
20          disruptions or financial harm, which shall iden-  
21          tify and prioritize risks to the national informa-  
22          tion infrastructure, including vulnerabilities and  
23          associated consequences; and

1           “(ii) coordinate and evaluate the mitigation  
2 or remediation of cyber vulnerabilities and con-  
3 sequences identified under clause (i);

4           “(U) regularly evaluate and assess tech-  
5 nologies designed to enhance the protection of  
6 the Federal information infrastructure and na-  
7 tional information infrastructure, including an  
8 assessment of the cost-effectiveness of the tech-  
9 nologies;

10           “(V) promote the use of the best practices  
11 recommended under section 247 to State and  
12 local governments and the private sector;

13           “(W) develop and implement outreach and  
14 awareness programs on cybersecurity, includ-  
15 ing—

16           “(i) a public education campaign to  
17 increase the awareness of cybersecurity,  
18 cyber safety, and cyber ethics, which shall  
19 include use of the Internet, social media,  
20 entertainment, and other media to reach  
21 the public;

22           “(ii) an education campaign to in-  
23 crease the understanding of State and local  
24 governments and private sector entities of  
25 the costs of failing to ensure effective secu-

1 rity of information infrastructure and cost-  
2 effective methods to mitigate and reme-  
3 diate vulnerabilities; and

4 “(iii) outcome-based performance  
5 measures to determine the success of the  
6 programs;

7 “(X) develop and implement a national cy-  
8 bersecurity exercise program that includes—

9 “(i) the participation of State and  
10 local governments, international partners  
11 of the United States, and the private sec-  
12 tor; and

13 “(ii) an after action report analyzing  
14 lessons learned from exercises and identi-  
15 fying vulnerabilities to be remediated or  
16 mitigated;

17 “(Y) coordinate with the Assistant Sec-  
18 retary for Infrastructure Protection to ensure  
19 that—

20 “(i) cybersecurity is appropriately ad-  
21 dressed in carrying out the infrastructure  
22 protection responsibilities described in sec-  
23 tion 201(d); and

24 “(ii) the operations of the Center and  
25 the Office of Infrastructure Protection

1           avoid duplication and use, to the maximum  
2           extent practicable, joint mechanisms for in-  
3           formation sharing and coordination with  
4           the private sector;

5           “(Z) oversee the activities of the Office of  
6           Emergency Communications established under  
7           section 1801; and

8           “(AA) perform such other duties as the  
9           Secretary may direct relating to the security  
10          and resiliency of the information and commu-  
11          nications infrastructure of the United States.

12          “(2) BUDGET ANALYSIS.—In conducting anal-  
13          ysis and prioritization of budgets under paragraph  
14          (1)(J), the Director—

15               “(A) in coordination with the Director of  
16               the Office of Management and Budget, may ac-  
17               cess information from any Federal agency re-  
18               garding the finances, budget, and programs of  
19               the Federal agency relevant to the security of  
20               the Federal information infrastructure;

21               “(B) may make recommendations to the  
22               Director of the Office of Management and  
23               Budget and the Director of Cyberspace Policy  
24               regarding the budget for each Federal agency  
25               to ensure that adequate funding is devoted to

1           securing the Federal information infrastructure,  
 2           in accordance with policies, principles, and  
 3           guidelines established by the Director under  
 4           this subtitle; and

5           “(C) shall provide copies of any rec-  
 6           ommendations made under subparagraph (B)  
 7           to—

8                   “(i) the Committee on Appropriations  
 9                   of the Senate;

10                   “(ii) the Committee on Appropriations  
 11                   of the House of Representatives; and

12                   “(iii) the appropriate committees of  
 13                   Congress.

14           “(g) USE OF MECHANISMS FOR COLLABORATION.—

15 In carrying out the responsibilities and authorities of the  
 16 Director under this subtitle, to the maximum extent prac-  
 17 ticable, the Director shall use mechanisms for collabora-  
 18 tion and information sharing (including mechanisms relat-  
 19 ing to the identification and communication of threats,  
 20 vulnerabilities, and associated consequences) established  
 21 by other components of the Department or other Federal  
 22 agencies to avoid unnecessary duplication or waste.

23           “(h) SUFFICIENCY OF RESOURCES PLAN.—

24                   “(1) REPORT.—Not later than 120 days after  
 25                   the date of enactment of this subtitle, the Director

1 of the Office of Management and Budget shall sub-  
2 mit to the appropriate committees of Congress and  
3 the Comptroller General of the United States a re-  
4 port on the resources and staff necessary to carry  
5 out fully the responsibilities under this subtitle.

6 ~~“(2) COMPTROLLER GENERAL REVIEW.—~~

7 ~~“(A) IN GENERAL.—The Comptroller Gen-~~  
8 ~~eral of the United States shall evaluate the rea-~~  
9 ~~sonableness and adequacy of the report sub-~~  
10 ~~mitted by the Director under paragraph (1).~~

11 ~~“(B) REPORT.—Not later than 60 days~~  
12 ~~after the date on which the report is submitted~~  
13 ~~under paragraph (1), the Comptroller General~~  
14 ~~shall submit to the appropriate committees of~~  
15 ~~Congress a report containing the findings of the~~  
16 ~~review under subparagraph (A).~~

17 ~~“(i) FUNCTIONS TRANSFERRED.—There are trans-~~  
18 ~~ferred to the Center the National Cyber Security Division,~~  
19 ~~the Office of Emergency Communications, and the Na-~~  
20 ~~tional Communications System, including all the func-~~  
21 ~~tions, personnel, assets, authorities, and liabilities of the~~  
22 ~~National Cyber Security Division and the National Com-~~  
23 ~~munications System.~~

1 ~~“SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COL-~~  
 2 ~~LABORATION.~~

3 ~~“(a) IN GENERAL.—The Director and the Assistant~~  
 4 ~~Secretary for Infrastructure Protection shall coordinate~~  
 5 ~~the information, communications, and physical infrastruc-~~  
 6 ~~ture protection responsibilities and activities of the Center~~  
 7 ~~and the Office of Infrastructure Protection.~~

8 ~~“(b) OVERSIGHT.—The Secretary shall ensure that~~  
 9 ~~the coordination described in subsection (a) occurs.~~

10 ~~“SEC. 244. UNITED STATES COMPUTER EMERGENCY READI-~~  
 11 ~~NESS TEAM.~~

12 ~~“(a) ESTABLISHMENT OF OFFICE.—There is estab-~~  
 13 ~~lished within the Center, the United States Computer~~  
 14 ~~Emergency Readiness Team, which shall be headed by a~~  
 15 ~~Director, who shall be selected from the Senior Executive~~  
 16 ~~Service by the Secretary.~~

17 ~~“(b) RESPONSIBILITIES.—The US-CERT shall—~~

18 ~~“(1) collect, coordinate, and disseminate infor-~~  
 19 ~~mation on—~~

20 ~~“(A) risks to the Federal information in-~~  
 21 ~~frastructure, information infrastructure that is~~  
 22 ~~owned, operated, controlled, or licensed for use~~  
 23 ~~by, or on behalf of, the Department of Defense,~~  
 24 ~~a military department, or another element of~~  
 25 ~~the intelligence community, or the national in-~~  
 26 ~~formation infrastructure; and~~

1           ~~“(B) security controls to enhance the secu-~~  
2           ~~rity of the Federal information infrastructure~~  
3           ~~or the national information infrastructure~~  
4           ~~against the risks identified in subparagraph~~  
5           ~~(A); and~~

6           ~~“(2) establish a mechanism for engagement~~  
7           ~~with the private sector.~~

8           ~~“(e) MONITORING, ANALYSIS, WARNING, AND RE-~~  
9           ~~SPONSE.—~~

10           ~~“(1) DUTIES.—Subject to paragraph (2), the~~  
11           ~~US-CERT shall—~~

12           ~~“(A) provide analysis and reports to Fed-~~  
13           ~~eral agencies on the security of the Federal in-~~  
14           ~~formation infrastructure;~~

15           ~~“(B) provide continuous, automated moni-~~  
16           ~~toring of the Federal information infrastructure~~  
17           ~~at external Internet access points, which shall~~  
18           ~~include detection and warning of threats,~~  
19           ~~vulnerabilities, traffic, trends, incidents, and~~  
20           ~~other anomalous activities affecting the infor-~~  
21           ~~mation security of the Federal information in-~~  
22           ~~frastructure;~~

23           ~~“(C) warn Federal agencies of threats,~~  
24           ~~vulnerabilities, incidents, and anomalous activi-~~

1 ties that could affect the Federal information  
2 infrastructure;

3 “(D) develop, recommend, and deploy secu-  
4 rity controls to mitigate or remediate  
5 vulnerabilities;

6 “(E) support Federal agencies in con-  
7 ducting risk assessments of the agency informa-  
8 tion infrastructure;

9 “(F) disseminate to Federal agencies risk  
10 analyses of incidents that could impair the risk-  
11 based security of the Federal information infra-  
12 structure;

13 “(G) develop and acquire predictive ana-  
14 lytic tools to evaluate threats, vulnerabilities,  
15 traffic, trends, incidents, and anomalous activi-  
16 ties;

17 “(H) aid in the detection of, and warn  
18 owners or operators of national information in-  
19 frastructure regarding, threats, vulnerabilities,  
20 and incidents, affecting the national informa-  
21 tion infrastructure, including providing—

22 “(i) timely, targeted, and actionable  
23 notifications of threats, vulnerabilities, and  
24 incidents; and

1                   “(ii) recommended security controls to  
2                   mitigate or remediate vulnerabilities; and

3                   “(I) respond to assistance requests from  
4                   Federal agencies and, subject to the availability  
5                   of resources, owners or operators of the na-  
6                   tional information infrastructure to—

7                   “(i) isolate, mitigate, or remediate in-  
8                   cidents;

9                   “(ii) recover from damages and miti-  
10                  gate or remediate vulnerabilities; and

11                  “(iii) evaluate security controls and  
12                  other actions taken to secure information  
13                  infrastructure and incorporate lessons  
14                  learned into best practices, policies, prin-  
15                  ciples, and guidelines.

16                  “(2) REQUIREMENT.—With respect to the Fed-  
17                  eral information infrastructure, the US-CERT shall  
18                  conduct the activities described in paragraph (1) in  
19                  a manner consistent with the responsibilities of the  
20                  head of a Federal agency described in section 3553  
21                  of title 44, United States Code.

22                  “(3) REPORT.—Not later than 1 year after the  
23                  date of enactment of this subtitle, and every year  
24                  thereafter, the Secretary shall—

1           “(A) in conjunction with the Inspector  
2           General of the Department, conduct an inde-  
3           pendent audit or review of the activities of the  
4           US-CERT under paragraph (1)(B); and

5           “(B) submit to the appropriate committees  
6           of Congress and the President a report regard-  
7           ing the audit or report.

8           “(d) PROCEDURES FOR FEDERAL GOVERNMENT.—  
9           Not later than 90 days after the date of enactment of this  
10          subtitle, the head of each Federal agency shall establish  
11          procedures for the Federal agency that ensure that the  
12          US-CERT can perform the functions described in sub-  
13          section (c) in relation to the Federal agency.

14          “(e) OPERATIONAL UPDATES.—The US-CERT shall  
15          provide unclassified and, as appropriate, classified updates  
16          regarding the composite security state of the Federal in-  
17          formation infrastructure to the Federal Information Secu-  
18          rity Taskforce.

19          “(f) FEDERAL POINTS OF CONTACT.—The Director  
20          of the US-CERT shall designate a principal point of con-  
21          tact within the US-CERT for each Federal agency to—

22                 “(1) maintain communication;

23                 “(2) ensure cooperative engagement and infor-  
24                 mation sharing; and

25                 “(3) respond to inquiries or requests.

1       “(g) REQUESTS FOR INFORMATION OR PHYSICAL AC-  
2       CESS.—

3               “(1) INFORMATION ACCESS.—Upon request of  
4       the Director of the US-CERT, the head of a Fed-  
5       eral agency or an Inspector General for a Federal  
6       agency shall provide any law enforcement informa-  
7       tion, intelligence information, terrorism information,  
8       or any other information (including information re-  
9       lating to incidents provided under subsections (a)(4)  
10      and (c) of section 246) relevant to the security of  
11      the Federal information infrastructure or the na-  
12      tional information infrastructure necessary to carry  
13      out the duties, responsibilities, and authorities under  
14      this subtitle.

15              “(2) PHYSICAL ACCESS.—Upon request of the  
16      Director, and in consultation with the head of a  
17      Federal agency, the Federal agency shall provide  
18      physical access to any facility of the Federal agency  
19      necessary to determine whether the Federal agency  
20      is in compliance with any policies, principles, and  
21      guidelines established by the Director under this  
22      subtitle, or otherwise necessary to carry out the du-  
23      ties, responsibilities, and authorities of the Director  
24      applicable to the Federal information infrastructure.

1 **“SEC. 245. ADDITIONAL AUTHORITIES OF THE DIRECTOR**  
2 **OF THE NATIONAL CENTER FOR CYBERSECU-**  
3 **RITY AND COMMUNICATIONS.**

4 **“(a) ACCESS TO INFORMATION.—**Unless otherwise  
5 directed by the President—

6 **“(1)** the Director shall access, receive, and ana-  
7 lyze law enforcement information, intelligence infor-  
8 mation, terrorism information, and any other infor-  
9 mation (including information relating to incidents  
10 provided under subsections (a)(4) and (e) of section  
11 246) relevant to the security of the Federal informa-  
12 tion infrastructure, information infrastructure that  
13 is owned, operated, controlled, or licensed for use by,  
14 or on behalf of, the Department of Defense, a mili-  
15 tary department, or another element of the intel-  
16 ligence community, or national information infra-  
17 structure from Federal agencies and, consistent with  
18 applicable law, State and local governments (includ-  
19 ing law enforcement agencies), and private entities,  
20 including information provided by any contractor to  
21 a Federal agency regarding the security of the agen-  
22 cy information infrastructure;

23 **“(2)** any Federal agency in possession of law  
24 enforcement information, intelligence information,  
25 terrorism information, or any other information (in-  
26 cluding information relating to incidents provided

1 under subsections (a)(4) and (c) of section 246) rel-  
2 evant to the security of the Federal information in-  
3 frastructure, information infrastructure that is  
4 owned, operated, controlled, or licensed for use by,  
5 or on behalf of, the Department of Defense, a mili-  
6 tary department, or another element of the intel-  
7 ligence community, or national information infra-  
8 structure shall provide that information to the Di-  
9 rector in a timely manner; and

10 “(3) the Director, in coordination with the At-  
11 torney General, the Privacy and Civil Liberties Over-  
12 sight Board established under section 1061 of the  
13 National Security Intelligence Reform Act of 2004  
14 (42 U.S.C. 2000ee), the Director of National Intel-  
15 ligence, and the Archivist of the United States, shall  
16 establish guidelines to ensure that information is  
17 transferred, stored, and preserved in accordance  
18 with applicable law and in a manner that protects  
19 the privacy and civil liberties of United States per-  
20 sons.

21 “(b) OPERATIONAL EVALUATIONS.—

22 “(1) IN GENERAL.—The Director—

23 “(A) subject to paragraph (2), shall de-  
24 velop, maintain, and enhance capabilities to  
25 evaluate the security of the Federal information

1 infrastructure as described in section  
2 3554(a)(3) of title 44, United States Code, in-  
3 cluding the ability to conduct risk-based pene-  
4 tration testing and vulnerability assessments;

5 “(B) in carrying out subparagraph (A),  
6 may request technical assistance from the Di-  
7 rector of the Federal Bureau of Investigation,  
8 the Director of the National Security Agency,  
9 the head of any other Federal agency that may  
10 provide support, and any nongovernmental enti-  
11 ty contracting with the Department or another  
12 Federal agency; and

13 “(C) in consultation with the Attorney  
14 General and the Privacy and Civil Liberties  
15 Oversight Board established under section 1061  
16 of the National Security Intelligence Reform  
17 Act of 2004 (42 U.S.C. 2000ee), shall develop  
18 guidelines to ensure compliance with all applica-  
19 ble laws relating to the privacy of United States  
20 persons in carrying out the operational evalua-  
21 tions under subparagraph (A).

22 “(2) OPERATIONAL EVALUATIONS.—

23 “(A) IN GENERAL.—The Director may  
24 conduct risk-based operational evaluations of  
25 the agency information infrastructure of any

1 Federal agency, at a time determined by the  
2 Director, in consultation with the head of the  
3 Federal agency, using the capabilities developed  
4 under paragraph (1)(A).

5 “(B) ANNUAL EVALUATION REQUIRE-  
6 MENT.—If the Director conducts an operational  
7 evaluation under subparagraph (A) or an oper-  
8 ational evaluation at the request of a Federal  
9 agency to meet the requirements of section  
10 3554 of title 44, United States Code, the oper-  
11 ational evaluation shall satisfy the requirements  
12 of section 3554 for the Federal agency for the  
13 year of the evaluation, unless otherwise speci-  
14 fied by the Director.

15 “(c) CORRECTIVE MEASURES AND MITIGATION  
16 PLANS.—If the Director determines that a Federal agency  
17 is not in compliance with applicable policies, principles,  
18 standards, and guidelines applicable to the Federal infor-  
19 mation infrastructure—

20 “(1) the Director, in consultation with the Di-  
21 rector of the Office of Management and Budget,  
22 may direct the head of the Federal agency to—

23 “(A) take corrective measures to meet the  
24 policies, principles, standards, and guidelines;  
25 and

1           ~~“(B) develop a plan to remediate or miti-~~  
2           ~~gate any vulnerabilities addressed by the poli-~~  
3           ~~cies, principles, standards, and guidelines;~~

4           ~~“(2) within such time period as the Director~~  
5           ~~shall prescribe, the head of the Federal agency~~  
6           ~~shall—~~

7           ~~“(A) implement a corrective measure or~~  
8           ~~develop a mitigation plan in accordance with~~  
9           ~~paragraph (1); or~~

10           ~~“(B) submit to the Director, the Director~~  
11           ~~of the Office of Management and Budget, the~~  
12           ~~Inspector General for the Federal agency, and~~  
13           ~~the appropriate committees of Congress a re-~~  
14           ~~port indicating why the Federal agency has not~~  
15           ~~implemented the corrective measure or devel-~~  
16           ~~oped a mitigation plan; and~~

17           ~~“(3) the Director may direct the isolation of~~  
18           ~~any component of the agency information infrastruc-~~  
19           ~~ture, consistent with the contingency or continuity of~~  
20           ~~operation plans applicable to the agency information~~  
21           ~~infrastructure, until corrective measures are taken~~  
22           ~~or mitigation plans approved by the Director are put~~  
23           ~~in place, if—~~

1           “(A) the head of the Federal agency has  
2 failed to comply with the corrective measures  
3 prescribed under paragraph (1); and

4           “(B) the failure to comply presents a sig-  
5 nificant danger to the Federal information in-  
6 frastructure.

7 **“SEC. 246. INFORMATION SHARING.**

8           “(a) FEDERAL AGENCIES.—

9           “(1) INFORMATION SHARING PROGRAM.—Con-  
10 sistent with the responsibilities described in section  
11 242 and 244, the Director, in consultation with the  
12 other members of the Chief Information Officers  
13 Council established under section 3603 of title 44,  
14 United States Code, and the Federal Information  
15 Security Taskforce, shall establish a program for  
16 sharing information with and between the Center  
17 and other Federal agencies that includes processes  
18 and procedures, including standard operating proce-  
19 dures—

20           “(A) under which the Director regularly  
21 shares with each Federal agency—

22           “(i) analysis and reports on the com-  
23 posite security state of the Federal infor-  
24 mation infrastructure and information in-  
25 frastructure that is owned, operated, con-

1           trolled, or licensed for use by, or on behalf  
2           of, the Department of Defense, a military  
3           department, or another element of the in-  
4           telligence community, which shall include  
5           information relating to threats,  
6           vulnerabilities, incidents, or anomalous ac-  
7           tivities;

8           “(ii) any available analysis and re-  
9           ports regarding the security of the agency  
10          information infrastructure; and

11          “(iii) means and methods of pre-  
12          venting, responding to, mitigating, and re-  
13          mediating vulnerabilities; and

14          “(B) under which the Director may re-  
15          quest information from Federal agencies con-  
16          cerning the security of the Federal information  
17          infrastructure, information infrastructure that  
18          is owned, operated, controlled, or licensed for  
19          use by, or on behalf of, the Department of De-  
20          fense, a military department, or another ele-  
21          ment of the intelligence community, or the na-  
22          tional information infrastructure necessary to  
23          carry out the duties of the Director under this  
24          subtitle or any other provision of law.

1           “(2) CONTENTS.—The program established  
2 under this section shall include—

3           “(A) timeframes for the sharing of infor-  
4 mation under paragraph (1);

5           “(B) guidance on what information shall  
6 be shared, including information regarding inci-  
7 dents;

8           “(C) a tiered structure that provides guid-  
9 ance for the sharing of urgent information; and

10          “(D) processes and procedures under  
11 which the Director or the head of a Federal  
12 agency may report noncompliance with the pro-  
13 gram to the Director of Cyberspace Policy.

14          “(3) US-CERT.—The Director of the US-  
15 CERT shall ensure that the head of each Federal  
16 agency has continual access to data collected by the  
17 US-CERT regarding the agency information infra-  
18 structure of the Federal agency.

19          “(4) FEDERAL AGENCIES.—

20          “(A) IN GENERAL.—The head of a Federal  
21 agency shall comply with all processes and pro-  
22 cedures established under this subsection re-  
23 garding notification to the Director relating to  
24 incidents.

1           “(B) IMMEDIATE NOTIFICATION RE-  
2           QUIRED.—Unless otherwise directed by the  
3           President, any Federal agency with a national  
4           security system shall immediately notify the Di-  
5           rector regarding any incident affecting the risk-  
6           based security of the national security system.

7           “(b) STATE AND LOCAL GOVERNMENTS, PRIVATE  
8           SECTOR, AND INTERNATIONAL PARTNERS.—

9           “(1) IN GENERAL.—The Director, shall estab-  
10          lish processes and procedures, including standard  
11          operating procedures, to promote bidirectional infor-  
12          mation sharing with State and local governments,  
13          private entities, and international partners of the  
14          United States on—

15                 “(A) threats, vulnerabilities, incidents, and  
16                 anomalous activities affecting the national in-  
17                 formation infrastructure; and

18                 “(B) means and methods of preventing, re-  
19                 sponding to, and mitigating and remediating  
20                 vulnerabilities.

21           “(2) CONTENTS.—The processes and proce-  
22          dures established under paragraph (1) shall in-  
23          clude—

24                 “(A) means or methods of accessing classi-  
25                 fied or unclassified information, as appropriate,

1 that will provide situational awareness of the  
2 security of the Federal information infrastruc-  
3 ture and the national information infrastructure  
4 relating to threats, vulnerabilities, traffic,  
5 trends, incidents, and other anomalous activi-  
6 ties affecting the Federal information infra-  
7 structure or the national information infra-  
8 structure;

9 “(B) a mechanism, established in consulta-  
10 tion with the heads of the relevant sector-spe-  
11 cific agencies, sector coordinating councils, and  
12 information sharing and analysis centers, by  
13 which owners and operators of covered critical  
14 infrastructure shall report incidents in the in-  
15 formation infrastructure for covered critical in-  
16 frastructure, to the extent the incident might  
17 indicate an actual or potential cyber vulner-  
18 ability, or exploitation of that vulnerability; and

19 “(C) an evaluation of the need to provide  
20 security clearances to employees of State and  
21 local governments, private entities, and inter-  
22 national partners to carry out this subsection.

23 “(3) GUIDELINES.—The Director, in consulta-  
24 tion with the Attorney General and the Director of  
25 National Intelligence, shall develop guidelines to pro-

1 tect the privacy and civil liberties of United States  
 2 persons and intelligence sources and methods, while  
 3 carrying out this subsection.

4 “(e) INCIDENTS.—

5 “(1) NON-FEDERAL ENTITIES.—

6 “(A) IN GENERAL.—

7 “(i) MANDATORY REPORTING.—Sub-  
 8 ject to clause (i), the owner or operator of  
 9 covered critical infrastructure shall report  
 10 any incident affecting the information in-  
 11 frastructure of covered critical infrastruc-  
 12 ture to the extent the incident might indi-  
 13 cate an actual or potential cyber vulner-  
 14 ability, or exploitation of a cyber vulner-  
 15 ability, in accordance with the policies and  
 16 procedures for the mechanism established  
 17 under subsection (b)(2)(B) and guidelines  
 18 developed under subsection (b)(3).

19 “(ii) LIMITATION.—Clause (i) shall  
 20 not authorize the Director, the Center, the  
 21 Department, or any other Federal entity to  
 22 compel the disclosure of information relat-  
 23 ing to an incident or conduct surveillance  
 24 unless otherwise authorized under chapter  
 25 119, chapter 121, or chapter 206 of title

1 18, United States Code, the Foreign Intel-  
2 ligence Surveillance Act of 1978 (50  
3 U.S.C. 1801 et seq.); or any other provi-  
4 sion of law.

5 “(B) REPORTING PROCEDURES.—The Di-  
6 rector shall establish procedures that enable  
7 and encourage the owner or operator of na-  
8 tional information infrastructure to report to  
9 the Director regarding incidents affecting such  
10 information infrastructure.

11 “(2) INFORMATION PROTECTION.—Notwith-  
12 standing any other provision of law, information re-  
13 ported under paragraph (1) shall be protected from  
14 unauthorized disclosure, in accordance with section  
15 251.

16 “(d) ADDITIONAL RESPONSIBILITIES.—In accord-  
17 ance with section 251, the Director shall—

18 “(1) share data collected on the Federal infor-  
19 mation infrastructure with the National Science  
20 Foundation and other accredited research institu-  
21 tions for the sole purpose of cybersecurity research  
22 in a manner that protects privacy and civil liberties  
23 of United States persons and intelligence sources  
24 and methods;

1           “(2) establish a website to provide an oppor-  
2           tunity for the public to provide—

3                   “(A) input about the operations of the  
4           Center; and

5                   “(B) recommendations for improvements  
6           of the Center; and

7           “(3) in coordination with the Secretary of De-  
8           fense, the Director of National Intelligence, the Sec-  
9           retary of State, and the Attorney General, develop  
10          information sharing pilot programs with inter-  
11          national partners of the United States.

12 **“SEC. 247. PRIVATE SECTOR ASSISTANCE.**

13          “(a) IN GENERAL.—The Director, in consultation  
14 with the Director of the National Institute of Standards  
15 and Technology, the Director of the National Security  
16 Agency, the head of any relevant sector-specific agency,  
17 the National Cybersecurity Advisory Council, State and  
18 local governments, and any private entities the Director  
19 determines appropriate, shall establish a program to pro-  
20 mote, and provide technical assistance authorized under  
21 section 242(f)(1)(S) relating to the implementation of,  
22 best practices and related standards and guidelines for se-  
23 curing the national information infrastructure, including  
24 the costs and benefits associated with the implementation  
25 of the best practices and related standards and guidelines.

1       “(b) ANALYSIS AND IMPROVEMENT OF STANDARDS  
2 AND GUIDELINES.—For purposes of the program estab-  
3 lished under subsection (a), the Director shall—

4               “(1) regularly assess and evaluate cybersecurity  
5 standards and guidelines issued by private sector or-  
6 ganizations, recognized international and domestic  
7 standards setting organizations, and Federal agen-  
8 cies; and

9               “(2) in coordination with the National Institute  
10 of Standards and Technology, encourage the devel-  
11 opment of, and recommend changes to, the stand-  
12 ards and guidelines described in paragraph (1) for  
13 securing the national information infrastructure.

14       “(c) GUIDANCE AND TECHNICAL ASSISTANCE.—

15               “(1) IN GENERAL.—The Director shall promote  
16 best practices and related standards and guidelines  
17 to assist owners and operators of national informa-  
18 tion infrastructure in increasing the security of the  
19 national information infrastructure and protecting  
20 against and mitigating or remediating known  
21 vulnerabilities.

22               “(2) REQUIREMENT.—Technical assistance pro-  
23 vided under section 242(f)(1)(S) and best practices  
24 promoted under this section shall be prioritized  
25 based on risk.

1       “(d) CRITERIA.—In promoting best practices or rec-  
2 ommending changes to standards and guidelines under  
3 this section, the Director shall ensure that best practices,  
4 and related standards and guidelines—

5           “(1) address cybersecurity in a comprehensive,  
6 risk-based manner;

7           “(2) include consideration of the cost of imple-  
8 menting such best practices or of implementing rec-  
9 ommended changes to standards and guidelines;

10          “(3) increase the ability of the owners or opera-  
11 tors of national information infrastructure to protect  
12 against and mitigate or remediate known  
13 vulnerabilities;

14          “(4) are suitable, as appropriate, for implemen-  
15 tation by small business concerns;

16          “(5) as necessary and appropriate, are sector  
17 specific;

18          “(6) to the maximum extent possible, incor-  
19 porate standards and guidelines established by pri-  
20 vate sector organizations, recognized international  
21 and domestic standards setting organizations, and  
22 Federal agencies; and

23          “(7) provide sufficient flexibility to permit a  
24 range of security solutions.

1 **“SEC. 248. CYBER VULNERABILITIES TO COVERED CRIT-**  
2 **ICAL INFRASTRUCTURE.**

3 **“(a) IDENTIFICATION OF CYBER**  
4 **VULNERABILITIES.—**

5 **“(1) IN GENERAL.—**Based on the risk-based as-  
6 sssments conducted under section 242(f)(1)(T)(i),  
7 the Director, in coordination with the head of the  
8 sector-specific agency with responsibility for covered  
9 critical infrastructure and the head of any Federal  
10 agency that is not a sector-specific agency with re-  
11 sponsibilities for regulating the covered critical infra-  
12 structure, and in consultation with the National Cy-  
13 bersecurity Advisory Council and any private sector  
14 entity determined appropriate by the Director, shall,  
15 on a continuous and sector-by-sector basis, identify  
16 and evaluate the cyber vulnerabilities to covered crit-  
17 ical infrastructure.

18 **“(2) FACTORS TO BE CONSIDERED.—**In identi-  
19 fying and evaluating cyber vulnerabilities under  
20 paragraph (1), the Director shall consider—

21 **“(A)** the perceived threat, including a con-  
22 sideration of adversary capabilities and intent,  
23 preparedness, target attractiveness, and deter-  
24 rence capabilities;

25 **“(B)** the potential extent and likelihood of  
26 death, injury, or serious adverse effects to

1 human health and safety caused by a disruption  
2 of the reliable operation of covered critical in-  
3 frastructure;

4 “(C) the threat to or potential impact on  
5 national security caused by a disruption of the  
6 reliable operation of covered critical infrastruc-  
7 ture;

8 “(D) the extent to which the disruption of  
9 the reliable operation of covered critical infra-  
10 structure will disrupt the reliable operation of  
11 other covered critical infrastructure;

12 “(E) the potential for harm to the econ-  
13 omy that would result from a disruption of the  
14 reliable operation of covered critical infrastruc-  
15 ture; and

16 “(F) other risk-based security factors that  
17 the Director, in consultation with the head of  
18 the sector-specific agency with responsibility for  
19 the covered critical infrastructure and the head  
20 of any Federal agency that is not a sector-spe-  
21 cific agency with responsibilities for regulating  
22 the covered critical infrastructure; determine to  
23 be appropriate and necessary to protect public  
24 health and safety; critical infrastructure; or na-  
25 tional and economic security.

1           “(3) REPORT.—

2                   “(A) IN GENERAL.—Not later than 180  
3 days after the date of enactment of this sub-  
4 title, and annually thereafter, the Director, in  
5 coordination with the head of the sector-specific  
6 agency with responsibility for the covered crit-  
7 ical infrastructure and the head of any Federal  
8 agency that is not a sector-specific agency with  
9 responsibilities for regulating the covered crit-  
10 ical infrastructure, shall submit to the appro-  
11 priate committees of Congress a report on the  
12 findings of the identification and evaluation of  
13 cyber vulnerabilities under this subsection.  
14 Each report submitted under this paragraph  
15 shall be submitted in an unclassified form, but  
16 may include a classified annex.

17                   “(B) INPUT.—For purposes of the reports  
18 required under subparagraph (A), the Director  
19 shall create a process under which owners and  
20 operators of covered critical infrastructure may  
21 provide input on the findings of the reports.

22           “(b) RISK-BASED PERFORMANCE REQUIREMENTS.—

23                   “(1) IN GENERAL.—Not later than 270 days  
24 after the date of the enactment of this subtitle, in  
25 coordination with the heads of the sector-specific

1 agencies with responsibility for covered critical infra-  
2 structure and the head of any Federal agency that  
3 is not a sector-specific agency with responsibilities  
4 for regulating the covered critical infrastructure, and  
5 in consultation with the National Cybersecurity Ad-  
6 visory Council and any private sector entity deter-  
7 mined appropriate by the Director, the Director  
8 shall issue interim final regulations establishing risk-  
9 based security performance requirements to secure  
10 covered critical infrastructure against cyber  
11 vulnerabilities through the adoption of security  
12 measures that satisfy the security performance re-  
13 quirements identified by the Director.

14 “(2) PROCEDURES.—The regulations issued  
15 under this subsection shall—

16 “(A) include a process under which owners  
17 and operators of covered critical infrastructure  
18 are informed of identified cyber vulnerabilities  
19 and security performance requirements de-  
20 signed to remediate or mitigate the cyber  
21 vulnerabilities, in combination with best prac-  
22 tices recommended under section 247;

23 “(B) establish a process for owners and  
24 operators of covered critical infrastructure to  
25 select security measures, including any best

1 practices recommended under section 247, that,  
 2 in combination, satisfy the security performance  
 3 requirements established by the Director under  
 4 this subsection;

5 “(C) establish a process for owners and op-  
 6 erators of covered critical infrastructure to de-  
 7 velop response plans for a national cyber emer-  
 8 gency declared under section 249; and

9 “(D) establish a process by which the Di-  
 10 rector—

11 “(i) is notified of the security meas-  
 12 ures selected by the owner or operator of  
 13 covered critical infrastructure under sub-  
 14 paragraph (B); and

15 “(ii) may determine whether the pro-  
 16 posed security measures satisfy the secu-  
 17 rity performance requirements established  
 18 by the Director under this subsection.

19 “(3) INTERNATIONAL COOPERATION ON SECUR-  
 20 ING COVERED CRITICAL INFRASTRUCTURE.—

21 “(A) IN GENERAL.—The Director, in co-  
 22 ordination with the head of the sector-specific  
 23 agency with responsibility for covered critical  
 24 infrastructure and the head of any Federal  
 25 agency that is not a sector-specific agency with

1 responsibilities for regulating the covered crit-  
2 ical infrastructure, shall—

3 “(i) consistent with the protection of  
4 intelligence sources and methods and other  
5 sensitive matters, inform the owner or op-  
6 erator of covered critical infrastructure  
7 that is located outside the United States  
8 and the government of the country in  
9 which the covered critical infrastructure is  
10 located of any cyber vulnerabilities to the  
11 covered critical infrastructure; and

12 “(ii) coordinate with the government  
13 of the country in which the covered critical  
14 infrastructure is located and, as appro-  
15 priate, the owner or operator of the cov-  
16 ered critical infrastructure, regarding the  
17 implementation of security measures or  
18 other measures to the covered critical in-  
19 frastructure to mitigate or remediate cyber  
20 vulnerabilities.

21 “(B) INTERNATIONAL AGREEMENTS.—The  
22 Director shall carry out the this paragraph in  
23 a manner consistent with applicable inter-  
24 national agreements.

1           ~~“(4) RISK-BASED SECURITY PERFORMANCE RE-~~  
2           ~~QUIREMENTS.—~~

3           ~~“(A) IN GENERAL.—The security perform-~~  
4           ~~ance requirements established by the Director~~  
5           ~~under this subsection shall be—~~

6                   ~~“(i) based on the factors listed in sub-~~  
7                   ~~section (a)(2); and~~

8                   ~~“(ii) designed to remediate or mitigate~~  
9                   ~~identified cyber vulnerabilities and any as-~~  
10                  ~~sociated consequences of an exploitation~~  
11                  ~~based on such vulnerabilities.~~

12           ~~“(B) CONSULTATION.—In establishing se-~~  
13           ~~curity performance requirements under this~~  
14           ~~subsection, the Director shall, to the maximum~~  
15           ~~extent practicable, consult with—~~

16                   ~~“(i) the Director of the National Se-~~  
17                   ~~curity Agency;~~

18                   ~~“(ii) the Director of the National In-~~  
19                   ~~stitute of Standards and Technology;~~

20                   ~~“(iii) the National Cybersecurity Advi-~~  
21                   ~~sory Council;~~

22                   ~~“(iv) the heads of sector-specific agen-~~  
23                   ~~cies; and~~

24                   ~~“(v) the heads of Federal agencies~~  
25                   ~~that are not a sector-specific agency with~~

1 responsibilities for regulating the covered  
2 critical infrastructure.

3 ~~“(C) ALTERNATIVE MEASURES.—~~

4 ~~“(i) IN GENERAL.—~~The owners and  
5 operators of covered critical infrastructure  
6 shall have flexibility to implement any se-  
7 curity measure, or combination thereof, to  
8 satisfy the security performance require-  
9 ments described in subparagraph (A) and  
10 the Director may not disapprove under this  
11 section any proposed security measures, or  
12 combination thereof, based on the presence  
13 or absence of any particular security meas-  
14 ure if the proposed security measures, or  
15 combination thereof, satisfy the security  
16 performance requirements established by  
17 the Director under this section.

18 ~~“(ii) RECOMMENDED SECURITY MEAS-~~  
19 ~~URES.—~~The Director may recommend to  
20 an owner and operator of covered critical  
21 infrastructure a specific security measure,  
22 or combination thereof, that will satisfy the  
23 security performance requirements estab-  
24 lished by the Director. The absence of the  
25 recommended security measures, or com-

1            bination thereof, may not serve as the  
2            basis for a disapproval of the security  
3            measure, or combination thereof, proposed  
4            by the owner or operator of covered critical  
5            infrastructure if the proposed security  
6            measure, or combination thereof, otherwise  
7            satisfies the security performance require-  
8            ments established by the Director under  
9            this section.

10 **“SEC. 249. NATIONAL CYBER EMERGENCIES.**

11            “(a) DECLARATION.—

12            “(1) IN GENERAL.—The President may issue a  
13            declaration of a national cyber emergency to covered  
14            critical infrastructure. Any declaration under this  
15            section shall specify the covered critical infrastruc-  
16            ture subject to the national cyber emergency.

17            “(2) NOTIFICATION.—Upon issuing a declara-  
18            tion under paragraph (1), the President shall, con-  
19            sistent with the protection of intelligence sources  
20            and methods, notify the owners and operators of the  
21            specified covered critical infrastructure of the nature  
22            of the national cyber emergency.

23            “(3) AUTHORITIES.—If the President issues a  
24            declaration under paragraph (1), the Director  
25            shall—

1           “(A) immediately direct the owners and  
2 operators of covered critical infrastructure sub-  
3 ject to the declaration under paragraph (1) to  
4 implement response plans required under sec-  
5 tion 248(b)(2)(C);

6           “(B) develop and coordinate emergency  
7 measures or actions necessary to preserve the  
8 reliable operation, and mitigate or remediate  
9 the consequences of the potential disruption, of  
10 covered critical infrastructure;

11           “(C) ensure that emergency measures or  
12 actions directed under this section represent the  
13 least disruptive means feasible to the operations  
14 of the covered critical infrastructure;

15           “(D) subject to subsection (f), direct ac-  
16 tions by other Federal agencies to respond to  
17 the national cyber emergency;

18           “(E) coordinate with officials of State and  
19 local governments, international partners of the  
20 United States, and private owners and opera-  
21 tors of covered critical infrastructure specified  
22 in the declaration to respond to the national  
23 cyber emergency;

1           “(F) initiate a process under section 248  
2           to address the cyber vulnerability that may be  
3           exploited by the national cyber emergency; and

4           “(G) provide voluntary technical assist-  
5           ance, if requested, under section 242(f)(1)(S).

6           “(4) REIMBURSEMENT.—A Federal agency  
7           shall be reimbursed for expenditures under this sec-  
8           tion from funds appropriated for the purposes of  
9           this section. Any funds received by a Federal agency  
10          as reimbursement for services or supplies furnished  
11          under the authority of this section shall be deposited  
12          to the credit of the appropriation or appropriations  
13          available on the date of the deposit for the services  
14          or supplies.

15          “(5) CONSULTATION.—In carrying out this sec-  
16          tion, the Director shall consult with the Secretary,  
17          the Secretary of Defense, the Director of the Na-  
18          tional Security Agency, the Director of the National  
19          Institute of Standards and Technology, and any  
20          other official, as directed by the President.

21          “(6) PRIVACY.—In carrying out this section,  
22          the Director shall ensure that the privacy and civil  
23          liberties of United States persons are protected.

24          “(b) DISCONTINUANCE OF EMERGENCY MEAS-  
25          URES.—

1           “(1) IN GENERAL.—Any emergency measure or  
2           action developed under this section shall cease to  
3           have effect not later than 30 days after the date on  
4           which the President issued the declaration of a na-  
5           tional cyber emergency, unless—

6                   “(A) the Director affirms in writing that  
7                   the emergency measure or action remains nec-  
8                   essary to address the identified national cyber  
9                   emergency; and

10                   “(B) the President issues a written order  
11                   or directive reaffirming the national cyber  
12                   emergency, the continuing nature of the na-  
13                   tional cyber emergency, or the need to continue  
14                   the adoption of the emergency measure or ac-  
15                   tion.

16           “(2) EXTENSIONS.—An emergency measure or  
17           action extended in accordance with paragraph (1)  
18           may—

19                   “(A) remain in effect for not more than 30  
20                   days after the date on which the emergency  
21                   measure or action was to cease to have effect;  
22                   and

23                   “(B) be extended for additional 30-day pe-  
24                   riods, if the requirements of paragraph (1) and  
25                   subsection (d) are met.

1 “(c) COMPLIANCE WITH EMERGENCY MEASURES.—

2 “(1) IN GENERAL.—Subject to paragraph (2),  
3 the owner or operator of covered critical infrastruc-  
4 ture shall immediately comply with any emergency  
5 measure or action developed by the Director under  
6 this section during the pendency of any declaration  
7 by the President under subsection (a)(1) or an ex-  
8 tension under subsection (b)(2).

9 “(2) ALTERNATIVE MEASURES.—If the Director  
10 determines that a proposed security measure, or any  
11 combination thereof, submitted by the owner or op-  
12 erator of covered critical infrastructure in accord-  
13 ance with the process established under section  
14 248(b)(2) addresses the cyber vulnerability associ-  
15 ated with the national cyber emergency that is the  
16 subject of the declaration under this section, the  
17 owner or operator may comply with paragraph (1) of  
18 this subsection by implementing the proposed secu-  
19 rity measure, or combination thereof, approved by  
20 the Director under the process established under  
21 section 248. Before submission of a proposed secu-  
22 rity measure, or combination thereof, and during the  
23 pendency of any review by the Director under the  
24 process established under section 248, the owner or  
25 operator of covered critical infrastructure shall re-

1 main in compliance with any emergency measure or  
2 action developed by the Director under this section  
3 during the pendency of any declaration by the Presi-  
4 dent under subsection (a)(1) or an extension under  
5 subsection (b)(2), until such time as the Director  
6 has approved an alternative proposed security meas-  
7 ure, or combination thereof, under this paragraph.

8 “(3) INTERNATIONAL COOPERATION ON NA-  
9 TIONAL CYBER EMERGENCIES.—

10 “(A) IN GENERAL.—The Director, in co-  
11 ordination with the head of the sector-specific  
12 agency with responsibility for covered critical  
13 infrastructure and the head of any Federal  
14 agency that is not a sector-specific agency with  
15 responsibilities for regulating the covered crit-  
16 ical infrastructure, shall—

17 “(i) consistent with the protection of  
18 intelligence sources and methods and other  
19 sensitive matters, inform the owner or op-  
20 erator of covered critical infrastructure  
21 that is located outside of the United States  
22 and the government of the country in  
23 which the covered critical infrastructure is  
24 located of any national cyber emergency

1 affecting the covered critical infrastruc-  
2 ture; and

3 “(ii) coordinate with the government  
4 of the country in which the covered critical  
5 infrastructure is located and, as appro-  
6 priate, the owner or operator of the cov-  
7 ered critical infrastructure, regarding the  
8 implementation of emergency measures or  
9 actions necessary to preserve the reliable  
10 operation, and mitigate or remediate the  
11 consequences of the potential disruption, of  
12 the covered critical infrastructure.

13 “(B) INTERNATIONAL AGREEMENTS.—The  
14 Director shall carry out this paragraph in a  
15 manner consistent with applicable international  
16 agreements.

17 “(4) LIMITATION ON COMPLIANCE AUTHOR-  
18 ITY.—The authority to direct compliance with an  
19 emergency measure or action under this section shall  
20 not authorize the Director, the Center, the Depart-  
21 ment, or any other Federal entity to compel the dis-  
22 closure of information or conduct surveillance unless  
23 otherwise authorized under chapter 119, chapter  
24 121, or chapter 206 of title 18, United States Code,  
25 the Foreign Intelligence Surveillance Act of 1978

1 (50 U.S.C. 1801 et seq.), or any other provision of  
2 law.

3 “(d) REPORTING.—

4 “(1) IN GENERAL.—Except as provided in para-  
5 graph (2), the President shall ensure that any dec-  
6 laration under subsection (a)(1) or any extension  
7 under subsection (b)(2) is reported to the appro-  
8 priate committees of Congress before the Director  
9 mandates any emergency measure or actions under  
10 subsection (a)(3).

11 “(2) EXCEPTION.—If notice cannot be given  
12 under paragraph (1) before mandating any emer-  
13 gency measure or actions under subsection (a)(3),  
14 the President shall provide the report required under  
15 paragraph (1) as soon as possible, along with a  
16 statement of the reasons for not providing notice in  
17 accordance with paragraph (1).

18 “(3) CONTENTS.—Each report under this sub-  
19 section shall describe—

20 “(A) the nature of the national cyber  
21 emergency;

22 “(B) the reasons that risk-based security  
23 requirements under section 248 are not suffi-  
24 cient to address the national cyber emergency;  
25 and

1           “(C) the actions necessary to preserve the  
2           reliable operation and mitigate the con-  
3           sequences of the potential disruption of covered  
4           critical infrastructure.

5           “(e) STATUTORY DEFENSES AND CIVIL LIABILITY  
6           LIMITATIONS FOR COMPLIANCE WITH EMERGENCY  
7           MEASURES.—

8           “(1) DEFINITIONS.—In this subsection—

9           “(A) the term ‘covered civil action’—

10           “(i) means a civil action filed in a  
11           Federal or State court against a covered  
12           entity; and

13           “(ii) does not include an action  
14           brought under section 2520 or 2707 of  
15           title 18, United States Code, or section  
16           110 or 308 of the Foreign Intelligence  
17           Surveillance Act of 1978 (50 U.S.C. 1810  
18           and 1828);

19           “(B) the term ‘covered entity’ means any  
20           entity that owns or operates covered critical in-  
21           frastructure, including any owner, operator, of-  
22           ficer, employee, agent, landlord, custodian, or  
23           other person acting for or on behalf of that en-  
24           tity with respect to the covered critical infra-  
25           structure; and

1           “(C) the term ‘noneconomic damages’  
2 means damages for losses for physical and emo-  
3 tional pain, suffering, inconvenience, physical  
4 impairment, mental anguish, disfigurement, loss  
5 of enjoyment of life, loss of society and compan-  
6 ionship, loss of consortium, hedonic damages,  
7 injury to reputation, and any other nonpecu-  
8 niary losses.

9           “(2) APPLICATION OF LIMITATIONS ON CIVIL  
10 LIABILITY.—The limitations on civil liability under  
11 paragraph (3) apply if—

12           “(A) the President has issued a declaration  
13 of national cyber emergency under subsection  
14 (a)(1);

15           “(B) the Director has—

16           “(i) issued emergency measures or ac-  
17 tions for which compliance is required  
18 under subsection (e)(1); or

19           “(ii) approved security measures  
20 under subsection (e)(2);

21           “(C) the covered entity is in compliance  
22 with—

23           “(i) the emergency measures or ac-  
24 tions required under subsection (e)(1); or

1           “(ii) security measures which the Di-  
2           rector has approved under subsection  
3           (e)(2); and

4           “(D)(i) the Director certifies to the court  
5           in which the covered civil action is pending that  
6           the actions taken by the covered entity during  
7           the period covered by the declaration under  
8           subsection (a)(1) were consistent with—

9           “(I) emergency measures or actions  
10          for which compliance is required under  
11          subsection (e)(1); or

12          “(II) security measures which the Di-  
13          rector has approved under subsection  
14          (e)(2); or

15          “(ii) notwithstanding the lack of a certifi-  
16          cation, the covered entity demonstrates by a  
17          preponderance of the evidence that the actions  
18          taken during the period covered by the declara-  
19          tion under subsection (a)(1) are consistent with  
20          the implementation of—

21          “(I) emergency measures or actions  
22          for which compliance is required under  
23          subsection (e)(1); or

1                   ~~“(H) security measures which the Di-~~  
2                   ~~rector has approved under subsection~~  
3                   ~~(e)(2).~~

4                   ~~“(3) LIMITATIONS ON CIVIL LIABILITY.—In any~~  
5                   ~~covered civil action that is related to any incident as-~~  
6                   ~~sociated with a cyber vulnerability covered by a dec-~~  
7                   ~~laration of a national cyber emergency and for which~~  
8                   ~~Director has issued emergency measures or actions~~  
9                   ~~for which compliance is required under subsection~~  
10                  ~~(e)(1) or for which the Director has approved secu-~~  
11                  ~~rity measures under subsection (e)(2), or that is the~~  
12                  ~~direct consequence of actions taken in good faith for~~  
13                  ~~the purpose of implementing security measures or~~  
14                  ~~actions which the Director has approved under sub-~~  
15                  ~~section (e)(2)—~~

16                  ~~“(A) the covered entity shall not be liable~~  
17                  ~~for any punitive damages intended to punish or~~  
18                  ~~deter, exemplary damages, or other damages~~  
19                  ~~not intended to compensate a plaintiff for ac-~~  
20                  ~~tual losses; and~~

21                  ~~“(B) noneconomic damages may be award-~~  
22                  ~~ed against a defendant only in an amount di-~~  
23                  ~~rectly proportional to the percentage of respon-~~  
24                  ~~sibility of such defendant for the harm to the~~  
25                  ~~plaintiff, and no plaintiff may recover non-~~

1 economic damages unless the plaintiff suffered  
2 physical harm.

3 ~~“(4) CIVIL ACTIONS ARISING OUT OF IMPLE-~~  
4 ~~MENTATION OF EMERGENCY MEASURES OR AC-~~  
5 ~~TIONS.—A covered civil action may not be main-~~  
6 ~~tained against a covered entity that is the direct~~  
7 ~~consequence of actions taken in good faith for the~~  
8 ~~purpose of implementing specific emergency meas-~~  
9 ~~ures or actions for which compliance is required~~  
10 ~~under subsection (e)(1), if—~~

11 ~~“(A) the President has issued a declaration~~  
12 ~~of national cyber emergency under subsection~~  
13 ~~(a)(1) and the action was taken during the pe-~~  
14 ~~riod covered by that declaration;~~

15 ~~“(B) the Director has issued emergency~~  
16 ~~measures or actions for which compliance is re-~~  
17 ~~quired under subsection (e)(1);~~

18 ~~“(C) the covered entity is in compliance~~  
19 ~~with the emergency measures required under~~  
20 ~~subsection (e)(1); and~~

21 ~~“(D)(i) the Director certifies to the court~~  
22 ~~in which the covered civil action is pending that~~  
23 ~~the actions taken by the entity during the pe-~~  
24 ~~riod covered by the declaration under subsection~~  
25 ~~(a)(1) were consistent with the implementation~~

1 of emergency measures or actions for which  
 2 compliance is required under subsection (e)(1);  
 3 or

4 “(ii) notwithstanding the lack of a certifi-  
 5 cation, the entity demonstrates by a preponder-  
 6 ance of the evidence that the actions taken dur-  
 7 ing the period covered by the declaration under  
 8 subsection (a)(1) are consistent with the imple-  
 9 mentation of emergency measures or actions for  
 10 which compliance is required under subsection  
 11 (e)(1).

12 “(5) CERTAIN ACTIONS NOT SUBJECT TO LIM-  
 13 TATIONS ON LIABILITY.—

14 “(A) ADDITIONAL OR INTERVENING  
 15 ACTS.—Paragraphs (2) through (4) shall not  
 16 apply to a civil action relating to any additional  
 17 or intervening acts or omissions by any covered  
 18 entity.

19 “(B) SERIOUS OR SUBSTANTIAL DAM-  
 20 AGE.—Paragraph (4) shall not apply to any  
 21 civil action brought by an individual—

22 “(i) whose recovery is otherwise pre-  
 23 cluded by application of paragraph (4);  
 24 and

25 “(ii) who has suffered—

1                   “(I) serious physical injury or  
2                   death; or

3                   “(II) substantial damage or de-  
4                   struction to his primary residence.

5                   “(C) RULE OF CONSTRUCTION.—Recovery  
6                   available under subparagraph (B) shall be lim-  
7                   ited to those damages available under subpara-  
8                   graphs (A) and (B) of paragraph (3), except  
9                   that neither reasonable and necessary medical  
10                  benefits nor lifetime total benefits for lost em-  
11                  ployment income due to permanent and total  
12                  disability shall be limited herein.

13                  “(D) INDEMNIFICATION.—In any civil ac-  
14                  tion brought under subparagraph (B), the  
15                  United States shall defend and indemnify any  
16                  covered entity. Any covered entity defended and  
17                  indemnified under this subparagraph shall fully  
18                  cooperate with the United States in the defense  
19                  by the United States in any proceeding and  
20                  shall be reimbursed the reasonable costs associ-  
21                  ated with such cooperation.

22                  “(f) RULE OF CONSTRUCTION.—Nothing in this sec-  
23                  tion shall be construed to—

24                         “(1) alter or supersede the authority of the Sec-  
25                         retary of Defense, the Attorney General, or the Di-

1 rector of National Intelligence in responding to a na-  
2 tional cyber emergency; or

3 “(2) limit the authority of the Director under  
4 section 248, after a declaration issued under this  
5 section expires.

6 **“SEC. 250. ENFORCEMENT.**

7 “(a) ANNUAL CERTIFICATION OF COMPLIANCE.—

8 “(1) IN GENERAL.—Not later than 6 months  
9 after the date on which the Director promulgates  
10 regulations under section 248(b), and every year  
11 thereafter, each owner or operator of covered critical  
12 infrastructure shall certify in writing to the Director  
13 whether the owner or operator has developed and  
14 implemented, or is implementing, security measures  
15 approved by the Director under section 248 and any  
16 applicable emergency measures or actions required  
17 under section 249 for any cyber vulnerabilities and  
18 national cyber emergencies.

19 “(2) FAILURE TO COMPLY.—If an owner or op-  
20 erator of covered critical infrastructure fails to sub-  
21 mit a certification in accordance with paragraph (1),  
22 or if the certification indicates the owner or operator  
23 is not in compliance, the Director may issue an  
24 order requiring the owner or operator to submit pro-  
25 posed security measures under section 248 or com-

1 ply with specific emergency measures or actions  
2 under section 249.

3 ~~“(b) RISK-BASED EVALUATIONS.—~~

4 ~~“(1) IN GENERAL.—Consistent with the factors~~  
5 ~~described in paragraph (3), the Director may per-~~  
6 ~~form an evaluation of the information infrastructure~~  
7 ~~of any specific system or asset constituting covered~~  
8 ~~critical infrastructure to assess the validity of a cer-~~  
9 ~~tification of compliance submitted under subsection~~  
10 ~~(a)(1).~~

11 ~~“(2) DOCUMENT REVIEW AND INSPECTION.—~~

12 ~~An evaluation performed under paragraph (1) may~~  
13 ~~include—~~

14 ~~“(A) a review of all documentation sub-~~  
15 ~~mitted to justify an annual certification of com-~~  
16 ~~pliance submitted under subsection (a)(1); and~~

17 ~~“(B) a physical or electronic inspection of~~  
18 ~~relevant information infrastructure to which the~~  
19 ~~security measures required under section 248 or~~  
20 ~~the emergency measures or actions required~~  
21 ~~under section 249 apply.~~

22 ~~“(3) EVALUATION SELECTION FACTORS.—In~~

23 ~~determining whether sufficient risk exists to justify~~  
24 ~~an evaluation under this subsection, the Director~~  
25 ~~shall consider—~~

1           “(A) the specific cyber vulnerabilities af-  
2           fecting or potentially affecting the information  
3           infrastructure of the specific system or asset  
4           constituting covered critical infrastructure;

5           “(B) any reliable intelligence or other in-  
6           formation indicating a cyber vulnerability or  
7           credible national cyber emergency to the infor-  
8           mation infrastructure of the specific system or  
9           asset constituting covered critical infrastruc-  
10          ture;

11          “(C) actual knowledge or reasonable sus-  
12          picion that the certification of compliance sub-  
13          mitted by a specific owner or operator of cov-  
14          ered critical infrastructure is false or otherwise  
15          inaccurate;

16          “(D) a request by a specific owner or oper-  
17          ator of covered critical infrastructure for such  
18          an evaluation; and

19          “(E) such other risk-based factors as iden-  
20          tified by the Director.

21          “(4) ~~SECTOR-SPECIFIC AGENCIES.~~—To carry  
22          out the risk-based evaluation authorized under this  
23          subsection, the Director may use the resources of a  
24          sector-specific agency with responsibility for the cov-  
25          ered critical infrastructure or any Federal agency

1 that is not a sector-specific agency with responsibil-  
2 ities for regulating the covered critical infrastructure  
3 with the concurrence of the head of the agency.

4 “(5) INFORMATION PROTECTION.—Information  
5 provided to the Director during the course of an  
6 evaluation under this subsection shall be protected  
7 from disclosure in accordance with section 251.

8 “(c) CIVIL PENALTIES.—

9 “(1) IN GENERAL.—Any person who violates  
10 section 248 or 249 shall be liable for a civil penalty.

11 “(2) NO PRIVATE RIGHT OF ACTION.—Nothing  
12 in this section confers upon any person, except the  
13 Director, a right of action against an owner or oper-  
14 ator of covered critical infrastructure to enforce any  
15 provision of this subtitle.

16 “(d) LIMITATION ON CIVIL LIABILITY.—

17 “(1) DEFINITION.—In this subsection—

18 “(A) the term ‘covered civil action’—

19 “(i) means a civil action filed in a  
20 Federal or State court against a covered  
21 entity; and

22 “(ii) does not include an action  
23 brought under section 2520 or 2707 of  
24 title 18, United States Code, or section  
25 110 or 308 of the Foreign Intelligence

1 Surveillance Act of 1978 (50 U.S.C. 1810  
2 and 1828);

3 “(B) the term ‘covered entity’ means any  
4 entity that owns or operates covered critical in-  
5 frastructure, including any owner, operator, of-  
6 ficer, employee, agent, landlord, custodian, or  
7 other person acting for or on behalf of that en-  
8 tity with respect to the covered critical infra-  
9 structure; and

10 “(C) the term ‘noneconomic damages’  
11 means damages for losses for physical and emo-  
12 tional pain, suffering, inconvenience, physical  
13 impairment, mental anguish, disfigurement, loss  
14 of enjoyment of life, loss of society and compan-  
15 ionship, loss of consortium, hedonic damages,  
16 injury to reputation, and any other nonpecu-  
17 niary losses.

18 “(2) LIMITATIONS ON CIVIL LIABILITY.—If a  
19 covered entity experiences an incident related to a  
20 cyber vulnerability identified under section 248(a),  
21 in any covered civil action for damages directly  
22 caused by the incident related to that cyber vulner-  
23 ability—

24 “(A) the covered entity shall not be liable  
25 for any punitive damages intended to punish or

1           deter, exemplary damages, or other damages  
2           not intended to compensate a plaintiff for ac-  
3           tual losses; and

4           “(B) noneconomic damages may be award-  
5           ed against a defendant only in an amount di-  
6           rectly proportional to the percentage of respon-  
7           sibility of such defendant for the harm to the  
8           plaintiff, and no plaintiff may recover non-  
9           economic damages unless the plaintiff suffered  
10          physical harm.

11          “(3) APPLICATION.—This subsection shall  
12          apply to claims made by any individual or non-  
13          governmental entity, including claims made by a  
14          State or local government agency on behalf of such  
15          individuals or nongovernmental entities, against a  
16          covered entity—

17               “(A) whose proposed security measures, or  
18               combination thereof, satisfy the security per-  
19               formance requirements established under sub-  
20               section 248(b) and have been approved by the  
21               Director;

22               “(B) that has been evaluated under sub-  
23               section (b) and has been found by the Director  
24               to have implemented the proposed security  
25               measures approved under section 248; and

1           “(C) that is in actual compliance with the  
2           approved security measures at the time of the  
3           incident related to that cyber vulnerability.

4           “(4) LIMITATION.—This subsection shall only  
5           apply to harm directly caused by the incident related  
6           to the cyber vulnerability and shall not apply to  
7           damages caused by any additional or intervening  
8           acts or omissions by the covered entity.

9           “(5) RULE OF CONSTRUCTION.—Except as pro-  
10          vided under paragraph (3), nothing in this sub-  
11          section shall be construed to abrogate or limit any  
12          right, remedy, or authority that the Federal Govern-  
13          ment or any State or local government, or any entity  
14          or agency thereof, may possess under any law, or  
15          that any individual is authorized by law to bring on  
16          behalf of the government.

17          “(e) REPORT TO CONGRESS.—The Director shall  
18          submit an annual report to the appropriate committees of  
19          Congress on the implementation and enforcement of the  
20          risk-based performance requirements of covered critical in-  
21          frastructure under subsection 248(b) and this section in-  
22          cluding—

23                 “(1) the level of compliance of covered critical  
24                 infrastructure with the risk-based security perform-  
25                 ance requirements issued under section 248(b);

1           “(2) how frequently the evaluation authority  
2           under subsection (b) was utilized and a summary of  
3           the aggregate results of the evaluations; and

4           “(3) any civil penalties imposed on covered crit-  
5           ical infrastructure.

6   **“SEC. 251. PROTECTION OF INFORMATION.**

7           “(a) DEFINITION.—In this section, the term ‘covered  
8           information’—

9           “(1) means—

10           “(A) any information required to be sub-  
11           mitted under sections 246, 248, and 249 to the  
12           Center by the owners and operators of covered  
13           critical infrastructure; and

14           “(B) any information submitted to the  
15           Center under the processes and procedures es-  
16           tablished under section 246 by State and local  
17           governments, private entities, and international  
18           partners of the United States regarding threats,  
19           vulnerabilities, and incidents affecting—

20           “(i) the Federal information infra-  
21           structure;

22           “(ii) information infrastructure that is  
23           owned, operated, controlled, or licensed for  
24           use by, or on behalf of, the Department of

1           Defense, a military department, or another  
2           element of the intelligence community; or

3           ~~“(iii) the national information infra-~~  
4           ~~structure; and~~

5           ~~“(2) shall not include any information described~~  
6           ~~under paragraph (1), if that information is sub-~~  
7           ~~mitted to—~~

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

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

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

14          ~~“(b) VOLUNTARILY SHARED CRITICAL INFRASTRUC-~~  
15          ~~TURE INFORMATION.—Covered information submitted in~~  
16          ~~accordance with this section shall be treated as voluntarily~~  
17          ~~shared critical infrastructure information under section~~  
18          ~~214, except that the requirement of section 214 that the~~  
19          ~~information be voluntarily submitted, including the re-~~  
20          ~~quirement for an express statement, shall not be required~~  
21          ~~for submissions of covered information.~~

22          ~~“(c) GUIDELINES.—~~

23          ~~“(1) IN GENERAL.—Subject to paragraph (2),~~  
24          ~~the Director shall develop and issue guidelines, in~~  
25          ~~consultation with the Secretary, Attorney General,~~

1 and the National Cybersecurity Advisory Council, as  
2 necessary to implement this section.

3 ~~“(2) REQUIREMENTS.—The guidelines devel-~~  
4 ~~oped under this section shall—~~

5 ~~“(A) consistent with section 214(e)(2)(D)~~  
6 ~~and (g) and the guidelines developed under sec-~~  
7 ~~tion 246(b)(3), include provisions for informa-~~  
8 ~~tion sharing among Federal, State, and local~~  
9 ~~and officials, private entities, or international~~  
10 ~~partners of the United States necessary to~~  
11 ~~carry out the authorities and responsibilities of~~  
12 ~~the Director;~~

13 ~~“(B) be consistent, to the maximum extent~~  
14 ~~possible, with policy guidance and implementa-~~  
15 ~~tion standards developed by the National Ar-~~  
16 ~~chives and Records Administration for con-~~  
17 ~~trolled unclassified information, including with~~  
18 ~~respect to marking, safeguarding, dissemination~~  
19 ~~and dispute resolution; and~~

20 ~~“(C) describe, with as much detail as pos-~~  
21 ~~sible, the categories and type of information en-~~  
22 ~~tities should voluntarily submit under sub-~~  
23 ~~sections (b) and (e)(1)(B) of section 246.~~

24 ~~“(d) PROCESS FOR REPORTING SECURITY PROB-~~  
25 ~~LEMS.—~~

1           “(1) ESTABLISHMENT OF PROCESS.—The Di-  
2           rector shall establish through regulation, and provide  
3           information to the public regarding, a process by  
4           which any person may submit a report to the Sec-  
5           retary regarding cybersecurity threats,  
6           vulnerabilities, and incidents affecting—

7                   “(A) the Federal information infrastruc-  
8                   ture;

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

14                  “(C) national information infrastructure.

15           “(2) ACKNOWLEDGMENT OF RECEIPT.—If a re-  
16           port submitted under paragraph (1) identifies the  
17           person making the report, the Director shall respond  
18           promptly to such person and acknowledge receipt of  
19           the report.

20           “(3) STEPS TO ADDRESS PROBLEM.—The Di-  
21           rector shall review and consider the information pro-  
22           vided in any report submitted under paragraph (1)  
23           and, at the sole, unreviewable discretion of the Di-  
24           rector, determine what, if any, steps are necessary

1 or appropriate to address any problems or defi-  
2 ciencies identified.

3 “(4) DISCLOSURE OF IDENTITY.—

4 “(A) IN GENERAL.—Except as provided in  
5 subparagraph (B), or with the written consent  
6 of the person, the Secretary may not disclose  
7 the identity of a person who has provided infor-  
8 mation described in paragraph (1).

9 “(B) REFERRAL TO THE ATTORNEY GEN-  
10 ERAL.—The Secretary shall disclose to the At-  
11 torney General the identity of a person de-  
12 scribed under subparagraph (A) if the matter is  
13 referred to the Attorney General for enforce-  
14 ment. The Director shall provide reasonable ad-  
15 vance notice to the affected person if disclosure  
16 of that person’s identity is to occur, unless such  
17 notice would risk compromising a criminal or  
18 civil enforcement investigation or proceeding.

19 “(c) RULES OF CONSTRUCTION.—Nothing in this  
20 section shall be construed to—

21 “(1) limit or otherwise affect the right, ability,  
22 duty, or obligation of any entity to use or disclose  
23 any information of that entity, including in the con-  
24 duct of any judicial or other proceeding;

1           “(2) prevent the classification of information  
2 submitted under this section if that information  
3 meets the standards for classification under Execu-  
4 tive Order 12958 or any successor of that order;

5           “(3) limit the right of an individual to make  
6 any disclosure—

7                   “(A) protected or authorized under section  
8 2302(b)(8) or 7211 of title 5, United States  
9 Code;

10                   “(B) to an appropriate official of informa-  
11 tion that the individual reasonably believes evi-  
12 dences a violation of any law, rule, or regula-  
13 tion, gross mismanagement, or substantial and  
14 specific danger to public health, safety, or secu-  
15 rity, and that is protected under any Federal or  
16 State law (other than those referenced in sub-  
17 paragraph (A)) that shields the disclosing indi-  
18 vidual against retaliation or discrimination for  
19 having made the disclosure if such disclosure is  
20 not specifically prohibited by law and if such in-  
21 formation is not specifically required by Execu-  
22 tive order to be kept secret in the interest of  
23 national defense or the conduct of foreign af-  
24 fairs; or

1           “(C) to the Special Counsel, the inspector  
2           general of an agency, or any other employee  
3           designated by the head of an agency to receive  
4           similar disclosures;

5           “(4) prevent the Director from using informa-  
6           tion required to be submitted under sections 246,  
7           248, or 249 for enforcement of this subtitle, includ-  
8           ing enforcement proceedings subject to appropriate  
9           safeguards;

10          “(5) authorize information to be withheld from  
11          Congress, the Government Accountability Office, or  
12          Inspector General of the Department; or

13          “(6) create a private right of action for enforce-  
14          ment of any provision of this section.

15          “(f) AUDIT.—

16          “(1) IN GENERAL.—Not later than 1 year after  
17          the date of enactment of the Protecting Cyberspace  
18          as a National Asset Act of 2010, the Inspector Gen-  
19          eral of the Department shall conduct an audit of the  
20          management of information submitted under sub-  
21          section (b) and report the findings to appropriate  
22          committees of Congress.

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

1           “(A) whether the information is adequately  
2 safeguarded against inappropriate disclosure;

3           “(B) the processes for marking and dis-  
4 seminating the information and resolving any  
5 disputes;

6           “(C) how the information is used for the  
7 purposes of this section, and whether that use  
8 is effective;

9           “(D) whether information sharing has been  
10 effective to fulfill the purposes of this section;

11           “(E) whether the kinds of information sub-  
12 mitted have been appropriate and useful, or  
13 overbroad or overnarrow;

14           “(F) whether the information protections  
15 allow for adequate accountability and trans-  
16 parency of the regulatory, enforcement, and  
17 other aspects of implementing this subtitle; and

18           “(G) any other factors at the discretion of  
19 the Inspector General.

20 **“SEC. 252. SECTOR-SPECIFIC AGENCIES.**

21           “(a) IN GENERAL.—The head of each sector-specific  
22 agency and the head of any Federal agency that is not  
23 a sector-specific agency with responsibilities for regulating  
24 covered critical infrastructure shall coordinate with the  
25 Director on any activities of the sector-specific agency or

1 Federal agency that relate to the efforts of the agency re-  
2 garding security or resiliency of the national information  
3 infrastructure, including critical infrastructure and cov-  
4 ered critical infrastructure, within or under the super-  
5 vision of the agency.

6 “(b) DUPLICATIVE REPORTING REQUIREMENTS.—

7 The head of each sector-specific agency and the head of  
8 any Federal agency that is not a sector-specific agency  
9 with responsibilities for regulating covered critical infra-  
10 structure shall coordinate with the Director to eliminate  
11 and avoid the creation of duplicate reporting or compli-  
12 ance requirements relating to the security or resiliency of  
13 the national information infrastructure, including critical  
14 infrastructure and covered critical infrastructure, within  
15 or under the supervision of the agency.

16 “(c) REQUIREMENTS.—

17 “(1) IN GENERAL.—To the extent that the head  
18 of each sector-specific agency and the head of any  
19 Federal agency that is not a sector-specific agency  
20 with responsibilities for regulating covered critical  
21 infrastructure has the authority to establish regula-  
22 tions, rules, or requirements or other required ac-  
23 tions that are applicable to the security of national  
24 information infrastructure, including critical infra-

1 structure and covered critical infrastructure, the  
2 head of that agency shall—

3 “(A) notify the Director in a timely fash-  
4 ion of the intent to establish the regulations,  
5 rules, requirements, or other required actions;

6 “(B) coordinate with the Director to en-  
7 sure that the regulations, rules, requirements,  
8 or other required actions are consistent with,  
9 and do not conflict or impede, the activities of  
10 the Director under sections 247, 248, and 249;  
11 and

12 “(C) in coordination with the Director, en-  
13 sure that the regulations, rules, requirements,  
14 or other required actions are implemented, as  
15 they relate to covered critical infrastructure, in  
16 accordance with subsection (a).

17 “(2) COORDINATION.—Coordination under  
18 paragraph (1)(B) shall include the active participa-  
19 tion of the Director in the process for developing  
20 regulations, rules, requirements, or other required  
21 actions.

22 “(3) RULE OF CONSTRUCTION.—Nothing in  
23 this section shall be construed to provide additional  
24 authority for any sector-specific agency or any Fed-  
25 eral agency that is not a sector-specific agency with

1 responsibilities for regulating national information  
2 infrastructure, including critical infrastructure or  
3 covered critical infrastructure, to establish standards  
4 or other measures that are applicable to the security  
5 of national information infrastructure not otherwise  
6 authorized by law.

7 **“SEC. 253. STRATEGY FOR FEDERAL CYBERSECURITY SUP-**  
8 **PLY CHAIN MANAGEMENT.**

9 “(a) IN GENERAL.—The Secretary, in consultation  
10 with the Director of Cyberspace Policy, the Director, the  
11 Secretary of Defense, the Secretary of Commerce, the Sec-  
12 retary of State, the Director of National Intelligence, the  
13 Administrator of General Services, the Administrator for  
14 Federal Procurement Policy, the other members of the  
15 Chief Information Officers Council established under sec-  
16 tion 3603 of title 44, United States Code, the Chief Acqui-  
17 sition Officers Council established under section 16A of  
18 the Office of Federal Procurement Policy Act (41 U.S.C.  
19 414b), the Chief Financial Officers Council established  
20 under section 302 of the Chief Financial Officers Act of  
21 1990 (31 U.S.C. 901 note), and the private sector, shall  
22 develop, periodically update, and implement a supply chain  
23 risk management strategy designed to ensure the security  
24 of the Federal information infrastructure, including pro-  
25 tection against unauthorized access to, alteration of infor-

1 mation in, disruption of operations of, interruption of com-  
2 munications or services of, and insertion of malicious soft-  
3 ware, engineering vulnerabilities, or otherwise corrupting  
4 software, hardware, services, or products intended for use  
5 in Federal information infrastructure.

6 “(b) CONTENTS.—The supply chain risk manage-  
7 ment strategy developed under subsection (a) shall—

8 “(1) address risks in the supply chain during  
9 the entire life cycle of any part of the Federal infor-  
10 mation infrastructure;

11 “(2) place particular emphasis on—

12 “(A) securing critical information systems  
13 and the Federal information infrastructure;

14 “(B) developing processes that—

15 “(i) incorporate all-source intelligence  
16 analysis into assessments of the supply  
17 chain for the Federal information infra-  
18 structure;

19 “(ii) assess risks from potential sup-  
20 pliers providing critical components or  
21 services of the Federal information infra-  
22 structure;

23 “(iii) assess risks from individual  
24 components, including all subcomponents;

1 or software used in or affecting the Fed-  
2 eral information infrastructure;

3 “(iv) manage the quality, configura-  
4 tion, and security of software, hardware,  
5 and systems of the Federal information in-  
6 frastructure throughout the life cycle of  
7 the software, hardware, or system, includ-  
8 ing components or subcomponents from  
9 secondary and tertiary sources;

10 “(v) detect the occurrence, reduce the  
11 likelihood of occurrence, and mitigate or  
12 remediate the risks associated with prod-  
13 ucts containing counterfeit components or  
14 malicious functions;

15 “(vi) enhance developmental and oper-  
16 ational test and evaluation capabilities, in-  
17 cluding software vulnerability detection  
18 methods and automated tools that shall be  
19 integrated into acquisition policy practices  
20 by Federal agencies and, where appro-  
21 priate, make the capabilities available for  
22 use by the private sector; and

23 “(vii) protect the intellectual property  
24 and trade secrets of suppliers of informa-

1           tion and communications technology prod-  
2           ucts and services;

3           ~~“(C) the use of internationally-recognized~~  
4           standards and standards developed by the pri-  
5           vate sector and developing a process, with the  
6           National Institute for Standards and Tech-  
7           nology, to make recommendations for improve-  
8           ments of the standards;

9           ~~“(D) identifying acquisition practices of~~  
10          Federal agencies that increase risks in the sup-  
11          ply chain and developing a process to provide  
12          recommendations for revisions to those proc-  
13          esses; and

14          ~~“(E) sharing with the private sector, to the~~  
15          fullest extent possible, the threats identified in  
16          the supply chain and working with the private  
17          sector to develop responses to those threats as  
18          identified; and

19          ~~“(3) to the extent practicable, promote the abil-~~  
20          ity of Federal agencies to procure commercial off the  
21          shelf information and communications technology  
22          products and services from a diverse pool of sup-  
23          pliers.

24          ~~“(e) IMPLEMENTATION.—The Federal Acquisition~~  
25          Regulatory Council established under section 25(a) of the

1 Office of Federal Procurement Policy Act (41 U.S.C.  
2 421(a)) shall—

3 “(1) amend the Federal Acquisition Regulation  
4 issued under section 25 of that Act to—

5 “(A) incorporate, where relevant, the sup-  
6 ply chain risk management strategy developed  
7 under subsection (a) to improve security  
8 throughout the acquisition process; and

9 “(B) direct that all software and hardware  
10 purchased by the Federal Government shall  
11 comply with standards developed or be inter-  
12 operable with automated tools approved by the  
13 National Institute of Standards and Tech-  
14 nology, to continually enhance security; and

15 “(2) develop a clause or set of clauses for inclu-  
16 sion in solicitations, contracts, and task and delivery  
17 orders that sets forth the responsibility of the con-  
18 tractor under the Federal Acquisition Regulation  
19 provisions implemented under this subsection.”.

20 **TITLE III—FEDERAL INFORMA-**  
21 **TION SECURITY MANAGE-**  
22 **MENT**

23 **SEC. 301. COORDINATION OF FEDERAL INFORMATION POL-**  
24 **ICY.**

25 (a) FINDINGS.—Congress finds that—

1           (1) since 2002 the Federal Government has ex-  
 2           perienced multiple high-profile incidents that re-  
 3           sulted in the theft of sensitive information amount-  
 4           ing to more than the entire print collection con-  
 5           tained in the Library of Congress, including person-  
 6           ally identifiable information, advanced scientific re-  
 7           search, and prenegotiated United States diplomatic  
 8           positions; and

9           (2) chapter 35 of title 44, United States Code,  
 10          must be amended to increase the coordination of  
 11          Federal agency activities and to enhance situational  
 12          awareness throughout the Federal Government using  
 13          more effective enterprise-wide automated moni-  
 14          toring, detection, and response capabilities.

15          (b) IN GENERAL.—Chapter 35 of title 44, United  
 16          States Code, is amended by striking subchapters II and  
 17          III and inserting the following:

18          “SUBCHAPTER II—INFORMATION SECURITY

19          “§ 3550. Purposes

20          “The purposes of this subchapter are to—

21                 “(1) provide a comprehensive framework for en-  
 22                 suring the effectiveness of information security con-  
 23                 trols over information resources that support the  
 24                 Federal information infrastructure and the oper-  
 25                 ations and assets of agencies;

1           “(2) recognize the highly networked nature of  
2 the current Federal information infrastructure and  
3 provide effective Government-wide management and  
4 oversight of the related information security risks,  
5 including coordination of information security efforts  
6 throughout the civilian, national security, and law  
7 enforcement communities;

8           “(3) provide for development and maintenance  
9 of prioritized and risk-based security controls re-  
10 quired to protect Federal information infrastructure  
11 and information systems;

12           “(4) provide a mechanism for improved over-  
13 sight of Federal agency information security pro-  
14 grams;

15           “(5) acknowledge that commercially developed  
16 information security products offer advanced, dy-  
17 namic, robust, and effective information security so-  
18 lutions, reflecting market solutions for the protection  
19 of critical information infrastructures important to  
20 the national defense and economic security of the  
21 Nation that are designed, built, and operated by the  
22 private sector; and

23           “(6) recognize that the selection of specific  
24 technical hardware and software information secu-

1       rity solutions should be left to individual agencies  
2       from among commercially developed products.

3       **“§ 3551. Definitions**

4       “(a) IN GENERAL.—Except as provided under sub-  
5       section (b), the definitions under section 3502 shall apply  
6       to this subchapter.

7       “(b) ADDITIONAL DEFINITIONS.—In this subchapter:

8               “(1) The term ‘agency information infrastruc-  
9       ture’—

10               “(A) means information infrastructure  
11               that is owned, operated, controlled, or licensed  
12               for use by, or on behalf of, an agency, including  
13               information systems used or operated by an-  
14               other entity on behalf of the agency; and

15               “(B) does not include national security  
16               systems.

17               “(2) The term ‘automated and continuous mon-  
18               itoring’ means monitoring at a frequency and suffi-  
19               ciency such that the data exchange requires little to  
20               no human involvement and is not interrupted;

21               “(3) The term ‘incident’ means an occurrence  
22               that—

23               “(A) actually or potentially jeopardizes—

24                       “(i) the information security of an in-  
25                       formation system; or

1                   “(ii) the information the system proc-  
2                   esses, stores, or transmits; or

3                   “(B) constitutes a violation or threat of  
4                   violation of security policies, security proce-  
5                   dures, or acceptable use policies.

6                   “(4) The term ‘information infrastructure’  
7                   means the underlying framework that information  
8                   systems and assets rely on to process, transmit, re-  
9                   ceive, or store information electronically, including  
10                  programmable electronic devices and communica-  
11                  tions networks and any associated hardware, soft-  
12                  ware, or data.

13                  “(5) The term ‘information security’ means  
14                  protecting information and information systems  
15                  from disruption or unauthorized access, use, disclo-  
16                  sure, modification, or destruction in order to pro-  
17                  vide—

18                         “(A) integrity, by guarding against im-  
19                         proper information modification or destruction,  
20                         including by ensuring information nonrepudi-  
21                         ation and authenticity;

22                         “(B) confidentiality, by preserving author-  
23                         ized restrictions on access and disclosure, in-  
24                         cluding means for protecting personal privacy  
25                         and proprietary information; and

1           ~~“(C) availability, by ensuring timely and~~  
2           ~~reliable access to and use of information.~~

3           ~~“(6) The term ‘information technology’ has the~~  
4           ~~meaning given that term in section 11101 of title~~  
5           ~~40.~~

6           ~~“(7) The term ‘management controls’ means~~  
7           ~~safeguards or countermeasures for an information~~  
8           ~~system that focus on the management of risk and~~  
9           ~~the management of information system security.~~

10          ~~“(8)(A) The term ‘national security system’~~  
11          ~~means any information system (including any tele-~~  
12          ~~communications system) used or operated by an~~  
13          ~~agency or by a contractor of an agency, or other or-~~  
14          ~~ganization on behalf of an agency—~~

15                 ~~“(i) the function, operation, or use of~~  
16                 ~~which—~~

17                         ~~“(I) involves intelligence activities;~~

18                         ~~“(II) involves cryptologic activities re-~~  
19                         ~~lated to national security;~~

20                         ~~“(III) involves command and control~~  
21                         ~~of military forces;~~

22                         ~~“(IV) involves equipment that is an~~  
23                         ~~integral part of a weapon or weapons sys-~~  
24                         ~~tem; or~~

1           “(V) subject to subparagraph (B), is  
2           critical to the direct fulfillment of military  
3           or intelligence missions; or

4           “(ii) that is protected at all times by proce-  
5           dures established for information that have  
6           been specifically authorized under criteria es-  
7           tablished by an Executive order or an Act of  
8           Congress to be kept classified in the interest of  
9           national defense or foreign policy.

10          “(B) Subparagraph (A)(i)(V) does not include a  
11          system that is to be used for routine administrative  
12          and business applications (including payroll, finance,  
13          logistics, and personnel management applications).

14          “(9) The term ‘operational controls’ means the  
15          safeguards and countermeasures for an information  
16          system that are primarily implemented and executed  
17          by individuals, not systems.

18          “(10) The term ‘risk’ means the potential for  
19          an unwanted outcome resulting from an incident, as  
20          determined by the likelihood of the occurrence of the  
21          incident and the associated consequences, including  
22          potential for an adverse outcome assessed as a func-  
23          tion of threats, vulnerabilities, and consequences as-  
24          sociated with an incident.

1           “(11) The term ‘risk-based security’ means se-  
2           curity commensurate with the risk and magnitude of  
3           harm resulting from the loss, misuse, or unauthor-  
4           ized access to, or modification, of information, in-  
5           cluding assuring that systems and applications used  
6           by the agency operate effectively and provide appro-  
7           priate confidentiality, integrity, and availability.

8           “(12) The term ‘security controls’ means the  
9           management, operational, and technical controls pre-  
10          scribed for an information system to protect the in-  
11          formation security of the system.

12          “(13) The term ‘technical controls’ means the  
13          safeguards or countermeasures for an information  
14          system that are primarily implemented and executed  
15          by the information system through mechanism con-  
16          tained in the hardware, software, or firmware com-  
17          ponents of the system.

18 **“§ 3552. Authority and functions of the National Cen-**  
19 **ter for Cybersecurity and Communica-**  
20 **tions**

21          “(a) IN GENERAL.—The Director of the National  
22 Center for Cybersecurity and Communications shall—

23               “(1) develop, oversee the implementation of,  
24               and enforce policies, principles, and guidelines on in-  
25               formation security, including through ensuring time-

1 ly agency adoption of and compliance with standards  
2 developed under section 20 of the National Institute  
3 of Standards and Technology Act (15 U.S.C. 278g-  
4 3) and subtitle E of title II of the Homeland Secu-  
5 rity Act of 2002;

6 “(2) provide to agencies security controls that  
7 agencies shall be required to be implemented to miti-  
8 gate and remediate vulnerabilities, attacks, and ex-  
9 ploitations discovered as a result of activities re-  
10 quired under this subchapter or subtitle E of title II  
11 of the Homeland Security Act of 2002;

12 “(3) to the extent practicable—

13 “(A) prioritize the policies, principles,  
14 standards, and guidelines promulgated under  
15 section 20 of the National Institute of Stand-  
16 ards and Technology Act (15 U.S.C. 278g-3),  
17 paragraph (1), and subtitle E of title II of the  
18 Homeland Security Act of 2002, based upon  
19 the risk of an incident; and

20 “(B) develop guidance that requires agen-  
21 cies to monitor, including automated and con-  
22 tinuous monitoring of, the effective implementa-  
23 tion of policies, principles, standards, and  
24 guidelines developed under section 20 of the  
25 National Institute of Standards and Technology

1 Act (~~15 U.S.C. 278g-3~~), paragraph (1), and  
2 subtitle E of title II of the Homeland Security  
3 Act of 2002;

4 “(C) ensure the effective operation of tech-  
5 nical capabilities within the National Center for  
6 Cybersecurity and Communications to enable  
7 automated and continuous monitoring of any  
8 information collected as a result of the guidance  
9 developed under subparagraph (B) and use the  
10 information to enhance the risk-based security  
11 of the Federal information infrastructure; and

12 “(D) ensure the effective operation of a se-  
13 cure system that satisfies information reporting  
14 requirements under sections ~~3553(e)~~ and  
15 ~~3556(e)~~;

16 “(4) require agencies, consistent with the stand-  
17 ards developed under section 20 of the National In-  
18 stitute of Standards and Technology Act (~~15 U.S.C.~~  
19 ~~278g-3~~) or paragraph (1) and the requirements of  
20 this subchapter, to identify and provide information  
21 security protections commensurate with the risk re-  
22 sulting from the disruption or unauthorized access,  
23 use, disclosure, modification, or destruction of—

24 “(A) information collected or maintained  
25 by or on behalf of an agency; or

1           ~~“(B) information systems used or operated~~  
 2           ~~by an agency or by a contractor of an agency~~  
 3           ~~or other organization on behalf of an agency;~~

4           ~~“(5) oversee agency compliance with the re-~~  
 5           ~~quirements of this subchapter, including coordi-~~  
 6           ~~nating with the Office of Management and Budget~~  
 7           ~~to use any authorized action under section 11303 of~~  
 8           ~~title 40 to enforce accountability for compliance with~~  
 9           ~~such requirements;~~

10           ~~“(6) review, at least annually, and approve or~~  
 11           ~~disapprove, agency information security programs~~  
 12           ~~required under section 3553(b); and~~

13           ~~“(7) coordinate information security policies~~  
 14           ~~and procedures with the Administrator for Elec-~~  
 15           ~~tronic Government and the Administrator for the~~  
 16           ~~Office of Information and Regulatory Affairs with~~  
 17           ~~related information resources management policies~~  
 18           ~~and procedures.~~

19           ~~“(b) NATIONAL SECURITY SYSTEMS.—The authori-~~  
 20           ~~ties of the Director under this section shall not apply to~~  
 21           ~~national security systems.~~

22   **“§ 3553. Agency responsibilities**

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

24           ~~“(1) be responsible for—~~

1           “(A) providing information security protec-  
2           tions commensurate with the risk and mag-  
3           nitude of the harm resulting from unauthorized  
4           access, use, disclosure, disruption, modification,  
5           or destruction of—

6                   “(i) information collected or main-  
7                   tained by or on behalf of the agency; and

8                   “(ii) agency information infrastruc-  
9                   ture;

10           “(B) complying with the requirements of  
11           this subchapter and related policies, procedures,  
12           standards, and guidelines, including—

13                   “(i) information security require-  
14                   ments, including security controls, devel-  
15                   oped by the Director of the National Cen-  
16                   ter for Cybersecurity and Communications  
17                   under section 3552, subtitle E of title II of  
18                   the Homeland Security Act of 2002, or  
19                   any other provision of law;

20                   “(ii) information security policies,  
21                   principles, standards, and guidelines pro-  
22                   mulgated under section 20 of the National  
23                   Institute of Standards and Technology Act  
24                   (15 U.S.C. 278g-3) and section  
25                   3552(a)(1);

1           “(iii) information security standards  
2           and guidelines for national security sys-  
3           tems issued in accordance with law and as  
4           directed by the President; and

5           “(iv) ensuring the standards imple-  
6           mented for information systems and na-  
7           tional security systems of the agency are  
8           complementary and uniform, to the extent  
9           practicable;

10          “(C) ensuring that information security  
11          management processes are integrated with  
12          agency strategic and operational planning pro-  
13          cesses, including policies, procedures, and prac-  
14          tices described in subsection (e)(1)(C);

15          “(D) as appropriate, maintaining secure  
16          facilities that have the capability of accessing,  
17          sending, receiving, and storing classified infor-  
18          mation;

19          “(E) maintaining a sufficient number of  
20          personnel with security clearances, at the ap-  
21          propriate levels, to access, send, receive and  
22          analyze classified information to carry out the  
23          responsibilities of this subchapter; and

24          “(F) ensuring that information security  
25          performance indicators and measures are in-

1 eluded in the annual performance evaluations of  
2 all managers, senior managers, senior executive  
3 service personnel, and political appointees;

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

9 “(A) assessing the risk and magnitude of  
10 the harm that could result from the disruption  
11 or unauthorized access, use, disclosure, modi-  
12 fication, or destruction of such information or  
13 information systems;

14 “(B) determining the levels of information  
15 security appropriate to protect such information  
16 and information systems in accordance with  
17 policies, principles, standards, and guidelines  
18 promulgated under section 20 of the National  
19 Institute of Standards and Technology Act (15  
20 U.S.C. 278g-3), section 3552(a)(1), and sub-  
21 title E of title II of the Homeland Security Act  
22 of 2002, for information security categoriza-  
23 tions and related requirements;

1           “(C) implementing policies and procedures  
2           to cost effectively reduce risks to an acceptable  
3           level;

4           “(D) periodically testing and evaluating in-  
5           formation security controls and techniques to  
6           ensure that such controls and techniques are  
7           operating effectively; and

8           “(E) withholding all bonus and cash  
9           awards to senior agency officials accountable  
10          for the operation of such agency information in-  
11          frastructure that are recognized by the Chief  
12          Information Security Officer as impairing the  
13          risk-based security information, information  
14          system, or agency information infrastructure;

15          “(3) delegate to a senior agency officer des-  
16          ignated as the Chief Information Security Officer  
17          the authority and budget necessary to ensure and  
18          enforce compliance with the requirements imposed  
19          on the agency under this subchapter, subtitle E of  
20          title II of the Homeland Security Act of 2002, or  
21          any other provision of law, including—

22                 “(A) overseeing the establishment, mainte-  
23                 nance, and management of a security oper-  
24                 ations center that has technical capabilities that

1 can, through automated and continuous moni-  
2 toring—

3 “(i) detect, report, respond to, con-  
4 tain, remediate, and mitigate incidents  
5 that impair risk-based security of the in-  
6 formation, information systems, and agen-  
7 cy information infrastructure, in accord-  
8 ance with policy provided by the National  
9 Center for Cybersecurity and Communica-  
10 tions;

11 “(ii) monitor and, on a risk-based  
12 basis, mitigate and remediate the  
13 vulnerabilities of every information system  
14 within the agency information infrastruc-  
15 ture;

16 “(iii) continually evaluate risks posed  
17 to information collected or maintained by  
18 or on behalf of the agency and information  
19 systems and hold senior agency officials  
20 accountable for ensuring the risk-based se-  
21 curity of such information and information  
22 systems;

23 “(iv) collaborate with the National  
24 Center for Cybersecurity and Communica-  
25 tions and appropriate public and private

1 sector security operations centers to ad-  
2 dress incidents that impact the security of  
3 information and information systems that  
4 extend beyond the control of the agency;  
5 and

6 “(v) report any incident described  
7 under clauses (i) and (ii), as directed by  
8 the policy of the National Center for Cy-  
9 bersecurity and Communications or the In-  
10 spector General of the agency;

11 “(B) collaborating with the Administrator  
12 for E-Government and the Chief Information  
13 Officer to establish, maintain, and update an  
14 enterprise network, system, storage, and secu-  
15 rity architecture, that can be accessed by the  
16 National Cybersecurity Communications Center  
17 and includes—

18 “(i) information on how security con-  
19 trols are implemented throughout the  
20 agency information infrastructure; and

21 “(ii) information on how the controls  
22 described under subparagraph (A) main-  
23 tain the appropriate level of confidentiality,  
24 integrity, and availability of information  
25 and information systems based on—

1           “(I) the policy of the National  
2           Center for Cybersecurity and Commu-  
3           nications; and

4           “(II) the standards or guidance  
5           developed by the National Institute of  
6           Standards and Technology;

7           “(C) developing, maintaining, and over-  
8           seeing an agency-wide information security pro-  
9           gram as required by subsection (b);

10          “(D) developing, maintaining, and over-  
11          seeing information security policies, procedures,  
12          and control techniques to address all applicable  
13          requirements, including those issued under sec-  
14          tion 3552;

15          “(E) training, consistent with the require-  
16          ments of section 406 of the Protecting Cyber-  
17          space as a National Asset Act of 2010, and  
18          overseeing personnel with significant respon-  
19          sibilities for information security with respect to  
20          such responsibilities; and

21          “(F) assisting senior agency officers con-  
22          cerning their responsibilities under paragraph  
23          (2);

24          “(4) ensure that the Chief Information Security  
25          Officer has a sufficient number of cleared and

1 trained personnel with technical skills identified by  
2 the National Center for Cybersecurity and Commu-  
3 nications as critical to maintaining the risk-based se-  
4 curity of agency information infrastructure as re-  
5 quired by the subchapter and other applicable laws;

6 “(5) ensure that the agency Chief Information  
7 Security Officer, in coordination with appropriate  
8 senior agency officials, reports not less than annu-  
9 ally to the head of the agency on the effectiveness  
10 of the agency information security program, includ-  
11 ing progress of remedial actions;

12 “(6) ensure that the Chief Information Security  
13 Officer—

14 “(A) possesses necessary qualifications, in-  
15 cluding education, professional certifications,  
16 training, experience, and the security clearance  
17 required to administer the functions described  
18 under this subchapter; and

19 “(B) has information security duties as the  
20 primary duty of that officer; and

21 “(7) ensure that components of that agency es-  
22 tablish and maintain an automated reporting mecha-  
23 nism that allows the Chief Information Security Of-  
24 ficer with responsibility for the entire agency, and all  
25 components thereof, to implement, monitor, and hold

1 senior agency officers accountable for the implemen-  
2 tation of appropriate security policies, procedures,  
3 and controls of agency components.

4 “(b) AGENCY-WIDE INFORMATION SECURITY PRO-  
5 GRAM.—Each agency shall develop, document, and imple-  
6 ment an agency-wide information security program, ap-  
7 proved by the National Center for Cybersecurity and Com-  
8 munications under section 3552(a)(6) and consistent with  
9 components across and within agencies, to provide infor-  
10 mation security for the information and information sys-  
11 tems that support the operations and assets of the agency,  
12 including those provided or managed by another agency,  
13 contractor, or other source, that includes—

14 “(1) frequent assessments, at least twice each  
15 month—

16 “(A) of the risk and magnitude of the  
17 harm that could result from the disruption or  
18 unauthorized access, use, disclosure, modifica-  
19 tion, or destruction of information and informa-  
20 tion systems that support the operations and  
21 assets of the agency; and

22 “(B) that assess whether information or  
23 information systems should be removed or mi-  
24 grated to more secure networks or standards  
25 and make recommendations to the head of the

1 agency and the Director of the National Center  
2 for Cybersecurity and Communications based  
3 on that assessment;

4 “(2) consistent with guidance developed under  
5 section 3554, vulnerability assessments and penetra-  
6 tion tests commensurate with the risk posed to an  
7 agency information infrastructure;

8 “(3) ensure that information security  
9 vulnerabilities are remediated or mitigated based on  
10 the risk posed to the agency;

11 “(4) policies and procedures that—

12 “(A) are informed and revised by the as-  
13 sessments required under paragraphs (1) and  
14 (2);

15 “(B) cost effectively reduce information se-  
16 curity risks to an acceptable level;

17 “(C) ensure that information security is  
18 addressed throughout the life cycle of each  
19 agency information system; and

20 “(D) ensure compliance with—

21 “(i) the requirements of this sub-  
22 chapter;

23 “(ii) policies and procedures pre-  
24 scribed by the National Center for Cyber-  
25 security and Communications;

1           “(iii) minimally acceptable system  
2 configuration requirements, as determined  
3 by the National Center for Cybersecurity  
4 and Communications; and

5           “(iv) any other applicable require-  
6 ments, including standards and guidelines  
7 for national security systems issued in ac-  
8 cordance with law and as directed by the  
9 President;

10          “(5) subordinate plans for providing risk-based  
11 information security for networks, facilities, and sys-  
12 tems or groups of information systems, as appro-  
13 priate;

14          “(6) role-based security awareness training,  
15 consistent with the requirements of section 406 of  
16 the Protecting Cyberspace as a National Asset Act  
17 of 2010, to inform personnel with access to the  
18 agency network, including contractors and other  
19 users of information systems that support the oper-  
20 ations and assets of the agency, of—

21           “(A) information security risks associated  
22 with agency activities; and

23           “(B) agency responsibilities in complying  
24 with agency policies and procedures designed to  
25 reduce those risks;

1           “(7) periodic testing and evaluation of the ef-  
2           fectiveness of information security policies, proce-  
3           dures, and practices, to be performed with a rigor  
4           and frequency depending on risk, which shall in-  
5           clude—

6                   “(A) testing and evaluation not less than  
7                   twice each year of security controls of informa-  
8                   tion collected or maintained by or on behalf of  
9                   the agency and every information system identi-  
10                  fied in the inventory required under section  
11                  3505(e);

12                  “(B) the effectiveness of ongoing moni-  
13                  toring, including automated and continuous  
14                  monitoring, vulnerability scanning, and intru-  
15                  sion detection and prevention of incidents posed  
16                  to the risk-based security of information and in-  
17                  formation systems as required under subsection  
18                  (a)(3); and

19                  “(C) testing relied on in—

20                          “(i) an operational evaluation under  
21                          section 3554;

22                          “(ii) an independent assessment under  
23                          section 3556; or

24                          “(iii) another evaluation, to the extent  
25                          specified by the Director;

1           “(8) a process for planning, implementing, eval-  
2           uating, and documenting remedial action to address  
3           any deficiencies in the information security policies,  
4           procedures, and practices of the agency;

5           “(9) procedures for detecting, reporting, and re-  
6           sponding to incidents, consistent with requirements  
7           issued under section 3552, that include—

8                   “(A) to the extent practicable, automated  
9                   and continuous monitoring of the use of infor-  
10                  mation and information systems;

11                  “(B) requirements for mitigating risks and  
12                  remediating vulnerabilities associated with such  
13                  incidents systemically within the agency infor-  
14                  mation infrastructure before substantial dam-  
15                  age is done; and

16                  “(C) notifying and coordinating with the  
17                  National Center for Cybersecurity and Commu-  
18                  nications, as required by this subchapter, sub-  
19                  title E of title II of the Homeland Security Act  
20                  of 2002, and any other provision of law; and

21           “(10) plans and procedures to ensure continuity  
22           of operations for information systems that support  
23           the operations and assets of the agency.

24           “(e) AGENCY REPORTING.—

25                   “(1) IN GENERAL.—Each agency shall—

1           “(A) ensure that information relating to  
2 the adequacy and effectiveness of information  
3 security policies, procedures, and practices, is  
4 available to the entities identified under para-  
5 graph (2) through the system developed under  
6 section 3552(a)(3), including information relat-  
7 ing to—

8                   “(i) compliance with the requirements  
9 of this subchapter;

10                   “(ii) the effectiveness of the informa-  
11 tion security policies, procedures, and prac-  
12 tices of the agency based on a determina-  
13 tion of the aggregate effect of identified  
14 deficiencies and vulnerabilities;

15                   “(iii) an identification and analysis of  
16 any significant deficiencies identified in  
17 such policies, procedures, and practices;

18                   “(iv) an identification of any vulner-  
19 ability that could impair the risk-based se-  
20 curity of the agency information infra-  
21 structure; and

22                   “(v) results of any operational evalua-  
23 tion conducted under section 3554 and  
24 plans of action to address the deficiencies

1           and vulnerabilities identified as a result of  
2           such operational evaluation;

3           “(B) follow the policy, guidance, and  
4           standards of the National Center for Cybersecu-  
5           rity and Communications, in consultation with  
6           the Federal Information Security Taskforce, to  
7           continually update, and ensure the electronic  
8           availability of both a classified and unclassified  
9           version of the information required under sub-  
10          paragraph (A);

11          “(C) ensure the information under sub-  
12          paragraph (A) addresses the adequacy and ef-  
13          fectiveness of information security policies, pro-  
14          cedures, and practices in plans and reports re-  
15          lating to—

16                 “(i) annual agency budgets;

17                 “(ii) information resources manage-  
18                 ment of this subchapter;

19                 “(iii) information technology manage-  
20                 ment and procurement under this chapter  
21                 or any other applicable provision of law;

22                 “(iv) subtitle E of title II of the  
23                 Homeland Security Act of 2002;

24                 “(v) program performance under sec-  
25                 tions 1105 and 1115 through 1119 of title

1           ~~31~~, and sections ~~2801~~ and ~~2805~~ of title  
2           ~~39~~;

3           ~~“(vi) financial management under~~  
4           ~~chapter 9 of title 31, and the Chief Finan-~~  
5           ~~cial Officers Act of 1990 (31 U.S.C. 501~~  
6           ~~note; Public Law 101-576) (and the~~  
7           ~~amendments made by that Act);~~

8           ~~“(vii) financial management systems~~  
9           ~~under the Federal Financial Management~~  
10          ~~Improvement Act (31 U.S.C. 3512 note);~~

11          ~~“(viii) internal accounting and admin-~~  
12          ~~istrative controls under section 3512 of~~  
13          ~~title 31; and~~

14          ~~“(ix) performance ratings, salaries,~~  
15          ~~and bonuses provided to the senior man-~~  
16          ~~agers and supporting personnel taking into~~  
17          ~~account program performance as it relates~~  
18          ~~to complying with this subchapter; and~~

19          ~~“(D) report any significant deficiency in a~~  
20          ~~policy, procedure, or practice identified under~~  
21          ~~subparagraph (A) or (B)—~~

22          ~~“(i) as a material weakness in report-~~  
23          ~~ing under section 3512 of title 31; and~~

24          ~~“(ii) if relating to financial manage-~~  
25          ~~ment systems, as an instance of a lack of~~

1           substantial compliance under the Federal  
2           Financial Management Improvement Act  
3           (31 U.S.C. 3512 note).

4           “(2) ADEQUACY AND EFFECTIVENESS INFOR-  
5           MATION.—Information required under paragraph  
6           (1)(A) shall, to the extent possible and in accordance  
7           with applicable law, policy, guidance, and standards,  
8           be available on an automated and continuous basis  
9           to—

10           “(A) the National Center for Cybersecurity  
11           and Communications;

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

14           “(C) the Committee on Government Over-  
15           sight and Reform of the House of Representa-  
16           tives;

17           “(D) the Committee on Homeland Security  
18           of the House of Representatives;

19           “(E) other appropriate authorization and  
20           appropriations committees of Congress;

21           “(F) the Inspector General of the Federal  
22           agency; and

23           “(G) the Comptroller General.

24           “(d) INCLUSIONS IN PERFORMANCE PLANS.—

1           “(1) IN GENERAL.—In addition to the require-  
2           ments of subsection (c), each agency, in consultation  
3           with the National Center for Cybersecurity and  
4           Communications, shall include as part of the per-  
5           formance plan required under section 1115 of title  
6           31 a description of the time periods the resources,  
7           including budget, staffing, and training, that are  
8           necessary to implement the program required under  
9           subsection (b).

10           “(2) RISK ASSESSMENTS.—The description  
11           under paragraph (1) shall be based on the risk and  
12           vulnerability assessments required under subsection  
13           (b) and evaluations required under section 3554.

14           “(e) NOTICE AND COMMENT.—Each agency shall  
15           provide the public with timely notice and opportunities for  
16           comment on proposed information security policies and  
17           procedures to the extent that such policies and procedures  
18           affect communication with the public.

19           “(f) MORE STRINGENT STANDARDS.—The head of  
20           an agency may employ standards for the cost effective in-  
21           formation security for information systems within or  
22           under the supervision of that agency that are more strin-  
23           gent than the standards the Director of the National Cen-  
24           ter for Cybersecurity and Communications prescribes  
25           under this subchapter, subtitle E of title II of the Home-

1 land Security Act of 2002, or any other provision of law,  
2 if the more stringent standards—

3           “(1) contain at least the applicable standards  
4           made compulsory and binding by the Director of the  
5           National Center for Cybersecurity and Communica-  
6           tions; and

7           “(2) are otherwise consistent with policies and  
8           guidelines issued under section 3552.

9 **“§ 3554. Annual operational evaluation**

10           “(a) GUIDANCE.—

11           “(1) IN GENERAL.—Each year the National  
12           Center for Cybersecurity and Communications shall  
13           oversee, coordinate, and develop guidance for the ef-  
14           fective implementation of operational evaluations of  
15           the Federal information infrastructure and agency  
16           information security programs and practices to de-  
17           termine the effectiveness of such program and prac-  
18           tices.

19           “(2) COLLABORATION IN DEVELOPMENT.—In  
20           developing guidance for the operational evaluations  
21           described under this section, the National Center for  
22           Cybersecurity and Communications shall collaborate  
23           with the Federal Information Security Taskforce  
24           and the Council of Inspectors General on Integrity  
25           and Efficiency, and other agencies as necessary, to

1 develop and update risk-based performance indica-  
2 tors and measures that assess the adequacy and ef-  
3 fectiveness of information security of an agency and  
4 the Federal information infrastructure.

5 “(3) CONTENTS OF OPERATIONAL EVALUA-  
6 TION.—Each operational evaluation under this sec-  
7 tion—

8 “(A) shall be prioritized based on risk; and

9 “(B) shall—

10 “(i) test the effectiveness of agency  
11 information security policies, procedures,  
12 and practices of the information systems of  
13 the agency, or a representative subset of  
14 those information systems;

15 “(ii) assess (based on the results of  
16 the testing) compliance with—

17 “(I) the requirements of this sub-  
18 chapter; and

19 “(II) related information security  
20 policies, procedures, standards, and  
21 guidelines;

22 “(iii) evaluate whether agencies—

23 “(I) effectively monitor, detect,  
24 analyze, protect, report, and respond  
25 to vulnerabilities and incidents;

1           “(II) report to and collaborate  
2           with the appropriate public and pri-  
3           vate security operation centers, the  
4           National Center for Cybersecurity and  
5           Communications, and law enforcement  
6           agencies; and

7           “(III) remediate or mitigate the  
8           risk posed by attacks and exploi-  
9           tations in a timely fashion in order to  
10          prevent future vulnerabilities and inci-  
11          dents; and

12          “(iv) identify deficiencies of agency in-  
13          formation security policies, procedures, and  
14          controls on the agency information infra-  
15          structure.

16          “(b) CONDUCT AN OPERATIONAL EVALUATION.—

17                 “(1) IN GENERAL.—Except as provided under  
18                 paragraph (2), and in consultation with the Chief  
19                 Information Officer and senior officials responsible  
20                 for the affected systems, the Chief Information Se-  
21                 curity Officer of each agency shall not less than an-  
22                 nually—

23                         “(A) conduct an operational evaluation of  
24                         the agency information infrastructure for

1 vulnerabilities, attacks, and exploitations of the  
2 agency information infrastructure;

3 “(B) evaluate the ability of the agency to  
4 monitor, detect, correlate, analyze, report, and  
5 respond to incidents; and

6 “(C) report to the head of the agency, the  
7 National Center for Cybersecurity and Commu-  
8 nications, the Chief Information Officer, and  
9 the Inspector General for the agency the find-  
10 ings of the operational evaluation.

11 “(2) SATISFACTION OF REQUIREMENTS BY  
12 OTHER EVALUATION.—Unless otherwise specified by  
13 the Director of the National Center for Cybersecu-  
14 rity and Communications, if the National Center for  
15 Cybersecurity and Communications conducts an  
16 operational evaluation of the agency information in-  
17 frastructure under section 245(b)(2)(A) of the  
18 Homeland Security Act of 2002, the Chief Informa-  
19 tion Security Officer may deem the requirements of  
20 paragraph (1) satisfied for the year in which the  
21 operational evaluation described under this para-  
22 graph is conducted.

23 “(e) CORRECTIVE MEASURES MITIGATION AND RE-  
24 MEDIATION PLANS.—

1           “(1) IN GENERAL.—In consultation with the  
2 National Center for Cybersecurity and Communica-  
3 tions and the Chief Information Officer, Chief Infor-  
4 mation Security Officers shall remediate or mitigate  
5 vulnerabilities in accordance with this subsection.

6           “(2) RISK-BASED PLAN.—After an operational  
7 evaluation is conducted under this section or under  
8 section 245(b) of the Homeland Security Act of  
9 2002, the agency shall submit to the National Cen-  
10 ter for Cybersecurity and Communications in a time-  
11 ly fashion a risk-based plan for addressing rec-  
12 ommendations and mitigating and remediating  
13 vulnerabilities identified as a result of such oper-  
14 ational evaluation, including a timeline and budget  
15 for implementing such plan.

16           “(3) APPROVAL OR DISAPPROVAL.—Not later  
17 than 15 days after receiving a plan submitted under  
18 paragraph (2), the National Center for Cybersecu-  
19 rity and Communications shall—

20                   “(A) approve or disprove the agency plan;  
21                   and

22                   “(B) comment on the adequacy and effec-  
23 tiveness of the plan.

24           “(4) ISOLATION FROM INFRASTRUCTURE.—

1           “(A) IN GENERAL.—The Director of the  
2 National Center for Cybersecurity and Commu-  
3 nications may, consistent with the contingency  
4 or continuity of operation plans applicable to  
5 such agency information infrastructure, order  
6 the isolation of any component of the Federal  
7 information infrastructure from any other Fed-  
8 eral information infrastructure, if—

9           “(i) an agency does not implement  
10 measures in a risk-based plan approved  
11 under this subsection; and

12           “(ii) the failure to comply presents a  
13 significant danger to the Federal informa-  
14 tion infrastructure.

15           “(B) DURATION.—An isolation under sub-  
16 paragraph (A) shall remain in effect until—

17           “(i) the Director of the National Cen-  
18 ter for Cybersecurity and Communications  
19 determines that corrective measures have  
20 been implemented; or

21           “(ii) an updated risk-based plan is ap-  
22 proved by the National Center for Cyberse-  
23 curity and Communications and imple-  
24 mented by the agency.

1       “(d) OPERATIONAL GUIDANCE.—The Director of the  
2 National Center for Cybersecurity and Communications  
3 shall—

4           “(1) not later than 180 days after the date of  
5 enactment of the Protecting Cyberspace as a Na-  
6 tional Asset Act of 2010, develop operational guid-  
7 ance for operational evaluations as required under  
8 this section that are risk-based and cost effective;  
9 and

10          “(2) periodically evaluate and ensure informa-  
11 tion is available on an automated and continuous  
12 basis through the system required under section  
13 3552(a)(3)(D) to Congress on—

14           “(A) the adequacy and effectiveness of the  
15 operational evaluations conducted under this  
16 section or section 245(b) of the Homeland Se-  
17 curity Act of 2002; and

18           “(B) possible executive and legislative ac-  
19 tions for cost-effectively managing the risks to  
20 the Federal information infrastructure.

21 **“§ 3555. Federal Information Security Taskforce**

22       “(a) ESTABLISHMENT.—There is established in the  
23 executive branch a Federal Information Security  
24 Taskforce.

1       “(b) MEMBERSHIP.—The members of the Federal In-  
2 formation Security Taskforce shall be full-time senior Gov-  
3 ernment employees and shall be as follows:

4           “(1) The Director of the National Center for  
5 Cybersecurity and Communications.

6           “(2) The Administrator of the Office of Elec-  
7 tronic Government of the Office of Management and  
8 Budget.

9           “(3) The Chief Information Security Officer of  
10 each agency described under section 901(b) of title  
11 31.

12           “(4) The Chief Information Security Officer of  
13 the Department of the Army, the Department of the  
14 Navy, and the Department of the Air Force.

15           “(5) A representative from the Office of Cyber-  
16 space Policy.

17           “(6) A representative from the Office of the Di-  
18 rector of National Intelligence.

19           “(7) A representative from the United States  
20 Cyber Command.

21           “(8) A representative from the National Secu-  
22 rity Agency.

23           “(9) A representative from the United States  
24 Computer Emergency Readiness Team.

1           “(10) A representative from the Intelligence  
2           Community Incident Response Center.

3           “(11) A representative from the Committee on  
4           National Security Systems.

5           “(12) A representative from the National Insti-  
6           tute for Standards and Technology.

7           “(13) A representative from the Council of In-  
8           spectors General on Integrity and Efficiency.

9           “(14) A representative from State and local  
10          government.

11          “(15) Any other officer or employee of the  
12          United States designated by the chairperson.

13          “(e) CHAIRPERSON AND VICE-CHAIRPERSON.—

14                 “(1) CHAIRPERSON.—The Director of the Na-  
15                 tional Center for Cybersecurity and Communications  
16                 shall act as chairperson of the Federal Information  
17                 Security Taskforce.

18                 “(2) VICE-CHAIRPERSON.—The vice chairperson  
19                 of the Federal Information Security Taskforce  
20                 shall—

21                         “(A) be selected by the Federal Informa-  
22                         tion Security Taskforce from among its mem-  
23                         bers;

24                         “(B) serve a 1-year term and may serve  
25                         multiple terms; and

1           “(C) serve as a liaison to the Chief Infor-  
2           mation Officer, Council of the Inspectors Gen-  
3           eral on Integrity and Efficiency, Committee on  
4           National Security Systems, and other councils  
5           or committees as appointed by the chairperson.

6           “(d) FUNCTIONS.—The Federal Information Security  
7 Taskforce shall—

8           “(1) be the principal interagency forum for col-  
9           laboration regarding best practices and recommenda-  
10          tions for agency information security and the secu-  
11          rity of the Federal information infrastructure;

12          “(2) assist in the development of and annually  
13          evaluate guidance to fulfill the requirements under  
14          sections 3554 and 3556;

15          “(3) share experiences and innovative ap-  
16          proaches relating to threats against the Federal in-  
17          formation infrastructure, information sharing and  
18          information security best practices, penetration test-  
19          ing regimes, and incident response, mitigation, and  
20          remediation;

21          “(4) promote the development and use of stand-  
22          ard performance indicators and measures for agency  
23          information security that—

24                  “(A) are outcome-based;

25                  “(B) focus on risk management;

1           “(C) align with the business and program  
2 goals of the agency;

3           “(D) measure improvements in the agency  
4 security posture over time; and

5           “(E) reduce burdensome and efficient per-  
6 formance indicators and measures;

7           “(5) recommend to the Office of Personnel  
8 Management the necessary qualifications to be es-  
9 tablished for Chief Information Security Officers to  
10 be capable of administering the functions described  
11 under this subchapter including education, training,  
12 and experience;

13           “(6) enhance information system processes by  
14 establishing a prioritized baseline of information se-  
15 curity measures and controls that can be continu-  
16 ously monitored through automated mechanisms;

17           “(7) evaluate the effectiveness and efficiency of  
18 any reporting and compliance requirements that are  
19 required by law related to the information security  
20 of Federal information infrastructure; and

21           “(8) submit proposed enhancements developed  
22 under paragraphs (1) through (7) to the Director of  
23 the National Center for Cybersecurity and Commu-  
24 nications.

25           “(e) TERMINATION.—

1           ~~“(1) IN GENERAL.—Except as provided under~~  
 2           ~~paragraph (2), the Federal Information Security~~  
 3           ~~Taskforce shall terminate 4 years after the date of~~  
 4           ~~enactment of the Protecting Cyberspace as a Na-~~  
 5           ~~tional Asset Act of 2010.~~

6           ~~“(2) EXTENSION.—The President may—~~

7                   ~~“(A) extend the Federal Information Secu-~~  
 8                   ~~rity Taskforce by executive order; and~~

9                   ~~“(B) make more than 1 extension under~~  
 10           ~~this paragraph for any period as the President~~  
 11           ~~may determine.~~

12   **“§ 3556. Independent Assessments**

13           ~~“(a) IN GENERAL.—~~

14           ~~“(1) INSPECTORS GENERAL ASSESSMENTS.—~~  
 15           ~~Not less than every 2 years, each agency with an In-~~  
 16           ~~spector General appointed under the Inspector Gen-~~  
 17           ~~eral Act of 1978 (5 U.S.C. App.) shall assess the~~  
 18           ~~adequacy and effectiveness of the information secu-~~  
 19           ~~rity program developed under section 3553(b) and~~  
 20           ~~(c), and evaluations conducted under section 3554.~~

21           ~~“(2) INDEPENDENT ASSESSMENTS.—For each~~  
 22           ~~agency to which paragraph (1) does not apply, the~~  
 23           ~~head of the agency shall engage an independent ex-~~  
 24           ~~ternal auditor to perform the assessment.~~



~~“3555. Federal Information Security Taskforce.~~

~~“3556. Independent assessments.~~

~~“3557. Protection of information.”.~~

1           ~~(2) OTHER REFERENCES.—~~

2                   ~~(A) Section 1001(e)(1)(A) of the Home-~~  
3                   ~~land Security Act of 2002 (6 U.S.C.~~  
4                   ~~511(e)(1)(A)) is amended by striking “section~~  
5                   ~~3532(3)” and inserting “section 3551(b)”.~~

6                   ~~(B) Section 2222(j)(6) of title 10, United~~  
7                   ~~States Code, is amended by striking “section~~  
8                   ~~3542(b)(2))” and inserting “section 3551(b)”.~~

9                   ~~(C) Section 2223(e)(3) of title 10, United~~  
10                   ~~States Code, is amended, by striking “section~~  
11                   ~~3542(b)(2))” and inserting “section 3551(b)”.~~

12                   ~~(D) Section 2315 of title 10, United States~~  
13                   ~~Code, is amended by striking “section~~  
14                   ~~3542(b)(2))” and inserting “section 3551(b)”.~~

15                   ~~(E) Section 20(a)(2) of the National Insti-~~  
16                   ~~tute of Standards and Technology Act (15~~  
17                   ~~U.S.C. 278g-3) is amended by striking “section~~  
18                   ~~3532(b)(2))” and inserting “section 3551(b)”.~~

19                   ~~(F) Section 21(b)(2) of the National Insti-~~  
20                   ~~tute of Standards and Technology Act (15~~  
21                   ~~U.S.C. 278g-4(b)(2)) is amended by striking~~  
22                   ~~“Institute and” and inserting “Institute, the~~  
23                   ~~Director of the National Center on Cybersecu-~~  
24                   ~~rity and Communications, and”.~~

1           (G) Section 21(b)(3) of the National Insti-  
2           tute of Standards and Technology Act (15  
3           U.S.C. 278g-4(b)(3)) is amended by inserting  
4           “the Director of the National Center on Cyber-  
5           security and Communications,” after “the Di-  
6           rector of the National Security Agency.”

7           (H) Section 8(d)(1) of the Cyber Security  
8           Research and Development Act (15 U.S.C.  
9           7406(d)(1)) is amended by striking “section  
10          3534(b)” and inserting “section 3553(b)”.

11          (3) HOMELAND SECURITY ACT OF 2002.—

12           (A) TITLE X.—The Homeland Security  
13           Act of 2002 (6 U.S.C. 101 et seq.) is amended  
14           by striking title X.

15           (B) TABLE OF CONTENTS.—The table of  
16           contents in section 1(b) of the Homeland Secu-  
17           rity Act of 2002 (6 U.S.C. 101 et seq.) is  
18           amended by striking the matter relating to title  
19           X.

20          (d) REPEAL OF OTHER STANDARDS.—

21           (1) IN GENERAL.—Section 11331 of title 40,  
22           United States Code, is repealed.

23           (2) TECHNICAL AND CONFORMING AMEND-  
24           MENTS.—

1           (A) Section 20(e)(3) of the National Insti-  
2           tute of Standards and Technology Act (15  
3           U.S.C. 278g-3(e)(3)) is amended by striking  
4           “under section 11331 of title 40, United States  
5           Code”.

6           (B) Section 20(d)(1) of the National Insti-  
7           tute of Standards and Technology Act (15  
8           U.S.C. 278g-3(d)(1)) is amended by striking  
9           “the Director of the Office of Management and  
10           Budget for promulgation under section 11331  
11           of title 40, United States Code” and inserting  
12           “the Secretary of Commerce for promulgation”.

13           (C) Section 11302(d) of title 40, United  
14           States Code, is amended by striking “under sec-  
15           tion 11331 of this title and”.

16           (D) Section 1874A (e)(2)(A)(ii) of the So-  
17           cial Security Act (42 U.S.C. 1395kk-  
18           1(e)(2)(A)(ii)) is amended by striking “section  
19           11331 of title 40, United States Code” and in-  
20           serting “section 3552 of title 44, United States  
21           Code”.

22           (E) Section 3504(g)(2) of title 44, United  
23           States Code, is amended by striking “section  
24           11331 of title 40” and inserting “section 3552  
25           of title 44”.

1           (F) Section 3504(h)(1) of title 44, United  
 2 States Code, is amended by inserting “, the Di-  
 3 rector of the National Center for Cybersecurity  
 4 and Communications,” after “the National In-  
 5 stitute of Standards and Technology”.

6           (G) Section 3504(h)(1)(B) of title 44,  
 7 United States Code, is amended by striking  
 8 “under section 11331 of title 40” and inserting  
 9 “section 3552 of title 44”.

10          (H) Section 3518(d) of title 44, United  
 11 States Code, is amended by striking “sections  
 12 11331 and 11332” and inserting “section  
 13 11332”.

14          (I) Section 3602(f)(8) of title 44, United  
 15 States Code, is amended by striking “under sec-  
 16 tion 11331 of title 40.

17          (J) Section 3603(f)(5) of title 44, United  
 18 States Code, is amended by striking “and pro-  
 19 mulgated under section 11331 of title 40.”.

20       **TITLE IV—RECRUITMENT AND**  
 21       **PROFESSIONAL DEVELOPMENT**

22       **SEC. 401. DEFINITIONS.**

23       In this title:

24           (1) **CYBERSECURITY MISSION.**—The term “cy-  
 25       bersecurity mission” means the activities of the Fed-

1 eral Government that encompass the full range of  
 2 threat reduction, vulnerability reduction, deterrence,  
 3 international engagement, incident response, resil-  
 4 iency, and recovery policies and activities, including  
 5 computer network operations, information assur-  
 6 ance, law enforcement, diplomacy, military, and in-  
 7 telligence missions as such activities relate to the se-  
 8 curity and stability of cyberspace.

9 ~~(2) FEDERAL AGENCY'S CYBERSECURITY MIS-~~  
 10 ~~SION.—~~The term “Federal agency’s cybersecurity  
 11 mission” means, with respect to any Federal agency,  
 12 the portion of the cybersecurity mission that is the  
 13 responsibility of the Federal agency.

14 **SEC. 402. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

15 (a) ~~IN GENERAL.—~~The Director of the Office of Per-  
 16 sonnel Management and the Director shall assess the  
 17 readiness and capacity of the Federal workforce to meet  
 18 the needs of the cybersecurity mission of the Federal Gov-  
 19 ernment.

20 (b) ~~STRATEGY.—~~

21 ~~(1) IN GENERAL.—~~Not later than 180 days  
 22 after the date of enactment of this Act, the Director  
 23 of the Office of Personnel Management shall develop  
 24 and implement a comprehensive workforce strategy  
 25 that enhances the readiness, capacity, training, and

1 recruitment and retention of Federal cybersecurity  
2 personnel.

3 (2) CONTENTS.—The strategy developed under  
4 paragraph (1) shall include—

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

7 (B) 10-year and 20-year projections of  
8 workforce needs.

9 **SEC. 403. STRATEGIC CYBERSECURITY WORKFORCE PLAN-**  
10 **NING.**

11 (a) FEDERAL AGENCY DEVELOPMENT OF STRA-  
12 TEGIC CYBERSECURITY WORKFORCE PLANS.—Not later  
13 than 180 days after the date of enactment of this Act and  
14 in every subsequent year, the head of each Federal agency  
15 shall develop a strategic cybersecurity workforce plan as  
16 part of the Federal agency performance plan required  
17 under section 1115 of title 31, United States Code.

18 (b) INTERAGENCY COORDINATION.—Each Federal  
19 agency shall develop a plan prepared under subsection  
20 (a)—

21 (1) on the basis of the assessment developed  
22 under section 402 and any subsequent guidance  
23 from the Director of the Office of Personnel Man-  
24 agement and the Director; and

1           (2) in consultation with the Director and the  
2 Director of the Office of Management and Budget.

3       (c) CONTENTS OF THE PLAN.—

4           (1) IN GENERAL.—Each plan prepared under  
5 subsection (a) shall include—

6           (A) a description of the Federal agency's  
7 cybersecurity mission;

8           (B) subject to paragraph (2), a description  
9 and analysis, relating to the specialized work-  
10 force needed by the Federal agency to fulfill the  
11 Federal agency's cybersecurity mission, includ-  
12 ing—

13           (i) the workforce needs of the Federal  
14 agency on the date of the report, and 10-  
15 year and 20-year projections of workforce  
16 needs;

17           (ii) hiring projections to meet work-  
18 force needs, including, for at least a 2-year  
19 period, specific occupation and grade lev-  
20 els;

21           (iii) long-term and short-term stra-  
22 tegic goals to address critical skills defi-  
23 ciencies, including analysis of the numbers  
24 of and reasons for attrition of employees;

1 (iv) recruitment strategies, including  
2 the use of student internships, part-time  
3 employment, student loan reimbursement,  
4 and telework, to attract highly qualified  
5 candidates from diverse backgrounds and  
6 geographic locations;

7 (v) an assessment of the sources and  
8 availability of individuals with needed ex-  
9 pertise;

10 (vi) ways to streamline the hiring  
11 process;

12 (vii) the barriers to recruiting and hir-  
13 ing individuals qualified in cybersecurity  
14 and recommendations to overcome the bar-  
15 riers; and

16 (viii) a training and development plan,  
17 consistent with the curriculum developed  
18 under section 406, to enhance and improve  
19 the knowledge of employees.

20 (2) FEDERAL AGENCIES WITH SMALL SPECIAL-  
21 IZED WORKFORCE.—In accordance with guidance  
22 provided by the Director of the Office of Personnel  
23 Management, a Federal agency that needs only a  
24 small specialized workforce to fulfill the Federal  
25 agency's cybersecurity mission may present the

1 workforce plan components referred to in paragraph  
2 (1)(B) as part of the Federal agency performance  
3 plan required under section 1115 of title 31, United  
4 States Code.

5 **SEC. 404. CYBERSECURITY OCCUPATION CLASSIFICATIONS.**

6 (a) **IN GENERAL.**—Not later than 1 year after the  
7 date of enactment of this Act, the Director of the Office  
8 of Personnel Management, in coordination with the Direc-  
9 tor, shall develop and issue comprehensive occupation clas-  
10 sifications for Federal employees engaged in cybersecurity  
11 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. 405. MEASURES OF CYBERSECURITY HIRING EFFEC-**  
18 **TIVENESS.**

19 (a) **IN GENERAL.**—The head of each Federal agency  
20 shall measure, and collect information on, indicators of the  
21 effectiveness of the recruitment and hiring by the Federal  
22 agency of a workforce needed to fulfill the Federal agen-  
23 cy's cybersecurity mission.

24 (b) **TYPES OF INFORMATION.**—The indicators of ef-  
25 fectiveness measured and subject to collection of informa-

1 tion under subsection (a) shall include indicators with re-  
2 spect to the following:

3           (1) ~~RECRUITING AND HIRING.~~—In relation to  
4 recruiting and hiring by the Federal agency—

5           (A) the ability to reach and recruit well-  
6 qualified individuals from diverse talent pools;

7           (B) the use and impact of special hiring  
8 authorities and flexibilities to recruit the most  
9 qualified applicants, including the use of stu-  
10 dent internship and scholarship programs for  
11 permanent hires;

12           (C) the use and impact of special hiring  
13 authorities and flexibilities to recruit diverse  
14 candidates, including criteria such as the vet-  
15 eran status, race, ethnicity, gender, disability,  
16 or national origin of the candidates; and

17           (D) the educational level, and source of ap-  
18 plicants.

19           (2) ~~SUPERVISORS.~~—In relation to the super-  
20 visors of the positions being filled—

21           (A) satisfaction with the quality of the ap-  
22 plicants interviewed and hired;

23           (B) satisfaction with the match between  
24 the skills of the individuals and the needs of the  
25 Federal agency;

1           (C) satisfaction of the supervisors with the  
2 hiring process and hiring outcomes;

3           (D) whether any mission-critical defi-  
4 ciencies were addressed by the individuals and  
5 the connection between the deficiencies and the  
6 performance of the Federal agency; and

7           (E) the satisfaction of the supervisors with  
8 the period of time elapsed to fill the positions.

9           (3) APPLICANTS.—The satisfaction of appli-  
10 cants with the hiring process, including clarity of job  
11 announcements, any reasons for withdrawal of an  
12 application, the user-friendliness of the application  
13 process, communication regarding status of applica-  
14 tions, and the timeliness of offers of employment.

15           (4) HIRED INDIVIDUALS.—In relation to the in-  
16 dividuals hired—

17           (A) satisfaction with the hiring process;

18           (B) satisfaction with the process of start-  
19 ing employment in the position for which the  
20 individual was hired;

21           (C) attrition; and

22           (D) the results of exit interviews.

23           (e) REPORTS.—

24           (1) IN GENERAL.—The head of each Federal  
25 agency shall submit the information collected under

1 this section to the Director of the Office of Per-  
2 sonnel Management on an annual basis and in ac-  
3 cordance with the regulations issued under sub-  
4 section (d).

5 (2) AVAILABILITY OF RECRUITING AND HIRING  
6 INFORMATION.—

7 (A) IN GENERAL.—The Director of the Of-  
8 fice of Personnel Management shall prepare an  
9 annual report containing the information re-  
10 ceived under paragraph (1) in a consistent for-  
11 mat to allow for a comparison of hiring effec-  
12 tiveness and experience across demographic  
13 groups and Federal agencies.

14 (B) SUBMISSION.—The Director of the Of-  
15 fice of Personnel Management shall—

16 (i) not later than 90 days after the re-  
17 ceipt of all information required to be sub-  
18 mitted under paragraph (1); make the re-  
19 port prepared under subparagraph (A)  
20 publicly available, including on the website  
21 of the Office of Personnel Management;  
22 and

23 (ii) before the date on which the re-  
24 port prepared under subparagraph (A) is

1           made publicly available; submit the report  
2           to Congress.

3       (d) REGULATIONS.—

4           (1) IN GENERAL.—Not later than 180 days  
5       after the date of enactment of this Act, the Director  
6       of the Office of Personnel Management shall issue  
7       regulations establishing the methodology, timing,  
8       and reporting of the data required to be submitted  
9       under this section.

10          (2) SCOPE AND DETAIL OF REQUIRED INFOR-  
11       MATION.—The regulations under paragraph (1) shall  
12       delimit the scope and detail of the information that  
13       a Federal agency is required to collect and submit  
14       under this section, taking account of the size and  
15       complexity of the workforce that the Federal agency  
16       needs to fulfill the Federal agency's cybersecurity  
17       mission.

18   **SEC. 406. TRAINING AND EDUCATION.**

19       (a) TRAINING.—

20           (1) FEDERAL GOVERNMENT EMPLOYEES AND  
21       FEDERAL CONTRACTORS.—The Director of the Of-  
22       fice of Personnel Management, in conjunction with  
23       the Director of the National Center for Cybersecu-  
24       rity and Communications, the Director of National  
25       Intelligence, the Secretary of Defense, and the Chief

1 Information Officers Council established under sec-  
2 tion ~~3603~~ of title 44, United States Code, shall es-  
3 tablish a cybersecurity awareness and education cur-  
4 riculum that shall be required for all Federal em-  
5 ployees and contractors engaged in the design, devel-  
6 opment, or operation of agency information infra-  
7 structure, as defined under section ~~3551~~ of title 44,  
8 United States Code.

9 (2) CONTENTS.—The curriculum established  
10 under paragraph (1) may include—

11 (A) role-based security awareness training;

12 (B) recommended cybersecurity practices;

13 (C) cybersecurity recommendations for  
14 traveling abroad;

15 (D) unclassified counterintelligence infor-  
16 mation;

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

19 (F) information regarding malicious activ-  
20 ity online;

21 (G) information regarding cybersecurity  
22 and law enforcement;

23 (H) identity management information;

24 (I) information regarding supply chain se-  
25 curity;

1           ~~(J)~~ information security risks associated  
2           with the activities of Federal employees; and

3           ~~(K)~~ the responsibilities of Federal employ-  
4           ees in complying with policies and procedures  
5           designed to reduce information security risks  
6           identified under subparagraph ~~(J)~~.

7           ~~(3)~~ FEDERAL CYBERSECURITY PROFES-  
8           SIONALS.—The Director of the Office of Personnel  
9           Management in conjunction with the Director of the  
10          National Center for Cybersecurity and Communica-  
11          tions, the Director of National Intelligence, the Sec-  
12          retary of Defense, the Director of the Office of Man-  
13          agement and Budget, and, as appropriate, colleges,  
14          universities, and nonprofit organizations with cyber-  
15          security training expertise, shall develop a program,  
16          to provide training to improve and enhance the skills  
17          and capabilities of Federal employees engaged in the  
18          cybersecurity mission, including training specific to  
19          the acquisition workforce.

20          ~~(4)~~ HEADS OF FEDERAL AGENCIES.—Not later  
21          than 30 days after the date on which an individual  
22          is appointed to a position at level I or II of the Ex-  
23          ecutive Schedule, the Director of the National Cen-  
24          ter for Cybersecurity and Communications and the  
25          Director of National Intelligence, or their designees,

1 shall provide that individual with a cybersecurity  
2 threat briefing.

3 ~~(5) CERTIFICATION.—~~The head of each Federal  
4 agency shall include in the annual report required  
5 under section ~~3553(e)~~ of title 44, United States  
6 Code, a certification regarding whether all officers,  
7 employees, and contractors of the Federal agency  
8 have completed the training required under this sub-  
9 section.

10 ~~(b) EDUCATION.—~~

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

18 ~~(2) K THROUGH 12.—~~The Secretary of Edu-  
19 cation, in coordination with the Director of the Na-  
20 tional Center for Cybersecurity and Communications  
21 and State and local governments, shall develop cur-  
22 riculum standards, guidelines, and recommended  
23 courses to address cyber safety, cybersecurity, and  
24 cyber ethics for students in kindergarten through  
25 grade 12.

1           (3) UNDERGRADUATE, GRADUATE, VOCA-  
2           TIONAL, AND TECHNICAL INSTITUTIONS.—

3           (A) SECRETARY OF EDUCATION.—The  
4           Secretary of Education, in coordination with  
5           the Director of the National Center for Cyber-  
6           security and Communications, shall—

7                   (i) develop curriculum standards and  
8                   guidelines to address cyber safety, cyberse-  
9                   curity, and cyber ethics for all students en-  
10                  rolled in undergraduate, graduate, voca-  
11                  tional, and technical institutions in the  
12                  United States; and

13                  (ii) analyze and develop recommended  
14                  courses for students interested in pursuing  
15                  careers in information technology, commu-  
16                  nications, computer science, engineering,  
17                  math, and science, as those subjects relate  
18                  to cybersecurity.

19           (B) OFFICE OF PERSONNEL MANAGE-  
20           MENT.—The Director of the Office of Personnel  
21           Management, in coordination with the Director,  
22           shall develop strategies and programs—

23                   (i) to recruit students from under-  
24                   graduate, graduate, vocational, and tech-  
25                   nical institutions in the United States to

1 serve as Federal employees engaged in  
2 cyber missions; and

3 (ii) that provide internship and part-  
4 time work opportunities with the Federal  
5 Government for students at the under-  
6 graduate, graduate, vocational, and tech-  
7 nical institutions in the United States.

8 (e) CYBER TALENT COMPETITIONS AND CHAL-  
9 LENGES.—

10 (1) IN GENERAL.—The Director of the National  
11 Center for Cybersecurity and Communications shall  
12 establish a program to ensure the effective operation  
13 of national and statewide competitions and chal-  
14 lenges that seek to identify, develop, and recruit tal-  
15 ented individuals to work in Federal agencies, State  
16 and local government agencies, and the private sec-  
17 tor to perform duties relating to the security of the  
18 Federal information infrastructure or the national  
19 information infrastructure.

20 (2) GROUPS AND INDIVIDUALS.—The program  
21 under this subsection shall include—

22 (A) high school students;

23 (B) undergraduate students;

24 (C) graduate students;

25 (D) academic and research institutions;

1           ~~(E)~~ veterans; and

2           ~~(F)~~ other groups or individuals as the Di-  
3           rector may determine.

4           ~~(3)~~ SUPPORT OF OTHER COMPETITIONS AND  
5           CHALLENGES.—The program under this subsection  
6           may support other competitions and challenges not  
7           established under this subsection through affiliation  
8           and cooperative agreements with—

9           ~~(A)~~ Federal agencies;

10          ~~(B)~~ regional, State, or community school  
11          programs supporting the development of cyber  
12          professionals; or

13          ~~(C)~~ other private sector organizations.

14          ~~(4)~~ AREAS OF TALENT.—The program under  
15          this subsection shall seek to identify, develop, and  
16          recruit exceptional talent relating to—

17          ~~(A)~~ ethical hacking;

18          ~~(B)~~ penetration testing;

19          ~~(C)~~ vulnerability Assessment;

20          ~~(D)~~ continuity of system operations;

21          ~~(E)~~ cyber forensics; and

22          ~~(F)~~ offensive and defensive cyber oper-  
23          ations.

1 **SEC. 407. CYBERSECURITY INCENTIVES.**

2 (a) AWARDS.—In making cash awards under chapter  
3 45 of title 5, United States Code, the President or the  
4 head of a Federal agency, in consultation with the Direc-  
5 tor, shall consider the success of an employee in fulfilling  
6 the objectives of the National Strategy, in a manner con-  
7 sistent with any policies, guidelines, procedures, instruc-  
8 tions, or standards established by the President.

9 (b) OTHER INCENTIVES.—The head of each Federal  
10 agency shall adopt best practices, developed by the Direc-  
11 tor of the National Center for Cybersecurity and Commu-  
12 nications and the Office of Management and Budget, re-  
13 garding effective ways to educate and motivate employees  
14 of the Federal Government to demonstrate leadership in  
15 cybersecurity, including—

16 (1) promotions and other nonmonetary awards;  
17 and

18 (2) publicizing information sharing accomplish-  
19 ments by individual employees and, if appropriate,  
20 the tangible benefits that resulted.

21 **SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR**  
22 **THE NATIONAL CENTER FOR CYBERSECU-**  
23 **RITY AND COMMUNICATIONS.**

24 (a) DEFINITIONS.—In this section:

1           (1) CENTER.—The term “Center” means the  
2 National Center for Cybersecurity and Communica-  
3 tions.

4           (2) DEPARTMENT.—The term “Department”  
5 means the Department of Homeland Security.

6           (3) DIRECTOR.—The term “Director” means  
7 the Director of the Center.

8           (4) ENTRY LEVEL POSITION.—The term “entry  
9 level position” means a position that—

10                   (A) is established by the Director in the  
11 Center; and

12                   (B) is classified at GS-7, GS-8, or GS-9  
13 of the General Schedule.

14           (5) SECRETARY.—The term “Secretary” means  
15 the Secretary of Homeland Security.

16           (6) SENIOR POSITION.—The term “senior posi-  
17 tion” means a position that—

18                   (A) is established by the Director in the  
19 Center; and

20                   (B) is not established under section 5108  
21 of title 5, United States Code, but is similar in  
22 duties and responsibilities for positions estab-  
23 lished under that section.

24           (b) RECRUITMENT AND RETENTION PROGRAM.—

1           (1) ESTABLISHMENT.—The Director may es-  
 2           tablish a program to assist in the recruitment and  
 3           retention of highly skilled personnel to carry out the  
 4           functions of the Center.

5           (2) CONSULTATION AND CONSIDERATIONS.—In  
 6           establishing a program under this section, the Direc-  
 7           tor shall—

8                   (A) consult with the Secretary; and

9                   (B) consider—

10                   (i) national and local employment  
 11                   trends;

12                   (ii) the availability and quality of can-  
 13                   didates;

14                   (iii) any specialized education or cer-  
 15                   tifications required for positions;

16                   (iv) whether there is a shortage of  
 17                   certain skills; and

18                   (v) such other factors as the Director  
 19                   determines appropriate.

20           (e) HIRING AND SPECIAL PAY AUTHORITIES.—

21           (1) DIRECT HIRE AUTHORITY.—Without regard  
 22           to the civil service laws (other than sections 3303  
 23           and 3328 of title 5, United States Code), the Direc-  
 24           tor may appoint not more than 500 employees under

1 this subsection to carry out the functions of the Cen-  
2 ter.

3 (2) RATES OF PAY.—

4 (A) ENTRY LEVEL POSITIONS.—The Direc-  
5 tor may fix the pay of the employees appointed  
6 to entry level positions under this subsection  
7 without regard to chapter 51 and subchapter  
8 III of chapter 53 of title 5, United States Code,  
9 relating to classification of positions and Gen-  
10 eral Schedule pay rates, except that the rate of  
11 pay for any such employee may not exceed the  
12 maximum rate of basic pay payable for a posi-  
13 tion at GS-10 of the General Schedule while  
14 that employee is in an entry level position.

15 (B) SENIOR POSITIONS.—

16 (i) IN GENERAL.—The Director may  
17 fix the pay of the employees appointed to  
18 senior positions under this subsection with-  
19 out regard to chapter 51 and subchapter  
20 III of chapter 53 of title 5, United States  
21 Code, relating to classification of positions  
22 and General Schedule pay rates, except  
23 that the rate of pay for any such employee  
24 may not exceed the maximum rate of basic

1 pay payable under section 5376 of title 5,  
2 United States Code.

3 (ii) HIGHER MAXIMUM RATES.—

4 (I) IN GENERAL.—Notwith-  
5 standing the limitation on rates of pay  
6 under clause (i)—

7 (aa) not more than 20 em-  
8 ployees, identified by the Direc-  
9 tor, may be paid at a rate of pay  
10 not to exceed the maximum rate  
11 of basic pay payable for a posi-  
12 tion at level I of the Executive  
13 Schedule under section 5312 of  
14 title 5, United States Code; and

15 (bb) not more than 5 em-  
16 ployees, identified by the Director  
17 with the approval of the Sec-  
18 retary, may be paid at a rate of  
19 pay not to exceed the maximum  
20 rate of basic pay payable for the  
21 Vice President under section 104  
22 of title 3, United States Code.

23 (II) NONDELEGATION OF AU-  
24 THORITY.—The Secretary or the Di-

1 rector may not delegate any authority  
2 under this clause.

3 (d) CONVERSION TO COMPETITIVE SERVICE.—

4 (1) DEFINITION.—In this subsection, the term  
5 “qualified employee” means any individual appointed  
6 to an excepted service position in the Department  
7 who performs functions relating to the security of  
8 the Federal information infrastructure or national  
9 information infrastructure.

10 (2) COMPETITIVE CIVIL SERVICE STATUS.—In  
11 consultation with the Director, the Secretary may  
12 grant competitive civil service status to a qualified  
13 employee if that employee is—

14 (A) employed in the Center; or

15 (B) transferring to the Center.

16 (e) RETENTION BONUSES.—

17 (1) AUTHORITY.—Notwithstanding section  
18 5754 of title 5, United States Code, the Director  
19 may—

20 (A) pay a retention bonus under that sec-  
21 tion to any individual appointed under this sub-  
22 section, if the Director determines that, in the  
23 absence of a retention bonus, there is a high  
24 risk that the individual would likely leave em-  
25 ployment with the Department; and

1           ~~(B)~~ exercise the authorities of the Office of  
 2           Personnel Management and the head of an  
 3           agency under that section with respect to reten-  
 4           tion bonuses paid under this subsection.

5           ~~(2)~~ LIMITATIONS ON AMOUNT OF ANNUAL BO-  
 6           NUSES.—

7           ~~(A)~~ DEFINITIONS.—In this paragraph:

8           (i) MAXIMUM TOTAL PAY.—The term  
 9           “maximum total pay” means—

10           ~~(I)~~ in the case of an employee de-  
 11           scribed under subsection ~~(e)(2)(B)(i)~~,  
 12           the total amount of pay paid in a cal-  
 13           endar year at the maximum rate of  
 14           basic pay payable for a position at  
 15           level I of the Executive Schedule  
 16           under section 5312 of title 5, United  
 17           States Code;

18           ~~(II)~~ in the case of an employee  
 19           described under subsection  
 20           ~~(e)(2)(B)(ii)(I)(aa)~~, the total amount  
 21           of pay paid in a calendar year at the  
 22           maximum rate of basic pay payable  
 23           for a position at level I of the Execu-  
 24           tive Schedule under section 5312 of  
 25           title 5, United States Code; and

1                   (III) in the case of an employee  
 2                   described under subsection  
 3                   ~~(c)(2)(B)(ii)(I)(bb)~~, the total amount  
 4                   of pay paid in a calendar year at the  
 5                   maximum rate of basic pay payable  
 6                   for the Vice President under section  
 7                   104 of title 3, United States Code.

8                   (ii) TOTAL COMPENSATION.—The  
 9                   term “total compensation” means—

10                   (I) the amount of pay paid to an  
 11                   employee in any calendar year; and

12                   (II) the amount of all retention  
 13                   bonuses paid to an employee in any  
 14                   calendar year.

15                   (B) LIMITATION.—The Director may not  
 16                   pay a retention bonus under this subsection to  
 17                   an employee that would result in the total com-  
 18                   pensation of that employee exceeding maximum  
 19                   total pay.

20                   (f) TERMINATION OF AUTHORITY.—The authority to  
 21                   make appointments and pay retention bonuses under this  
 22                   section shall terminate 3 years after the date of enactment  
 23                   of this Act.

24                   (g) REPORTS.—

1           (1) ~~PLAN FOR EXECUTION OF AUTHORITIES.—~~  
 2           Not later than 120 days of enactment of this Act,  
 3           the Director shall submit a report to the appropriate  
 4           committees of Congress with a plan for the execu-  
 5           tion of the authorities provided under this section.

6           (2) ~~ANNUAL REPORT.—~~Not later than 6  
 7           months after the date of enactment of this Act, and  
 8           every year thereafter, the Director shall submit to  
 9           the appropriate committees of Congress a detailed  
 10          report that—

11                   (A) discusses how the actions taken during  
 12                   the period of the report are fulfilling the critical  
 13                   hiring needs of the Center;

14                   (B) assesses metrics relating to individuals  
 15                   hired under the authority of this section, includ-  
 16                   ing—

17                           (i) the numbers of individuals hired;  
 18                           (ii) the turnover in relevant positions;  
 19                           (iii) with respect to each individual  
 20                   hired—

21                                   (I) the position for which hired;  
 22                                   (II) the salary paid;  
 23                                   (III) any retention bonus paid  
 24                   and the amount of the bonus;

- 1           (IV) the geographic location from  
2           which hired;
- 3           (V) the immediate past salary;  
4           and
- 5           (VI) whether the individual was a  
6           noncareer appointee in the Senior Ex-  
7           ecutive Service or an appointee to a  
8           position of a confidential or policy-de-  
9           termining character under schedule C  
10          of subpart C of part 213 of title 5 of  
11          the Code of Federal Regulations be-  
12          fore the hiring; and
- 13          (iv) whether public notice for recruit-  
14          ment was made, and if so—
- 15               (I) the total number of qualified  
16               applicants;
- 17               (II) the number of veteran pref-  
18               erence eligible candidates who applied;
- 19               (III) the time from posting to job  
20               offer; and
- 21               (IV) statistics on diversity, in-  
22               cluding age, disability, race, gender,  
23               and national origin, of individuals  
24               hired under the authority of this sec-



1 carry out a research and development program for the  
2 purpose of improving the security of information infra-  
3 structure.

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

7 “(1) advance the development and accelerate  
8 the deployment of more secure versions of funda-  
9 mental Internet protocols and architectures, includ-  
10 ing for the secure domain name addressing system  
11 and routing security;

12 “(2) improve and create technologies for detect-  
13 ing and analyzing attacks or intrusions, including  
14 analysis of malicious software;

15 “(3) improve and create mitigation and recov-  
16 ery methodologies, including techniques for contain-  
17 ment of attacks and development of resilient net-  
18 works and systems;

19 “(4) develop and support infrastructure and  
20 tools to support cybersecurity research and develop-  
21 ment efforts, including modeling, testbeds, and data  
22 sets for assessment of new cybersecurity tech-  
23 nologies;

1           “(5) assist the development and support of  
2 technologies to reduce vulnerabilities in process con-  
3 trol systems;

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

6           “(7) test, evaluate, and facilitate, with appro-  
7 priate protections for any proprietary information  
8 concerning the technologies, the transfer of tech-  
9 nologies associated with the engineering of less vul-  
10 nerable software and securing the information tech-  
11 nology software development lifecycle;

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

14           “(9) assist the development of technologies de-  
15 signed to increase the security and resiliency of tele-  
16 communications networks;

17           “(10) advance the protection of privacy and  
18 civil liberties in cybersecurity technology and prac-  
19 tices; and

20           “(11) address other risks identified by the Di-  
21 rector of the National Center for Cybersecurity and  
22 Communications.

23           “(e) COORDINATION WITH OTHER RESEARCH INI-  
24 TIATIVES.—The Under Secretary—

1           “(1) shall ensure that the research and develop-  
2           ment program carried out under subsection (a) is  
3           consistent with the national strategy to increase the  
4           security and resilience of cyberspace developed by  
5           the Director of Cyberspace Policy under section 101  
6           of the Protecting Cyberspace as a National Asset  
7           Act of 2010, or any succeeding strategy;

8           “(2) shall, to the extent practicable, coordinate  
9           the research and development activities of the De-  
10          partment with other ongoing research and develop-  
11          ment security-related initiatives, including research  
12          being conducted by—

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

15                 “(B) the National Academy of Sciences;

16                 “(C) other Federal agencies, as defined  
17                 under section 241;

18                 “(D) other Federal and private research  
19                 laboratories, research entities, and universities  
20                 and institutions of higher education, and rel-  
21                 evant nonprofit organizations; and

22                 “(E) international partners of the United  
23                 States;

24           “(3) shall carry out any research and develop-  
25          ment project under subsection (a) through a reim-

1        bursable agreement with an appropriate Federal  
2        agency, as defined under section 241, if the Federal  
3        agency—

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

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

8                “(4) may make grants to, or enter into coopera-  
9                tive agreements, contracts, other transactions, or re-  
10              imburseable agreements with, the entities described in  
11              paragraph (2); and

12              “(5) shall submit a report to the appropriate  
13              committees of Congress on a review of the cyberse-  
14              curity activities, and the capacity, of the national  
15              laboratories and other research entities available to  
16              the Department to determine if the establishment of  
17              a national laboratory dedicated to cybersecurity re-  
18              search and development is necessary.

19              “(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIB-  
20              ERITIES ISSUES.—

21              “(1) CONSULTATION.—In carrying out research  
22              and development projects under subsection (a), the  
23              Under Secretary shall consult with the Privacy Offi-  
24              cer appointed under section 222 and the Officer for

1 Civil Rights and Civil Liberties of the Department  
2 appointed under section 705.

3 “(2) **PRIVACY IMPACT ASSESSMENTS.**—In ac-  
4 cordance with sections 222 and 705, the Privacy Of-  
5 ficer shall conduct privacy impact assessments and  
6 the Officer for Civil Rights and Civil Liberties shall  
7 conduct reviews, as appropriate, for research and de-  
8 velopment projects carried out under subsection (a)  
9 that the Under Secretary determines could have an  
10 impact on privacy, civil rights, or civil liberties.

11 **“SEC. 239. NATIONAL CYBERSECURITY ADVISORY COUNCIL.**

12 “(a) **ESTABLISHMENT.**—Not later than 90 days after  
13 the date of enactment of this section, the Secretary shall  
14 establish an advisory committee under section 871 on pri-  
15 vate sector cybersecurity, to be known as the National Cy-  
16 bersecurity Advisory Council (in this section referred to  
17 as the ‘Council’).

18 “(b) **RESPONSIBILITIES.**—

19 “(1) **IN GENERAL.**—The Council shall advise  
20 the Director of the National Center for Cybersecu-  
21 rity and Communications on the implementation of  
22 the cybersecurity provisions affecting the private sec-  
23 tor under this subtitle and subtitle E.

24 “(2) **INCENTIVES AND REGULATIONS.**—The  
25 Council shall advise the Director of the National

1 Center for Cybersecurity and Communications and  
2 appropriate committees of Congress (as defined in  
3 section 241) and any other congressional committee  
4 with jurisdiction over the particular matter regard-  
5 ing how market incentives and regulations may be  
6 implemented to enhance the cybersecurity and eco-  
7 nomic security of the Nation.

8 “(e) MEMBERSHIP.—

9 “(1) IN GENERAL.—The members of the Coun-  
10 cil shall be appointed the Director of the National  
11 Center for Cybersecurity and Communications and  
12 shall, to the extent practicable, represent a geo-  
13 graphic and substantive cross-section of owners and  
14 operators of critical infrastructure and others with  
15 expertise in cybersecurity, including, as appro-  
16 priate—

17 “(A) representatives of covered critical in-  
18 frastructure (as defined under section 241);

19 “(B) academic institutions with expertise  
20 in cybersecurity;

21 “(C) Federal, State, and local government  
22 agencies with expertise in cybersecurity;

23 “(D) a representative of the National Se-  
24 curity Telecommunications Advisory Council, as  
25 established by Executive Order 12382 (47 Fed.

1           Reg. 40531; relating to the establishment of the  
2           advisory council); as amended by Executive  
3           Order 13286 (68 Fed. Reg. 10619), as in effect  
4           on August 3, 2009, or any successor entity;

5           “(E) a representative of the Communica-  
6           tions Sector Coordinating Council, or any suc-  
7           cessor entity;

8           “(F) a representative of the Information  
9           Technology Sector Coordinating Council, or any  
10          successor entity;

11          “(G) individuals, acting in their personal  
12          capacity, with demonstrated technical expertise  
13          in cybersecurity; and

14          “(H) such other individuals as the Director  
15          determines to be appropriate, including owners  
16          of small business concerns (as defined under  
17          section 3 of the Small Business Act (15 U.S.C.  
18          632)).

19          “(2) TERM.—The members of the Council shall  
20          be appointed for 2 year terms and may be appointed  
21          to consecutive terms.

22          “(3) LEADERSHIP.—The Chairperson and Vice-  
23          Chairperson of the Council shall be selected by mem-  
24          bers of the Council from among the members of the  
25          Council and shall serve 2-year terms.

1       “(d) APPLICABILITY OF FEDERAL ADVISORY COM-  
 2 MITTEE ACT.—The Federal Advisory Committee Act (5  
 3 U.S.C. App.) shall not apply to the Council.”.

4 **SEC. 503. PRIORITIZED CRITICAL INFORMATION INFRA-  
 5 STRUCTURE.**

6       Section 210E(a)(2) of the Homeland Security Act of  
 7 2002 (6 U.S.C. 1241(a)(2)) is amended—

8           (1) by striking “In accordance” and inserting  
 9 the following:

10               “(A) IN GENERAL.—In accordance”; and

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

12               “(B) CONSIDERATIONS.—In establishing  
 13 and maintaining a list under subparagraph (A),  
 14 the Secretary, in coordination with the Director  
 15 of the National Center for Cybersecurity and  
 16 Communications and in consultation with the  
 17 National Cybersecurity Advisory Council,  
 18 shall—

19                       “(i) consider cyber vulnerabilities and  
 20 consequences by sector, including—

21                               “(I) the factors listed in section  
 22 248(a)(2);

23                               “(II) interdependencies between  
 24 components of covered critical infra-

1 structure (as defined under section  
2 241); and

3 “(III) any other security related  
4 factor determined appropriate by the  
5 Secretary; and

6 “(ii) add covered critical infrastruc-  
7 ture to or delete covered critical infrastruc-  
8 ture from the list based on the factors list-  
9 ed in clause (i) for purposes of sections  
10 248 and 249.

11 “(C) NOTIFICATION.—The Secretary—

12 “(i) shall notify the owner or operator  
13 of any system or asset added under sub-  
14 paragraph (B)(ii) to the list established  
15 and maintained under subparagraph (A) as  
16 soon as is practicable;

17 “(ii) shall develop a mechanism for an  
18 owner or operator notified under clause (i)  
19 to provide relevant information to the Sec-  
20 retary and the Director of the National  
21 Center for Cybersecurity and Communica-  
22 tions relating to the inclusion of the sys-  
23 tem or asset on the list, including any in-  
24 formation that the owner or operator be-

1           believes may have led to the improper inclu-  
 2           sion of the system or asset on the list; and  
 3           “~~(iii)~~ at the sole and unreviewable dis-  
 4           cretion of the Secretary, may revise the list  
 5           based on information provided in clause  
 6           ~~(ii)~~.”.

7 **SEC. 504. NATIONAL CENTER FOR CYBERSECURITY AND**  
 8           **COMMUNICATIONS ACQUISITION AUTHORI-**  
 9           **TIES.**

10       (a) **IN GENERAL.**—The National Center for Cyberse-  
 11       curity and Communications is authorized to use the au-  
 12       thorities under subsections ~~(e)(1)~~ and ~~(d)(1)(B)~~ of section  
 13       2304 of title 10, United States Code, instead of the au-  
 14       thorities under subsections ~~(e)(1)~~ and ~~(d)(1)(B)~~ of section  
 15       303 of the Federal Property and Administrative Services  
 16       Act of 1949 ~~(41 U.S.C. 253)~~, subject to all other require-  
 17       ments of section 303 of the Federal Property and Admin-  
 18       istrative Services Act of 1949.

19       (b) **GUIDELINES.**—Not later than 90 days after the  
 20       date of enactment of this Act, the chief procurement offi-  
 21       cer of the Department of Homeland Security shall issue  
 22       guidelines for use of the authority under subsection (a).

23       (c) **TERMINATION.**—The National Center for Cyber-  
 24       security and Communications may not use the authority

1 under subsection (a) on and after the date that is 3 years  
2 after the date of enactment of this Act.

3 ~~(d) REPORTING.—~~

4 ~~(1) IN GENERAL.—~~On a semiannual basis, the  
5 Director of the National Center for Cybersecurity  
6 and Communications shall submit a report on use of  
7 the authority granted by subsection (a) to—

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

10 ~~(B) the Committee on Homeland Security~~  
11 ~~of the House of Representatives.~~

12 ~~(2) CONTENTS.—~~Each report submitted under  
13 paragraph ~~(1)~~ shall include, at a minimum—

14 ~~(A) the number of contract actions taken~~  
15 ~~under the authority under subsection (a) during~~  
16 ~~the period covered by the report; and~~

17 ~~(B) for each contract action described in~~  
18 ~~subparagraph (A)—~~

19 ~~(i) the total dollar value of the con-~~  
20 ~~tract action;~~

21 ~~(ii) a summary of the market research~~  
22 ~~conducted by the National Center for Cy-~~  
23 ~~bersecurity and Communications, including~~  
24 ~~a list of all offerors who were considered~~  
25 ~~and those who actually submitted bids, in~~

1 order to determine that use of the author-  
2 ity was appropriate; and

3 (iii) a copy of the justification and ap-  
4 proval documents required by section  
5 303(f) of the Federal Property and Admin-  
6 istrative Services Act of 1949 (41 U.S.C.  
7 253(f)).

8 (3) ~~CLASSIFIED ANNEX~~.—A report submitted  
9 under this subsection shall be submitted in an un-  
10 classified form, but may include a classified annex,  
11 if necessary.

12 **SEC. 505. TECHNICAL AND CONFORMING AMENDMENTS.**

13 (a) ~~ELIMINATION OF ASSISTANT SECRETARY FOR~~  
14 ~~CYBERSECURITY AND COMMUNICATIONS~~.—The Homeland  
15 Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

16 (1) in section 103(a)(8) (6 U.S.C. 113(a)(8)),  
17 by striking “, cybersecurity,”;

18 (2) in section 514 (6 U.S.C. 321e)—

19 (A) by striking subsection (b); and

20 (B) by redesignating subsection (e) as sub-  
21 section (b); and

22 (3) in section 1801(b) (6 U.S.C. 571(b)), by  
23 striking “shall report to the Assistant Secretary for  
24 Cybersecurity and Communications” and inserting

1 “shall report to the Director of the National Center  
2 for Cybersecurity and Communications”.

3 (b) CIO COUNCIL.—Section 3603(b) of title 44,  
4 United States Code, is amended—

5 (1) by redesignating paragraph (7) as para-  
6 graph (8); and

7 (2) by inserting after paragraph (6) the fol-  
8 lowing:

9 “(7) The Director of the National Center for  
10 Cybersecurity and Communications.”.

11 (c) REPEAL.—The Homeland Security Act of 2002  
12 (6 U.S.C. 101 et seq) is amended—

13 (1) by striking section 223 (6 U.S.C. 143); and

14 (2) by redesignating sections 224 and 225 (6  
15 U.S.C. 144 and 145) as sections 223 and 224, re-  
16 spectively.

17 (d) TECHNICAL CORRECTION.—Section 1802(a) of  
18 the Homeland Security Act of 2002 (6 U.S.C. 572(a)) is  
19 amended in the matter preceding paragraph (1) by strik-  
20 ing “Department of”.

21 (e) EXECUTIVE SCHEDULE POSITION.—Section 5313  
22 of title 5, United States Code, is amended by adding at  
23 the end the following:

24 “Director of the National Center for Cybersecurity  
25 and Communications.”.

1 (f) TABLE OF CONTENTS.—The table of contents in  
 2 section 1(b) of the Homeland Security Act of 2002 (6  
 3 U.S.C. 101 et seq.) is amended—

4 (1) by striking the items relating to sections  
 5 ~~223~~, ~~224~~, and ~~225~~ and inserting the following:

“Sec. ~~223~~. NET guard.

“Sec. ~~224~~. Cyber Security Enhancements Act of 2002.”; and

6 (2) by inserting after the item relating to sec-  
 7 tion ~~237~~ the following:

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

“Sec. ~~239~~. National Cybersecurity Advisory Council.

“Subtitle E—Cybersecurity

“Sec. ~~241~~. Definitions.

“Sec. ~~242~~. National Center for Cybersecurity and Communications.

“Sec. ~~243~~. Physical and cyber infrastructure collaboration.

“Sec. ~~244~~. United States Computer Emergency Readiness Team.

“Sec. ~~245~~. Additional authorities of the Director of the National Center for Cy-  
 bersecurity and Communications.

“Sec. ~~246~~. Information sharing.

“Sec. ~~247~~. Private sector assistance.

“Sec. ~~248~~. Cyber vulnerabilities to covered critical infrastructure.

“Sec. ~~249~~. National cyber emergencies.

“Sec. ~~250~~. Enforcement.

“Sec. ~~251~~. Protection of information.

“Sec. ~~252~~. Sector-specific agencies.

“Sec. ~~253~~. Strategy for Federal cybersecurity supply chain management.”.

## 8 **SECTION 1. SHORT TITLE.**

9 *This Act may be cited as the “Protecting Cyberspace*  
 10 *as a National Asset Act of 2010”.*

## 11 **SEC. 2. TABLE OF CONTENTS.**

12 *The table of contents for this Act is as follows:*

*Sec. 1. Short title.*

*Sec. 2. Table of contents.*

*Sec. 3. Definitions.*

### TITLE I—OFFICE OF CYBERSPACE POLICY

*Sec. 101. Establishment of the Office of Cyberspace Policy.*

- Sec. 102. Appointment and responsibilities of the Director.*  
*Sec. 103. Prohibition on political campaigning.*  
*Sec. 104. Review of Federal agency budget requests relating to the National Strategy.*  
*Sec. 105. Access to intelligence.*  
*Sec. 106. Consultation.*  
*Sec. 107. Reports to Congress.*

*TITLE II—NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS*

- Sec. 201. Cybersecurity.*

*TITLE III—FEDERAL INFORMATION SECURITY MANAGEMENT*

- Sec. 301. Coordination of Federal information policy.*

*TITLE IV—RECRUITMENT AND PROFESSIONAL DEVELOPMENT*

- Sec. 401. Definitions.*  
*Sec. 402. Assessment of cybersecurity workforce.*  
*Sec. 403. Strategic cybersecurity workforce planning.*  
*Sec. 404. Cybersecurity occupation classifications.*  
*Sec. 405. Measures of cybersecurity hiring effectiveness.*  
*Sec. 406. Training and education.*  
*Sec. 407. Cybersecurity incentives.*  
*Sec. 408. Recruitment and retention program for the National Center for Cybersecurity and Communications.*

*TITLE V—OTHER PROVISIONS*

- Sec. 501. Cybersecurity research and development.*  
*Sec. 502. Prioritized critical information infrastructure.*  
*Sec. 503. National Center for Cybersecurity and Communications acquisition authorities.*  
*Sec. 504. Evaluation of the effective implementation of Office of Management and Budget information security related policies and directives.*  
*Sec. 505. Technical and conforming amendments.*

**1 SEC. 3. DEFINITIONS.**

**2       *In this Act:***

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

**6                               (A) the Committee on Homeland Security**  
**7                               and Governmental Affairs of the Senate;**

1           (B) *the Committee on Homeland Security of*  
2           *the House of Representatives;*

3           (C) *the Committee on Oversight and Gov-*  
4           *ernment Reform of the House of Representatives;*  
5           *and*

6           (D) *any other congressional committee with*  
7           *jurisdiction over the particular matter.*

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

12           (3) *CYBERSPACE.—The term “cyberspace” means*  
13           *the interdependent network of information infrastruc-*  
14           *ture, and includes the Internet, telecommunications*  
15           *networks, computer systems, and embedded processors*  
16           *and controllers in critical industries.*

17           (4) *DIRECTOR.—The term “Director” means the*  
18           *Director of Cyberspace Policy established under sec-*  
19           *tion 101.*

20           (5) *FEDERAL AGENCY.—The term “Federal agen-*  
21           *cy”—*

22           (A) *means any executive department, Gov-*  
23           *ernment corporation, Government controlled cor-*  
24           *poration, or other establishment in the executive*  
25           *branch of the Government (including the Execu-*

1           *tive Office of the President), or any independent*  
2           *regulatory agency; and*

3           *(B) does not include the governments of the*  
4           *District of Columbia and of the territories and*  
5           *possessions of the United States and their var-*  
6           *ious subdivisions.*

7           (6) *FEDERAL INFORMATION INFRASTRUCTURE.*—  
8           *The term “Federal information infrastructure”—*

9           *(A) means information infrastructure that*  
10           *is owned, operated, controlled, or licensed for use*  
11           *by, or on behalf of, any Federal agency, includ-*  
12           *ing information systems used or operated by an-*  
13           *other entity on behalf of a Federal agency; and*

14           *(B) does not include—*

15           *(i) a national security system; or*

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

21           (7) *INCIDENT.*—*The term “incident” has the*  
22           *meaning given that term in section 3551 of title 44,*  
23           *United States Code, as added by this Act.*

24           (8) *INFORMATION INFRASTRUCTURE.*—*The term*  
25           *“information infrastructure” means the underlying*

1 *framework that information systems and assets rely*  
2 *on to process, transmit, receive, or store information*  
3 *electronically, including programmable electronic de-*  
4 *vices and communications networks and any associ-*  
5 *ated hardware, software, or data.*

6 (9) *INFORMATION SECURITY.*—*The term “infor-*  
7 *mation security” means protecting information and*  
8 *information systems from disruption or unauthorized*  
9 *access, use, disclosure, modification, or destruction in*  
10 *order to provide—*

11 (A) *integrity, by guarding against im-*  
12 *proper information modification or destruction,*  
13 *including by ensuring information nonrepudi-*  
14 *ation and authenticity;*

15 (B) *confidentiality, by preserving author-*  
16 *ized restrictions on access and disclosure, includ-*  
17 *ing means for protecting personal privacy and*  
18 *proprietary information; and*

19 (C) *availability, by ensuring timely and re-*  
20 *liable access to and use of information.*

21 (10) *INFORMATION TECHNOLOGY.*—*The term “in-*  
22 *formation technology” has the meaning given that*  
23 *term in section 11101 of title 40, United States Code.*

24 (11) *INTELLIGENCE COMMUNITY.*—*The term “in-*  
25 *telligence community” has the meaning given that*

1 *term under section 3(4) of the National Security Act*  
2 *of 1947 (50 U.S.C. 401a(4)).*

3 (12) *KEY RESOURCES.*—*The term “key re-*  
4 *sources” has the meaning given that term in section*  
5 *2 of the Homeland Security Act of 2002 (6 U.S.C.*  
6 *101)*

7 (13) *NATIONAL CENTER FOR CYBERSECURITY*  
8 *AND COMMUNICATIONS.*—*The term “National Center*  
9 *for Cybersecurity and Communications” means the*  
10 *National Center for Cybersecurity and Communica-*  
11 *tions established under section 242(a) of the Home-*  
12 *land Security Act of 2002, as added by this Act.*

13 (14) *NATIONAL INFORMATION INFRASTRUC-*  
14 *TURE.*—*The term “national information infrastruc-*  
15 *ture” means information infrastructure—*

16 (A) *that is owned, operated, or controlled*  
17 *within or from the United States; and*

18 (B) *that is not owned, operated, controlled,*  
19 *or licensed for use by a Federal agency.*

20 (15) *NATIONAL SECURITY SYSTEM.*—*The term*  
21 *“national security system” has the meaning given*  
22 *that term in section 3551 of title 44, United States*  
23 *Code, as added by this Act.*

24 (16) *NATIONAL STRATEGY.*—*The term “National*  
25 *Strategy” means the national strategy to increase the*

1       *security and resiliency of cyberspace developed under*  
2       *section 101(a)(1).*

3               (17) *OFFICE.*—*The term “Office” means the Of-*  
4       *fice of Cyberspace Policy established under section*  
5       *101.*

6               (18) *RESILIENCY.*—*The term “resiliency” means*  
7       *the ability to eliminate or reduce the magnitude or*  
8       *duration of a disruptive event, including the ability*  
9       *to prevent, prepare for, respond to, and recover from*  
10       *the event.*

11              (19) *RISK.*—*The term “risk” means the potential*  
12       *for an unwanted outcome resulting from an incident,*  
13       *as determined by the likelihood of the occurrence of*  
14       *the incident and the associated consequences, includ-*  
15       *ing potential for an adverse outcome assessed as a*  
16       *function of threats, vulnerabilities, and consequences*  
17       *associated with an incident.*

18              (20) *RISK-BASED SECURITY.*—*The term “risk-*  
19       *based security” has the meaning given that term in*  
20       *section 3551 of title 44, United States Code, as added*  
21       *by this Act.*

1                   **TITLE I—OFFICE OF**  
2                   **CYBERSPACE POLICY**

3   **SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBERSPACE**  
4                   **POLICY.**

5           (a) *ESTABLISHMENT OF OFFICE.*—*There is established*  
6 *in the Executive Office of the President an Office of Cyber-*  
7 *space Policy which shall—*

8                   (1) *develop, not later than 1 year after the date*  
9 *of enactment of this Act, and update as needed, but*  
10 *not less frequently than once every 2 years, a national*  
11 *strategy to increase the security and resiliency of*  
12 *cyberspace, that includes goals and objectives relating*  
13 *to—*

14                           (A) *computer network operations, including*  
15 *offensive activities, defensive activities, and other*  
16 *activities;*

17                           (B) *information assurance;*

18                           (C) *protection of critical infrastructure and*  
19 *key resources;*

20                           (D) *research and development priorities;*

21                           (E) *law enforcement;*

22                           (F) *diplomacy;*

23                           (G) *homeland security;*

24                           (H) *protection of privacy and civil liberties;*

25                           (I) *military and intelligence activities; and*

1           *(J) identity management and authentica-*  
2           *tion;*

3           *(2) oversee, coordinate, and integrate all policies*  
4           *and activities of the Federal Government across all*  
5           *instruments of national power relating to ensuring*  
6           *the security and resiliency of cyberspace, including—*

7           *(A) diplomatic, economic, military, intel-*  
8           *ligence, homeland security, and law enforcement*  
9           *policies and activities within and among Federal*  
10          *agencies; and*

11          *(B) offensive activities, defensive activities,*  
12          *and other policies and activities necessary to en-*  
13          *sure effective capabilities to operate in cyber-*  
14          *space;*

15          *(3) ensure that all Federal agencies comply with*  
16          *appropriate guidelines, policies, and directives from*  
17          *the Department of Homeland Security, other Federal*  
18          *agencies with responsibilities relating to cyberspace*  
19          *security or resiliency, and the National Center for*  
20          *Cybersecurity and Communications; and*

21          *(4) ensure that Federal agencies have access to,*  
22          *receive, and appropriately disseminate law enforce-*  
23          *ment information, intelligence information, terrorism*  
24          *information, and any other information (including*  
25          *information relating to incidents provided under sub-*

1 sections (a)(4) and (c) of section 246 of the Homeland  
2 Security Act of 2002, as added by this Act) relevant  
3 to—

4 (A) the security of the Federal information  
5 infrastructure or the national information infra-  
6 structure; and

7 (B) the security of—

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

13 (ii) a national security system.

14 (b) *DIRECTOR OF CYBERSPACE POLICY.*—

15 (1) *IN GENERAL.*—There shall be a Director of  
16 Cyberspace Policy, who shall be the head of the Office.

17 (2) *EXECUTIVE SCHEDULE POSITION.*—Section  
18 5312 of title 5, United States Code, is amended by  
19 adding at the end the following:

20 “Director of Cyberspace Policy.”.

21 **SEC. 102. APPOINTMENT AND RESPONSIBILITIES OF THE**  
22 **DIRECTOR.**

23 (a) *APPOINTMENT.*—

1           (1) *IN GENERAL.*—*The Director shall be ap-*  
2           *pointed by the President, by and with the advice and*  
3           *consent of the Senate.*

4           (2) *QUALIFICATIONS.*—*The President shall ap-*  
5           *point the Director from among individuals who have*  
6           *demonstrated ability and knowledge in information*  
7           *technology, cybersecurity, and the operations, secu-*  
8           *rity, and resiliency of communications networks.*

9           (3) *PROHIBITION.*—*No person shall serve as Di-*  
10          *rector while serving in any other position in the Fed-*  
11          *eral Government.*

12          (b) *RESPONSIBILITIES.*—*The Director shall—*

13                 (1) *advise the President regarding the establish-*  
14                 *ment of policies, goals, objectives, and priorities for*  
15                 *securing the information infrastructure of the Nation;*

16                 (2) *advise the President and other entities within*  
17                 *the Executive Office of the President regarding mecha-*  
18                 *nisms to build, and improve the resiliency and effi-*  
19                 *ciency of, the information and communication indus-*  
20                 *try of the Nation, in collaboration with the private*  
21                 *sector, while promoting national economic interests;*

22                 (3) *work with Federal agencies to—*

23                         (A) *oversee, coordinate, and integrate the*  
24                         *implementation of the National Strategy, includ-*  
25                         *ing coordination with—*

- 1                   (i) the Department of Homeland Secu-  
2                   rity;
- 3                   (ii) the Department of Defense;
- 4                   (iii) the Department of Commerce;
- 5                   (iv) the Department of State;
- 6                   (v) the Department of Justice;
- 7                   (vi) the Department of Energy;
- 8                   (vii) through the Director of National  
9                   Intelligence, the intelligence community;  
10                  and
- 11                  (viii) and any other Federal agency  
12                  with responsibilities relating to the Na-  
13                  tional Strategy; and
- 14                  (B) resolve any disputes that arise between  
15                  Federal agencies relating to the National Strat-  
16                  egy or other matters within the responsibility of  
17                  the Office;
- 18                  (4) if the policies or activities of a Federal agen-  
19                  cy are not in compliance with the responsibilities of  
20                  the Federal agency under the National Strategy—
- 21                       (A) notify the Federal agency;
- 22                       (B) transmit a copy of each notification  
23                       under subparagraph (A) to the President and the  
24                       appropriate congressional committees; and

1           (C) coordinate the efforts to bring the Fed-  
2           eral agency into compliance;

3           (5) ensure the adequacy of protections for pri-  
4           vacy and civil liberties in carrying out the respon-  
5           sibilities of the Director under this title, including  
6           through consultation with the Privacy and Civil Lib-  
7           erties Oversight Board established under section 1061  
8           of the National Security Intelligence Reform Act of  
9           2004 (42 U.S.C. 2000ee);

10          (6) upon reasonable request, appear before any  
11          duly constituted committees of the Senate or of the  
12          House of Representatives;

13          (7) recommend to the Office of Management and  
14          Budget or the head of a Federal agency actions (in-  
15          cluding requests to Congress relating to the re-  
16          programming of funds) that the Director determines  
17          are necessary to ensure risk-based security of—

18                (A) the Federal information infrastructure;

19                (B) information infrastructure that is  
20                owned, operated, controlled, or licensed for use  
21                by, or on behalf of, the Department of Defense,  
22                a military department, or another element of the  
23                intelligence community; or

24                (C) a national security system;

1           (8) *advise the Administrator of the Office of E-*  
2           *Government and Information Technology and the Ad-*  
3           *ministrator of the Office of Information and Regu-*  
4           *latory Affairs on the development, and oversee the im-*  
5           *plementation, of policies, principles, standards, guide-*  
6           *lines, and budget priorities for information technology*  
7           *functions and activities of the Federal Government;*

8           (9) *coordinate and ensure, to the maximum ex-*  
9           *tent practicable, that the standards and guidelines de-*  
10          *veloped for national security systems and the stand-*  
11          *ards and guidelines under section 20 of the National*  
12          *Institute of Standards and Technology Act (15 U.S.C.*  
13          *278g-3) are complementary and unified;*

14          (10) *in consultation with the Administrator of*  
15          *the Office of Information and Regulatory Affairs, co-*  
16          *ordinate efforts of Federal agencies relating to the de-*  
17          *velopment of regulations, rules, requirements, or other*  
18          *actions applicable to the national information infra-*  
19          *structure to ensure, to the maximum extent prac-*  
20          *ticable, that the efforts are complementary;*

21          (11) *coordinate the activities of the Office of*  
22          *Science and Technology Policy, the National Eco-*  
23          *nomical Council, the Office of Management and Budget,*  
24          *the National Security Council, the Homeland Secu-*  
25          *rity Council, and the United States Trade Represent-*

1        *ative related to the National Strategy and other mat-*  
 2        *ters within the purview of the Office;*

3            *(12) carry out the responsibilities for national*  
 4        *security and emergency preparedness communications*  
 5        *described in section 706 of the Communications Act*  
 6        *of 1934 (47 U.S.C. 606) to ensure integration and co-*  
 7        *ordination; and*

8            *(13) as assigned by the President, other duties*  
 9        *relating to the security and resiliency of cyberspace.*

10        *(c) CONFORMING REGULATIONS AND ORDERS.—The*  
 11        *President shall amend the regulations and orders issued*  
 12        *under section 706 of the Communications Act of 1934 (47*  
 13        *U.S.C. 606) in accordance with subsection (b)(12).*

14        **SEC. 103. PROHIBITION ON POLITICAL CAMPAIGNING.**

15        *Section 7323(b)(2)(B) of title 5, United States Code,*  
 16        *is amended—*

17            *(1) in clause (i), by striking “or” at the end;*

18            *(2) in clause (ii), by striking the period at the*  
 19        *end and inserting “; or”; and*

20            *(3) by adding at the end the following:*

21                    *“(iii) notwithstanding the exception*  
 22                    *under subparagraph (A) (relating to an ap-*  
 23                    *pointment made by the President, by and*  
 24                    *with the advice and consent of the Senate),*  
 25                    *the Director of Cyberspace Policy.”.*

1 **SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET REQUESTS**  
2 **RELATING TO THE NATIONAL STRATEGY.**

3 (a) *IN GENERAL.*—For each fiscal year, the head of  
4 each Federal agency shall transmit to the Director a copy  
5 of any portion of the budget of the Federal agency intended  
6 to implement the National Strategy at the same time as  
7 that budget request is submitted to the Office of Manage-  
8 ment and Budget in the preparation of the budget of the  
9 President submitted to Congress under section 1105 (a) of  
10 title 31, United States Code.

11 (b) *TIMELY SUBMISSIONS.*—The head of each Federal  
12 agency shall ensure the timely development and submission  
13 to the Director of each proposed budget under this section,  
14 in such format as may be designated by the Director with  
15 the concurrence of the Director of the Office of Management  
16 and Budget.

17 (c) *ADEQUACY OF THE PROPOSED BUDGET RE-*  
18 *QUESTS.*—With the assistance of, and in coordination with,  
19 the Office of E-Government and Information Technology  
20 and the National Center for Cybersecurity and Communica-  
21 tions, the Director shall review each budget submission to  
22 assess the adequacy of the proposed request with regard to  
23 implementation of the National Strategy, including the  
24 overall sufficiency of the requests to implement effectively  
25 the National Strategy across all Federal agencies.

1           (d) *INADEQUATE BUDGET REQUESTS.*—*If the Director*  
2 *concludes that a budget request submitted under subsection*  
3 *(a) is inadequate, in whole or in part, to implement the*  
4 *objectives of the National Strategy, the Director shall sub-*  
5 *mit to the Director of the Office of Management and Budget*  
6 *and the head of the Federal agency submitting the budget*  
7 *request a written description of funding levels and specific*  
8 *initiatives that would, in the determination of the Director,*  
9 *make the request adequate.*

10 **SEC. 105. ACCESS TO INTELLIGENCE.**

11           *The Director shall have access to law enforcement in-*  
12 *formation, intelligence information, terrorism information,*  
13 *and any other information (including information relating*  
14 *to incidents provided under subsections (a)(4) and (c) of*  
15 *section 246 of the Homeland Security Act of 2002, as added*  
16 *by this Act) that is obtained by, or in the possession of,*  
17 *any Federal agency that the Director determines relevant*  
18 *to the security of—*

19                   (1) *the Federal information infrastructure;*

20                   (2) *information infrastructure that is owned, op-*  
21 *erated, controlled, or licensed for use by, or on behalf*  
22 *of, the Department of Defense, a military department,*  
23 *or another element of the intelligence community;*

24                   (3) *a national security system; or*

25                   (4) *national information infrastructure.*

1 **SEC. 106. CONSULTATION.**

2 (a) *IN GENERAL.*—*The Director may consult and ob-*  
3 *tain recommendations from, as needed, such Presidential*  
4 *and other advisory entities as the Director determines will*  
5 *assist in carrying out the mission of the Office, including—*

6 (1) *the National Security Telecommunications*  
7 *Advisory Committee;*

8 (2) *the National Infrastructure Advisory Coun-*  
9 *cil;*

10 (3) *the Privacy and Civil Liberties Oversight*  
11 *Board;*

12 (4) *the President’s Intelligence Advisory Board;*

13 (5) *the Critical Infrastructure Partnership Advi-*  
14 *sory Council;*

15 (6) *the Committee on Foreign Investment in the*  
16 *United States;*

17 (7) *the Information Security and Privacy Advi-*  
18 *sory Board;*

19 (8) *the National Cybersecurity Advisory Council*  
20 *established under section 239 of the Homeland Secu-*  
21 *rity Act of 2002, as added by this Act; and*

22 (9) *any other entity that may provide assistance*  
23 *to the Director.*

24 (b) *NATIONAL STRATEGY.*—*In developing and updat-*  
25 *ing the National Strategy the Director shall consult with*

1 *the National Cybersecurity Advisory Council and, as ap-*  
 2 *propriate, State and local governments and private entities.*

3 **SEC. 107. REPORTS TO CONGRESS.**

4 (a) *IN GENERAL.*—*The Director shall submit an an-*  
 5 *nual report to the appropriate congressional committees de-*  
 6 *scribing the activities, ongoing projects, and plans of the*  
 7 *Federal Government designed to meet the goals and objec-*  
 8 *tives of the National Strategy.*

9 (b) *CLASSIFIED ANNEX.*—*A report submitted under*  
 10 *this section shall be submitted in an unclassified form, but*  
 11 *may include a classified annex, if necessary.*

12 (c) *PUBLIC REPORT.*—*An unclassified version of each*  
 13 *report submitted under this section shall be made available*  
 14 *to the public.*

15 **TITLE II—NATIONAL CENTER**  
 16 **FOR CYBERSECURITY AND**  
 17 **COMMUNICATIONS**

18 **SEC. 201. CYBERSECURITY.**

19 *Title II of the Homeland Security Act of 2002 (6*  
 20 *U.S.C. 121 et seq.) is amended by adding at the end the*  
 21 *following:*

22 **“Subtitle E—Cybersecurity**

23 **“SEC. 241. DEFINITIONS.**

24 *“In this subtitle—*

1           “(1) the term ‘agency information infrastructure’  
2           means the Federal information infrastructure of a  
3           particular Federal agency;

4           “(2) the term ‘appropriate committees of Con-  
5           gress’ means the Committee on Homeland Security  
6           and Governmental Affairs of the Senate and the Com-  
7           mittee on Homeland Security of the House of Rep-  
8           resentatives;

9           “(3) the term ‘Center’ means the National Center  
10          for Cybersecurity and Communications established  
11          under section 242(a);

12          “(4) the term ‘covered critical infrastructure’  
13          means a system or asset identified by the Secretary  
14          as covered critical infrastructure under section 254;

15          “(5) the term ‘cyber risk’ means any risk to in-  
16          formation infrastructure, including physical or per-  
17          sonnel risks and security vulnerabilities, that, if ex-  
18          ploited or not mitigated, could pose a significant risk  
19          of disruption to the operation of information infra-  
20          structure essential to the reliable operation of covered  
21          critical infrastructure;

22          “(6) the term ‘Director’ means the Director of the  
23          Center appointed under section 242(b)(1);

24          “(7) the term ‘Federal agency’—

1           “(A) means any executive department, mili-  
2           tary department, Government corporation, Gov-  
3           ernment controlled corporation, or other estab-  
4           lishment in the executive branch of the Govern-  
5           ment (including the Executive Office of the  
6           President), or any independent regulatory agen-  
7           cy; and

8           “(B) does not include the governments of the  
9           District of Columbia and of the territories and  
10          possessions of the United States and their var-  
11          ious subdivisions;

12          “(8) the term ‘Federal information infrastruc-  
13          ture’—

14               “(A) means information infrastructure that  
15               is owned, operated, controlled, or licensed for use  
16               by, or on behalf of, any Federal agency, includ-  
17               ing information systems used or operated by an-  
18               other entity on behalf of a Federal agency; and

19               “(B) does not include—

20                       “(i) a national security system; or

21                       “(ii) information infrastructure that is  
22                       owned, operated, controlled, or licensed for  
23                       use by, or on behalf of, the Department of  
24                       Defense, a military department, or another  
25                       element of the intelligence community;

1           “(9) the term ‘incident’ has the meaning given  
2 that term in section 3551 of title 44, United States  
3 Code;

4           “(10) the term ‘information infrastructure’  
5 means the underlying framework that information  
6 systems and assets rely on to process, transmit, re-  
7 ceive, or store information electronically, including—

8                   “(A) programmable electronic devices and  
9                   communications networks; and

10                   “(B) any associated hardware, software, or  
11                   data;

12           “(11) the term ‘information security’ means pro-  
13 tecting information and information systems from  
14 disruption or unauthorized access, use, disclosure,  
15 modification, or destruction in order to provide—

16                   “(A) integrity, by guarding against im-  
17                   proper information modification or destruction,  
18                   including by ensuring information nonrepudi-  
19                   ation and authenticity;

20                   “(B) confidentiality, by preserving author-  
21                   ized restrictions on access and disclosure, includ-  
22                   ing means for protecting personal privacy and  
23                   proprietary information; and

24                   “(C) availability, by ensuring timely and  
25                   reliable access to and use of information;

1           “(12) the term ‘information sharing and anal-  
2           ysis center’ means a self-governed forum whose mem-  
3           bers work together within a specific sector of critical  
4           infrastructure to identify, analyze, and share with  
5           other members and the Federal Government critical  
6           information relating to threats, vulnerabilities, or in-  
7           cidents to the security and resiliency of the critical  
8           infrastructure that comprises the specific sector;

9           “(13) the term ‘information system’ has the  
10          meaning given that term in section 3502 of title 44,  
11          United States Code;

12          “(14) the term ‘intelligence community’ has the  
13          meaning given that term in section 3(4) of the Na-  
14          tional Security Act of 1947 (50 U.S.C. 401a(4));

15          “(15) the term ‘management controls’ means  
16          safeguards or countermeasures for an information  
17          system that focus on the management of risk and the  
18          management of information system security;

19          “(16) the term ‘National Cybersecurity Advisory  
20          Council’ means the National Cybersecurity Advisory  
21          Council established under section 239;

22          “(17) the term ‘national cyber emergency’ means  
23          an actual or imminent action by any individual or  
24          entity to exploit a cyber risk in a manner that dis-  
25          rupts, attempts to disrupt, or poses a significant risk

1       *of disruption to the operation of the information in-*  
2       *frastructure essential to the reliable operation of cov-*  
3       *ered critical infrastructure;*

4               “(18) the term ‘national information infrastruc-

5       *ture’ means information infrastructure—*

6                       “(A) that is owned, operated, or controlled

7       *within or from the United States; and*

8                       “(B) that is not owned, operated, controlled,

9       *or licensed for use by a Federal agency;*

10               “(19) the term ‘national security system’ has the

11       *meaning given that term in section 3551 of title 44,*

12       *United States Code;*

13               “(20) the term ‘operational controls’ means the

14       *safeguards and countermeasures for an information*

15       *system that are primarily implemented and executed*

16       *by individuals not systems;*

17               “(21) the term ‘sector-specific agency’ means the

18       *relevant Federal agency responsible for infrastructure*

19       *protection activities in a designated critical infra-*

20       *structure sector or key resources category under the*

21       *National Infrastructure Protection Plan, or any other*

22       *appropriate Federal agency identified by the Presi-*

23       *dent after the date of enactment of this subtitle;*

24               “(22) the term ‘sector coordinating councils’

25       *means self-governed councils that are composed of rep-*

1        *representatives of key stakeholders within a specific sec-*  
2        *tor of critical infrastructure that serve as the prin-*  
3        *cipal private sector policy coordination and planning*  
4        *entities with the Federal Government relating to the*  
5        *security and resiliency of the critical infrastructure*  
6        *that comprise that sector;*

7                *“(23) the term ‘security controls’ means the*  
8        *management, operational, and technical controls pre-*  
9        *scribed for an information system to protect the infor-*  
10        *mation security of the system;*

11                *“(24) the term ‘small business concern’ has the*  
12        *meaning given that term under section 3 of the Small*  
13        *Business Act (15 U.S.C. 632);*

14                *“(25) the term ‘technical controls’ means the*  
15        *safeguards or countermeasures for an information*  
16        *system that are primarily implemented and executed*  
17        *by the information system through mechanisms con-*  
18        *tained in the hardware, software, or firmware compo-*  
19        *nents of the system;*

20                *“(26) the term ‘terrorism information’ has the*  
21        *meaning given that term in section 1016 of the Intel-*  
22        *ligence Reform and Terrorism Prevention Act of 2004*  
23        *(6 U.S.C. 485);*

24                *“(27) the term ‘United States person’ has the*  
25        *meaning given that term in section 101 of the Foreign*

1 *Intelligence Surveillance Act of 1978 (50 U.S.C.*  
2 *1801); and*

3 “(28) *the term ‘US-CERT’ means the United*  
4 *States Computer Emergency Readiness Team estab-*  
5 *lished under section 244.*

6 **“SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND**  
7 **COMMUNICATIONS.**

8 “(a) *ESTABLISHMENT.—*

9 “(1) *IN GENERAL.—There is established within*  
10 *the Department a National Center for Cybersecurity*  
11 *and Communications.*

12 “(2) *OPERATIONAL ENTITY.—The Center may—*

13 “(A) *enter into contracts for the procure-*  
14 *ment of property and services for the Center; and*

15 “(B) *appoint employees of the Center in ac-*  
16 *cordance with the civil service laws of the United*  
17 *States.*

18 “(b) *DIRECTOR.—*

19 “(1) *IN GENERAL.—The Center shall be headed*  
20 *by a Director, who shall be appointed by the Presi-*  
21 *dent, by and with the advice and consent of the Sen-*  
22 *ate.*

23 “(2) *REPORTING TO SECRETARY.—The Director*  
24 *shall report directly to the Secretary and serve as the*  
25 *principal advisor to the Secretary on cybersecurity*

1       *and the operations, security, and resiliency of the in-*  
2       *formation infrastructure and communications infra-*  
3       *structure of the United States.*

4               “(3) *PRESIDENTIAL ADVICE.*—*The Director shall*  
5       *regularly advise the President on the exercise of the*  
6       *authorities provided under this subtitle or any other*  
7       *provision of law relating to the security of the Federal*  
8       *information infrastructure or an agency information*  
9       *infrastructure.*

10              “(4) *QUALIFICATIONS.*—*The Director shall be*  
11       *appointed from among individuals who have—*

12                      “(A) *a demonstrated ability in and knowl-*  
13       *edge of information technology, cybersecurity,*  
14       *and the operations, security and resiliency of*  
15       *communications networks; and*

16                      “(B) *significant executive leadership and*  
17       *management experience in the public or private*  
18       *sector.*

19              “(5) *LIMITATION ON SERVICE.*—

20                      “(A) *IN GENERAL.*—*Subject to subpara-*  
21       *graph (B), the individual serving as the Director*  
22       *may not, while so serving, serve in any other ca-*  
23       *capacity in the Federal Government, except to the*  
24       *extent that the individual serving as Director is*  
25       *doing so in an acting capacity.*

1           “(B) *EXCEPTION.*—*The Director may serve*  
2           *on any commission, board, council, or similar*  
3           *entity with responsibilities or duties relating to*  
4           *cybersecurity or the operations, security, and re-*  
5           *siliency of the information infrastructure and*  
6           *communications infrastructure of the United*  
7           *States at the direction of the President or as oth-*  
8           *erwise provided by law.*

9           “(c) *DEPUTY DIRECTORS.*—

10           “(1) *IN GENERAL.*—*There shall be not less than*  
11           *2 Deputy Directors for the Center, who shall report*  
12           *to the Director.*

13           “(2) *INFRASTRUCTURE PROTECTION.*—

14           “(A) *APPOINTMENT.*—*There shall be a Dep-*  
15           *uty Director appointed by the Secretary, who*  
16           *shall have expertise in infrastructure protection.*

17           “(B) *RESPONSIBILITIES.*—*The Deputy Di-*  
18           *rector appointed under subparagraph (A)*  
19           *shall—*

20           “(i) *assist the Director and the Assist-*  
21           *ant Secretary for Infrastructure Protection*  
22           *in coordinating, managing, and directing*  
23           *the information, communications, and*  
24           *physical infrastructure protection respon-*  
25           *sibilities and activities of the Department,*

1           *including activities under Homeland Secu-*  
2           *rity Presidential Directive–7, or any suc-*  
3           *cessor thereto, and the National Infrastruc-*  
4           *ture Protection Plan, or any successor there-*  
5           *to;*

6           “(ii) *review the budget for the Center*  
7           *and the Office of Infrastructure Protection*  
8           *before submission of the budget to the Sec-*  
9           *retary to ensure that activities are appro-*  
10          *priately coordinated;*

11          “(iii) *develop, update periodically, and*  
12          *submit to the appropriate committees of*  
13          *Congress a strategic plan detailing how*  
14          *critical infrastructure protection activities*  
15          *will be coordinated between the Center, the*  
16          *Office of Infrastructure Protection, and the*  
17          *private sector;*

18          “(iv) *subject to the direction of the Di-*  
19          *rector resolve conflicts between the Center*  
20          *and the Office of Infrastructure Protection*  
21          *relating to the information, communica-*  
22          *tions, and physical infrastructure protection*  
23          *responsibilities of the Center and the Office*  
24          *of Infrastructure Protection; and*

1                   “(v) perform such other duties as the  
2                   Director may assign.

3                   “(C) ANNUAL EVALUATION.—The Assistant  
4                   Secretary for Infrastructure Protection shall sub-  
5                   mit annually to the Director an evaluation of  
6                   the performance of the Deputy Director ap-  
7                   pointed under subparagraph (A).

8                   “(3) INTELLIGENCE COMMUNITY.—The Director  
9                   of National Intelligence shall identify an employee of  
10                  an element of the intelligence community to serve as  
11                  a Deputy Director of the Center. The employee shall  
12                  be detailed to the Center on a reimbursable basis for  
13                  such period as is agreed to by the Director and the  
14                  Director of National Intelligence, and, while serving  
15                  as Deputy Director, shall report directly to the Direc-  
16                  tor of the Center.

17                  “(d) LIAISON OFFICERS.—

18                  “(1) IN GENERAL.—The Secretary of Defense, the  
19                  Attorney General, the Secretary of Commerce, and the  
20                  Director of National Intelligence shall detail per-  
21                  sonnel to the Center to act as full-time liaisons with  
22                  the Department of Defense, the Department of Justice,  
23                  the National Institute of Standards and Technology,  
24                  and elements of the intelligence community to assist  
25                  in coordination between and among the Center, the

1 *Department of Defense, the Department of Justice, the*  
2 *National Institute of Standards and Technology, and*  
3 *elements of the intelligence community.*

4 “(2) *PRIVATE SECTOR.*—

5 “(A) *IN GENERAL.*—*Consistent with appli-*  
6 *cable law and ethics requirements, and except as*  
7 *provided in subparagraph (B), the Director may*  
8 *authorize representatives from private sector en-*  
9 *tities to participate in the activities of the Center*  
10 *to improve the information sharing, analysis,*  
11 *and coordination of activities of the US-CERT.*

12 “(B) *LIMITATION.*—*A representative from a*  
13 *private sector entity authorized to participate in*  
14 *the activities of the Center under subparagraph*  
15 *(A) may not participate in any activities of the*  
16 *Center under section 248, 249, or 250.*

17 “(e) *PRIVACY OFFICER.*—

18 “(1) *IN GENERAL.*—*The Director, in consultation*  
19 *with the Secretary, shall designate a full-time privacy*  
20 *officer, who shall report to the Director.*

21 “(2) *DUTIES.*—*The privacy officer designated*  
22 *under paragraph (1) shall have primary responsi-*  
23 *bility for implementation by the Center of the privacy*  
24 *policy for the Department established by the Privacy*  
25 *Officer appointed under section 222.*

1       “(f) *DUTIES OF DIRECTOR.*—

2               “(1) *IN GENERAL.*—*The Director shall—*

3                       “(A) *working cooperatively with the private*  
4                       *sector, lead the Federal effort to secure, protect,*  
5                       *and ensure the resiliency of the Federal informa-*  
6                       *tion infrastructure, national information infra-*  
7                       *structure, and communications infrastructure of*  
8                       *the United States, including communications*  
9                       *networks;*

10                      “(B) *assist in the identification, remedi-*  
11                      *ation, and mitigation of vulnerabilities to the*  
12                      *Federal information infrastructure and the na-*  
13                      *tional information infrastructure;*

14                      “(C) *provide dynamic, comprehensive, and*  
15                      *continuous situational awareness of the security*  
16                      *status of the Federal information infrastructure,*  
17                      *national information infrastructure, information*  
18                      *infrastructure that is owned, operated, con-*  
19                      *trolled, or licensed for use by, or on behalf of, the*  
20                      *Department of Defense, a military department,*  
21                      *or another element of the intelligence community,*  
22                      *and information infrastructure located outside*  
23                      *the United States the disruption of which could*  
24                      *result in national or regional catastrophic dam-*  
25                      *age in the United States by sharing and inte-*

1           *grating classified and unclassified information,*  
2           *including information relating to threats,*  
3           *vulnerabilities, traffic, trends, incidents, and*  
4           *other anomalous activities affecting the infra-*  
5           *structure or systems, on a routine and contin-*  
6           *uous basis with—*

7                   “(i) *the National Threat Operations*  
8                   *Center of the National Security Agency;*

9                   “(ii) *the United States Cyber Com-*  
10                  *mand, including the Joint Task Force-Glob-*  
11                  *al Network Operations;*

12                  “(iii) *the Cyber Crime Center of the*  
13                  *Department of Defense;*

14                  “(iv) *the National Cyber Investigative*  
15                  *Joint Task Force;*

16                  “(v) *the Intelligence Community Inci-*  
17                  *dent Response Center;*

18                  “(vi) *any other Federal agency, or*  
19                  *component thereof, identified by the Direc-*  
20                  *tor; and*

21                  “(vii) *any non-Federal entity, includ-*  
22                  *ing, where appropriate, information shar-*  
23                  *ing and analysis centers, identified by the*  
24                  *Director, with the concurrence of the owner*

1            *or operator of that entity and consistent*  
2            *with applicable law;*

3            *“(D) work with the entities described in*  
4            *subparagraph (C) to establish policies and proce-*  
5            *dures that enable information sharing between*  
6            *and among the entities;*

7            *“(E)(i) develop, in coordination with the*  
8            *Assistant Secretary for Infrastructure Protection,*  
9            *other Federal agencies, the private sector, and*  
10           *State and local governments, a national incident*  
11           *response plan that details the roles of Federal*  
12           *agencies, State and local governments, and the*  
13           *private sector, including plans to be executed in*  
14           *response to a declaration of a national cyber*  
15           *emergency by the President under section 249;*  
16           *and*

17           *“(i) establish mechanisms for assisting*  
18           *owners or operators of critical infrastructure, in-*  
19           *cluding covered critical infrastructure, in the de-*  
20           *ployment of emergency measures or other ac-*  
21           *tions, including measures to restore the critical*  
22           *infrastructure in the event of the destruction or*  
23           *a serious disruption of the critical infrastruc-*  
24           *ture;*

1           “(F) conduct risk-based assessments of the  
2           Federal information infrastructure with respect  
3           to acts of terrorism, natural disasters, and other  
4           large-scale disruptions and provide the results of  
5           the assessments to the Director of Cyberspace  
6           Policy and to affected Federal agencies;

7           “(G) develop, oversee the implementation of,  
8           and enforce policies, principles, and guidelines  
9           on information security for the Federal informa-  
10          tion infrastructure, including timely adoption of  
11          and compliance with standards developed by the  
12          National Institute of Standards and Technology  
13          under section 20 of the National Institute of  
14          Standards and Technology Act (15 U.S.C. 278g-  
15          3);

16          “(H) provide assistance to the National In-  
17          stitute of Standards and Technology in devel-  
18          oping standards under section 20 of the National  
19          Institute of Standards and Technology Act (15  
20          U.S.C. 278g-3);

21          “(I) provide to Federal agencies mandatory  
22          security controls to mitigate and remediate  
23          vulnerabilities of and incidents affecting the Fed-  
24          eral information infrastructure;

1           “(J) subject to paragraph (2), and as need-  
2           ed, assist the Director of the Office of Manage-  
3           ment and Budget and the Director of Cyberspace  
4           Policy in conducting analysis and prioritization  
5           of budgets, resources, and policies relating to the  
6           security of the Federal information infrastruc-  
7           ture;

8           “(K) in accordance with section 253, de-  
9           velop, periodically update, and implement a sup-  
10          ply chain risk management strategy to enhance,  
11          in a risk-based and cost-effective manner, the se-  
12          curity of the communications and information  
13          technology products and services purchased by  
14          the Federal Government;

15          “(L) notify the Director of Cyberspace Pol-  
16          icy of any incident involving the Federal infor-  
17          mation infrastructure, information infrastruc-  
18          ture that is owned, operated, controlled, or li-  
19          censed for use by, or on behalf of, the Depart-  
20          ment of Defense, a military department, or an-  
21          other element of the intelligence community, or  
22          the national information infrastructure that  
23          could compromise or significantly affect eco-  
24          nomic or national security;

1           “(M) consult, in coordination with the Di-  
2           rector of Cyberspace Policy, with appropriate  
3           international partners to enhance the security of  
4           the Federal information infrastructure, national  
5           information infrastructure, and information in-  
6           frastructure located outside the United States the  
7           disruption of which could result in national or  
8           regional catastrophic damage in the United  
9           States;

10           “(N)(i) coordinate and integrate informa-  
11           tion to analyze the composite security state of the  
12           Federal information infrastructure and informa-  
13           tion infrastructure that is owned, operated, con-  
14           trolled, or licensed for use by, or on behalf of, the  
15           Department of Defense, a military department,  
16           or another element of the intelligence community;

17           “(i) ensure the information required under  
18           clause (i) and section 3553(c)(1)(A) of title 44,  
19           United States Code, including the views of the  
20           Director on the adequacy and effectiveness of in-  
21           formation security throughout the Federal infor-  
22           mation infrastructure and information infra-  
23           structure that is owned, operated, controlled, or  
24           licensed for use by, or on behalf of, the Depart-  
25           ment of Defense, a military department, or an-

1           *other element of the intelligence community, is*  
2           *available on an automated and continuous basis*  
3           *through the system maintained under section*  
4           *3552(a)(3)(D) of title 44, United States Code;*

5           *“(iii) in conjunction with the quadrennial*  
6           *homeland security review required under section*  
7           *707, and at such other times determined appro-*  
8           *priate by the Director, analyze the composite se-*  
9           *curity state of the national information infra-*  
10           *structure and submit to the President, Congress,*  
11           *and the Secretary a report regarding actions*  
12           *necessary to enhance the composite security state*  
13           *of the national information infrastructure based*  
14           *on the analysis; and*

15           *“(iv) foster collaboration and serve as the*  
16           *primary contact between the Federal Govern-*  
17           *ment, State and local governments, and private*  
18           *entities on matters relating to the security of the*  
19           *Federal information infrastructure and the na-*  
20           *tional information infrastructure;*

21           *“(O) oversee the development, implementa-*  
22           *tion, and management of security requirements*  
23           *for Federal agencies relating to the external ac-*  
24           *cess points to or from the Federal information*  
25           *infrastructure;*

1           “(P) establish, develop, and oversee the ca-  
2           pabilities and operations within the US-CERT  
3           as required by section 244;

4           “(Q) oversee the operations of the National  
5           Communications System, as described in Execu-  
6           tive Order 12472 (49 Fed. Reg. 13471; relating  
7           to the assignment of national security and emer-  
8           gency preparedness telecommunications func-  
9           tions), as amended by Executive Order 13286  
10          (68 Fed. Reg. 10619) and Executive Order 13407  
11          (71 Fed. Reg. 36975), or any successor thereto,  
12          including planning for and providing commu-  
13          nications for the Federal Government under all  
14          circumstances, including crises, emergencies, at-  
15          tacks, recoveries, and reconstitutions;

16          “(R) ensure, in coordination with the pri-  
17          vacy officer designated under subsection (e), the  
18          Privacy Officer appointed under section 222,  
19          and the Director of the Office of Civil Rights and  
20          Civil Liberties appointed under section 705, that  
21          the activities of the Center comply with all poli-  
22          cies, regulations, and laws protecting the privacy  
23          and civil liberties of United States persons;

24          “(S) subject to the availability of resources,  
25          in accordance with applicable law relating to the

1           *protection of trade secrets, and at the discretion*  
2           *of the Director, provide voluntary technical as-*  
3           *sistance—*

4                     “(i) *at the request of an owner or oper-*  
5                     *ator of covered critical infrastructure, to as-*  
6                     *sist the owner or operator in complying*  
7                     *with sections 248 and 249, including imple-*  
8                     *menting required security or emergency*  
9                     *measures and developing response plans for*  
10                    *national cyber emergencies declared under*  
11                    *section 249; and*

12                    “(ii) *at the request of the owner or op-*  
13                    *erator of national information infrastruc-*  
14                    *ture that is not covered critical infrastruc-*  
15                    *ture, and based on risk, to assist the owner*  
16                    *or operator in implementing best practices,*  
17                    *and related standards and guidelines, rec-*  
18                    *ommended under section 247 and other*  
19                    *measures necessary to mitigate or remediate*  
20                    *vulnerabilities of the information infra-*  
21                    *structure and the consequences of efforts to*  
22                    *exploit the vulnerabilities;*

23                    “(T)(i) *conduct, in consultation with the*  
24                    *National Cybersecurity Advisory Council, the*  
25                    *head of appropriate sector-specific agencies, and*

1           any private sector entity determined appropriate  
2           by the Director, risk-based assessments of na-  
3           tional information infrastructure and informa-  
4           tion infrastructure located outside the United  
5           States the disruption of which could result in  
6           national or regional catastrophic damage in the  
7           United States, on a sector-by-sector basis, with  
8           respect to acts of terrorism, natural disasters,  
9           and other large-scale disruptions or financial  
10          harm, which shall identify and prioritize risks to  
11          the national information infrastructure and in-  
12          formation infrastructure located outside the  
13          United States the disruption of which could re-  
14          sult in national or regional catastrophic damage  
15          in the United States, including vulnerabilities  
16          and associated consequences; and

17                 “(i) coordinate and evaluate the mitigation  
18                 or remediation of vulnerabilities and con-  
19                 sequences identified under clause (i);

20                 “(U) regularly evaluate and assess tech-  
21                 nologies designed to enhance the protection of the  
22                 Federal information infrastructure and national  
23                 information infrastructure, including an assess-  
24                 ment of the cost-effectiveness of the technologies;

1           “(V) promote the use of the best practices  
2 recommended under section 247 to State and  
3 local governments and the private sector;

4           “(W) develop and implement outreach and  
5 awareness programs on cybersecurity, includ-  
6 ing—

7                   “(i) a public education campaign to  
8 increase the awareness of cybersecurity,  
9 cyber safety, and cyber ethics, which shall  
10 include use of the Internet, social media, en-  
11 tertainment, and other media to reach the  
12 public;

13                   “(ii) an education campaign to in-  
14 crease the understanding of State and local  
15 governments and private sector entities of  
16 the costs of failing to ensure effective secu-  
17 rity of information infrastructure and cost-  
18 effective methods to mitigate and remediate  
19 vulnerabilities; and

20                   “(iii) outcome-based performance  
21 measures to determine the success of the  
22 programs;

23           “(X) develop and implement a national cy-  
24 bersecurity exercise program that includes—

1           “(i) the participation of State and  
2 local governments, international partners of  
3 the United States, and the private sector;

4           “(ii) an after action report analyzing  
5 lessons learned from exercises and identi-  
6 fying vulnerabilities to be remediated or  
7 mitigated; and

8           “(iii) oversight, in coordination with  
9 the Director of the Office of Cyberspace Pol-  
10 icy, of the efforts by Federal agencies to ad-  
11 dress deficiencies identified in the after ac-  
12 tion reports required under clause (ii);

13           “(Y) coordinate with the Assistant Sec-  
14 retary for Infrastructure Protection to ensure  
15 that—

16           “(i) cybersecurity is appropriately ad-  
17 dressed in carrying out the infrastructure  
18 protection responsibilities described in sec-  
19 tion 201(d); and

20           “(ii) the operations of the Center and  
21 the Office of Infrastructure Protection avoid  
22 duplication and use, to the maximum extent  
23 practicable, joint mechanisms for informa-  
24 tion sharing and coordination with the pri-  
25 vate sector;

1           “(Z) oversee the activities of the Office of  
2           Emergency Communications established under  
3           section 1801;

4           “(AA) in coordination with the Director of  
5           the Office of Cyberspace Policy and the heads of  
6           relevant Federal agencies, develop and imple-  
7           ment an identity management strategy for cyber-  
8           space, which shall include, at a minimum, re-  
9           search and development goals, an analysis of ap-  
10          propriate protections for privacy and civil lib-  
11          erties, and mechanisms to develop and dissemi-  
12          nate best practices and standards relating to  
13          identity management, including usability and  
14          transparency; and

15          “(BB) perform such other duties as the Sec-  
16          retary may direct relating to the security and re-  
17          siliency of the information and communications  
18          infrastructure of the United States.

19          “(2) BUDGET ANALYSIS.—In conducting analysis  
20          and prioritization of budgets under paragraph (1)(J),  
21          the Director—

22                 “(A) in coordination with the Director of  
23                 the Office of Management and Budget, may ac-  
24                 cess information from any Federal agency re-  
25                 garding the finances, budget, and programs of

1           *the Federal agency relevant to the security of the*  
2           *Federal information infrastructure;*

3           “(B) may make recommendations to the Di-  
4           rector of the Office of Management and Budget  
5           and the Director of Cyberspace Policy regarding  
6           the budget for each Federal agency to ensure that  
7           adequate funding is devoted to securing the Fed-  
8           eral information infrastructure, in accordance  
9           with policies, principles, and guidelines estab-  
10          lished by the Director under this subtitle; and

11          “(C) shall provide copies of any rec-  
12          ommendations made under subparagraph (B)  
13          to—

14                 “(i) the Committee on Appropriations  
15                 of the Senate;

16                 “(ii) the Committee on Appropriations  
17                 of the House of Representatives; and

18                 “(iii) the appropriate committees of  
19                 Congress.

20          “(g) *USE OF MECHANISMS FOR COLLABORATION.*—*In*  
21          *carrying out the responsibilities and authorities of the Di-*  
22          *rector under this subtitle, to the maximum extent prac-*  
23          *ticable, the Director shall use mechanisms for collaboration*  
24          *and information sharing (including mechanisms relating*  
25          *to the identification and communication of threats,*

1 *vulnerabilities, and associated consequences) established by*  
2 *other components of the Department or other Federal agen-*  
3 *cies to avoid unnecessary duplication or waste.*

4 “(h) *SUFFICIENCY OF RESOURCES PLAN.*—

5 “(1) *REPORT.*—*Not later than 120 days after the*  
6 *date of enactment of this subtitle, the Director of the*  
7 *Office of Management and Budget shall submit to the*  
8 *appropriate committees of Congress and the Comp-*  
9 *troller General of the United States a report on the*  
10 *resources and staff necessary to carry out fully the re-*  
11 *sponsibilities under this subtitle.*

12 “(2) *COMPTROLLER GENERAL REVIEW.*—

13 “(A) *IN GENERAL.*—*The Comptroller Gen-*  
14 *eral of the United States shall evaluate the rea-*  
15 *sonableness and adequacy of the report submitted*  
16 *by the Director under paragraph (1).*

17 “(B) *REPORT.*—*Not later than 60 days*  
18 *after the date on which the report is submitted*  
19 *under paragraph (1), the Comptroller General*  
20 *shall submit to the appropriate committees of*  
21 *Congress a report containing the findings of the*  
22 *review under subparagraph (A).*

23 “(i) *FUNCTIONS TRANSFERRED.*—*There are trans-*  
24 *ferred to the Center the National Cyber Security Division,*  
25 *the Office of Emergency Communications, and the National*

1 *Communications System, including all the functions, per-*  
2 *sonnel, assets, authorities, and liabilities of the National*  
3 *Cyber Security Division, the Office of Emergency Commu-*  
4 *nications, and the National Communications System.*

5 “(j) *ASSISTANT TO THE DIRECTOR FOR STATE, LOCAL,*  
6 *AND PRIVATE SECTOR OUTREACH.—The Director shall*  
7 *identify a senior official in the Center who—*

8 “(1) *shall report directly to the Director; and*

9 “(2) *in coordination with the Special Assistant*  
10 *to the Secretary appointed under section 102(f),*  
11 *shall—*

12 “(A) *advise the Director on policies and*  
13 *regulations, rules, requirements or other actions*  
14 *affecting the private sector, including the eco-*  
15 *nom ic impact;*

16 “(B) *work with individual businesses and*  
17 *other nongovernmental organizations to foster*  
18 *dialogue with the Center;*

19 “(C) *foster partnerships and facilitate com-*  
20 *munication between the Center and State and*  
21 *local governments and private sector entities;*

22 “(D) *coordinate and maintain communica-*  
23 *tion and interaction with State and local gov-*  
24 *ernments and private sector entities on matters*  
25 *relating to the security of the Federal informa-*

1            *tion infrastructure and the national information*  
2            *infrastructure;*

3            *“(E) assist the Director in sharing best*  
4            *practices, guidelines, and other important infor-*  
5            *mation relating to the policies, goals, and activi-*  
6            *ties of the Center;*

7            *“(F) assist the Director in developing and*  
8            *implementing the national cybersecurity exercise*  
9            *program under subsection (f)(1)(X) as it relates*  
10           *to State and local governments and private sec-*  
11           *tor entities;*

12           *“(G) assist the Director in developing the*  
13           *national incident response plan under subsection*  
14           *(f)(1)(E) as it relates to State and local govern-*  
15           *ments and private sector entities;*

16           *“(H) assist the Director in information*  
17           *sharing activities of the Center as it relates to*  
18           *State and local governments and private sector*  
19           *entities; and*

20           *“(I) perform any other duties, as directed*  
21           *by the Director.*

22    **“SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COL-**  
23           **LABORATION.**

24           *“(a) IN GENERAL.—The Director and the Assistant*  
25           *Secretary for Infrastructure Protection shall coordinate the*

1 *information, communications, and physical infrastructure*  
2 *protection responsibilities and activities of the Center and*  
3 *the Office of Infrastructure Protection.*

4 “(b) *OVERSIGHT.*—*The Secretary shall ensure that the*  
5 *coordination described in subsection (a) occurs.*

6 “**SEC. 244. UNITED STATES COMPUTER EMERGENCY READI-**  
7 **NESS TEAM.**

8 “(a) *ESTABLISHMENT OF OFFICE.*—*There is estab-*  
9 *lished within the Center, the United States Computer Emer-*  
10 *gency Readiness Team, which shall be headed by a Director,*  
11 *who shall be selected from the Senior Executive Service by*  
12 *the Secretary.*

13 “(b) *RESPONSIBILITIES.*—*The US-CERT shall—*

14 “(1) *collect, coordinate, and disseminate infor-*  
15 *mation on—*

16 “(A) *risks to the Federal information infra-*  
17 *structure, information infrastructure that is*  
18 *owned, operated, controlled, or licensed for use*  
19 *by, or on behalf of, the Department of Defense,*  
20 *a military department, or another element of the*  
21 *intelligence community, or the national informa-*  
22 *tion infrastructure; and*

23 “(B) *security controls to enhance the secu-*  
24 *rity of the Federal information infrastructure or*

1           *the national information infrastructure against*  
2           *the risks identified in subparagraph (A); and*

3           “(2) *establish a mechanism for engagement with*  
4           *the private sector.*

5           “(c) *MONITORING, ANALYSIS, WARNING, AND RE-*  
6           *SPONSE.—*

7           “(1) *DUTIES.—Subject to paragraph (2), the*  
8           *US-CERT shall—*

9                   “(A) *provide analysis and reports to Fed-*  
10                   *eral agencies on the security of the Federal infor-*  
11                   *mation infrastructure;*

12                   “(B) *provide continuous, automated moni-*  
13                   *toring of the Federal information infrastructure*  
14                   *at external Internet access points, which shall in-*  
15                   *clude detection and warning of threats,*  
16                   *vulnerabilities, traffic, trends, incidents, and*  
17                   *other anomalous activities affecting the informa-*  
18                   *tion security of the Federal information infra-*  
19                   *structure;*

20                   “(C) *warn Federal agencies of threats,*  
21                   *vulnerabilities, incidents, and anomalous activi-*  
22                   *ties that could affect the Federal information in-*  
23                   *frastructure;*

1           “(D) develop, recommend, and deploy secu-  
2           rity controls to mitigate or remediate  
3           vulnerabilities;

4           “(E) support Federal agencies in con-  
5           ducting risk assessments of the agency informa-  
6           tion infrastructure;

7           “(F) disseminate to Federal agencies risk  
8           analyses of incidents that could impair the risk-  
9           based security of the Federal information infra-  
10          structure;

11          “(G) develop and acquire predictive ana-  
12          lytic tools to evaluate threats, vulnerabilities,  
13          traffic, trends, incidents, and anomalous activi-  
14          ties;

15          “(H) aid in the detection of, and warn own-  
16          ers or operators of national information infra-  
17          structure regarding, threats, vulnerabilities, and  
18          incidents, affecting the national information in-  
19          frastructure, including providing—

20                  “(i) timely, targeted, and actionable  
21                  notifications of threats, vulnerabilities, and  
22                  incidents;

23                  “(ii) notifications under this subpara-  
24                  graph; and

1                   “(iii) recommended security controls to  
2                   mitigate or remediate vulnerabilities; and

3                   “(I) respond to assistance requests from  
4                   Federal agencies and, subject to the availability  
5                   of resources, owners or operators of the national  
6                   information infrastructure to—

7                   “(i) isolate, mitigate, or remediate in-  
8                   cidents;

9                   “(ii) recover from damages and miti-  
10                  gate or remediate vulnerabilities; and

11                  “(iii) evaluate security controls and  
12                  other actions taken to secure information  
13                  infrastructure and incorporate lessons  
14                  learned into best practices, policies, prin-  
15                  ciples, and guidelines.

16                  “(2) *REQUIREMENT.*—With respect to the Fed-  
17                  eral information infrastructure, the US-CERT shall  
18                  conduct the activities described in paragraph (1) in  
19                  a manner consistent with the responsibilities of the  
20                  head of a Federal agency described in section 3553 of  
21                  title 44, United States Code.

22                  “(3) *REPORT.*—Not later than 1 year after the  
23                  date of enactment of this subtitle, and every year  
24                  thereafter, the Secretary shall—

1           “(A) *in conjunction with the Inspector Gen-*  
2           *eral of the Department, conduct an independent*  
3           *audit or review of the activities of the US–CERT*  
4           *under paragraph (1)(B)), which shall include, at*  
5           *a minimum, an assessment of whether and to*  
6           *what extent the activities authorized under para-*  
7           *graph (1)(B) have monitored communications*  
8           *other than communications to or from a Federal*  
9           *agency; and*

10           “(B) *submit to the appropriate committees*  
11           *of Congress and the President a report regarding*  
12           *the audit or review under subparagraph (A).*

13           “(4) *CLASSIFIED ANNEX.—A report submitted*  
14           *under paragraph (3) shall be submitted in an unclas-*  
15           *sified form, but may include a classified annex, if*  
16           *necessary.*

17           “(d) *PROCEDURES FOR FEDERAL GOVERNMENT.—Not*  
18           *later than 90 days after the date of enactment of this sub-*  
19           *title, the head of each Federal agency shall establish proce-*  
20           *dures for the Federal agency that ensure that the US–CERT*  
21           *can perform the functions described in subsection (c) in re-*  
22           *lation to the Federal agency.*

23           “(e) *OPERATIONAL UPDATES.—The US–CERT shall*  
24           *provide unclassified and, as appropriate, classified updates*  
25           *regarding the composite security state of the Federal infor-*

1 *mation infrastructure to the Federal Information Security*  
2 *Taskforce.*

3 “(f) *FEDERAL POINTS OF CONTACT.*—*The Director of*  
4 *the US–CERT shall designate a principal point of contact*  
5 *within the US–CERT for each Federal agency to—*

6 “(1) *maintain communication;*

7 “(2) *ensure cooperative engagement and infor-*  
8 *mation sharing; and*

9 “(3) *respond to inquiries or requests.*

10 “(g) *REQUESTS FOR INFORMATION OR PHYSICAL AC-*  
11 *CESS.*—

12 “(1) *INFORMATION ACCESS.*—*Upon request of the*  
13 *Director of the US–CERT, the head of a Federal*  
14 *agency or an Inspector General for a Federal agency*  
15 *shall provide any law enforcement information, intel-*  
16 *ligence information, terrorism information, or any*  
17 *other information (including information relating to*  
18 *incidents provided under subsections (a)(4) and (c) of*  
19 *section 246) relevant to the security of the Federal in-*  
20 *formation infrastructure or the national information*  
21 *infrastructure necessary to carry out the duties, re-*  
22 *sponsibilities, and authorities under this subtitle.*

23 “(2) *PHYSICAL ACCESS.*—*Upon request of the*  
24 *Director, and in consultation with the head of a Fed-*  
25 *eral agency, the Federal agency shall provide physical*

1       *access to any facility of the Federal agency necessary*  
2       *to determine whether the Federal agency is in compli-*  
3       *ance with any policies, principles, and guidelines es-*  
4       *tablished by the Director under this subtitle, or other-*  
5       *wise necessary to carry out the duties, responsibilities,*  
6       *and authorities of the Director applicable to the Fed-*  
7       *eral information infrastructure.*

8       **“SEC. 245. ADDITIONAL AUTHORITIES OF THE DIRECTOR**  
9                               **OF THE NATIONAL CENTER FOR CYBERSECU-**  
10                              **RITY AND COMMUNICATIONS.**

11       “(a) *ACCESS TO INFORMATION.*—*Unless otherwise di-*  
12       *rected by the President—*

13               “(1) *the Director shall access, receive, and ana-*  
14       *lyze law enforcement information, intelligence infor-*  
15       *mation, terrorism information, and any other infor-*  
16       *mation (including information relating to incidents*  
17       *provided under subsections (a)(4) and (c) of section*  
18       *246) relevant to the security of the Federal informa-*  
19       *tion infrastructure, information infrastructure that is*  
20       *owned, operated, controlled, or licensed for use by, or*  
21       *on behalf of, the Department of Defense, a military*  
22       *department, or another element of the intelligence*  
23       *community, or national information infrastructure*  
24       *from Federal agencies and, consistent with applicable*  
25       *law, State and local governments (including law en-*

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

5               *“(2) any Federal agency in possession of law en-*  
6       *forcement information, intelligence information, ter-*  
7       *rorism information, or any other information (in-*  
8       *cluding information relating to incidents provided*  
9       *under subsections (a)(4) and (c) of section 246) rel-*  
10       *evant to the security of the Federal information infra-*  
11       *structure, information infrastructure that is owned,*  
12       *operated, controlled, or licensed for use by, or on be-*  
13       *half of, the Department of Defense, a military depart-*  
14       *ment, or another element of the intelligence commu-*  
15       *nity, or national information infrastructure shall*  
16       *provide that information to the Director in a timely*  
17       *manner; and*

18               *“(3) the Director, in coordination with the Di-*  
19       *rector of the Office of Management and Budget, the*  
20       *Attorney General, the Privacy and Civil Liberties*  
21       *Oversight Board established under section 1061 of the*  
22       *National Security Intelligence Reform Act of 2004 (42*  
23       *U.S.C. 2000ee), the Director of National Intelligence,*  
24       *and the Archivist of the United States, shall establish*

1 *guidelines to ensure that information is transferred,*  
2 *stored, and preserved—*

3 *“(A) in accordance with applicable laws re-*  
4 *lating to the protection of trade secrets and other*  
5 *applicable laws; and*

6 *“(B) in a manner that protects the privacy*  
7 *and civil liberties of United States persons and*  
8 *intelligence sources and methods.*

9 *“(b) OPERATIONAL EVALUATIONS.—*

10 *“(1) IN GENERAL.—The Director—*

11 *“(A) subject to paragraph (2), shall develop,*  
12 *maintain, and enhance capabilities to evaluate*  
13 *the security of the Federal information infra-*  
14 *structure as described in section 3554(a)(3) of*  
15 *title 44, United States Code, including the abil-*  
16 *ity to conduct risk-based penetration testing and*  
17 *vulnerability assessments;*

18 *“(B) in carrying out subparagraph (A),*  
19 *may request technical assistance from the Direc-*  
20 *tor of the Federal Bureau of Investigation, the*  
21 *Director of the National Security Agency, the*  
22 *head of any other Federal agency that may pro-*  
23 *vide support, and any nongovernmental entity*  
24 *contracting with the Department or another Fed-*  
25 *eral agency; and*

1           “(C) *in consultation with the Attorney Gen-*  
2           *eral and the Privacy and Civil Liberties Over-*  
3           *sight Board established under section 1061 of the*  
4           *National Security Intelligence Reform Act of*  
5           *2004 (42 U.S.C. 2000ee), shall develop guidelines*  
6           *to ensure compliance with all applicable laws re-*  
7           *lating to the privacy of United States persons in*  
8           *carrying out the operational evaluations under*  
9           *subparagraph (A).*

10          “(2) *OPERATIONAL EVALUATIONS.—*

11           “(A) *IN GENERAL.—The Director may con-*  
12           *duct risk-based operational evaluations of the*  
13           *agency information infrastructure of any Fed-*  
14           *eral agency, at a time determined by the Direc-*  
15           *tor, in consultation with the head of the Federal*  
16           *agency, using the capabilities developed under*  
17           *paragraph (1)(A).*

18           “(B) *ANNUAL EVALUATION REQUIRE-*  
19           *MENT.—If the Director conducts an operational*  
20           *evaluation under subparagraph (A) or an oper-*  
21           *ational evaluation at the request of a Federal*  
22           *agency to meet the requirements of section 3554*  
23           *of title 44, United States Code, the operational*  
24           *evaluation shall satisfy the requirements of sec-*  
25           *tion 3554 for the Federal agency for the year of*

1           *the evaluation, unless otherwise specified by the*  
2           *Director.*

3           “(c) *CORRECTIVE MEASURES AND MITIGATION*  
4 *PLANS.—If the Director determines that a Federal agency*  
5 *is not in compliance with applicable policies, principles,*  
6 *standards, and guidelines applicable to the Federal infor-*  
7 *mation infrastructure—*

8           “(1) *the Director, in consultation with the Direc-*  
9 *tor of the Office of Management and Budget, may di-*  
10 *rect the head of the Federal agency to—*

11           “(A) *take corrective measures to meet the*  
12 *policies, principles, standards, and guidelines;*  
13 *and*

14           “(B) *develop a plan to remediate or miti-*  
15 *gate any vulnerabilities addressed by the poli-*  
16 *cies, principles, standards, and guidelines;*

17           “(2) *within such time period as the Director*  
18 *shall prescribe, the head of the Federal agency shall—*

19           “(A) *implement a corrective measure or de-*  
20 *velop a mitigation plan in accordance with*  
21 *paragraph (1); or*

22           “(B) *submit to the Director, the Director of*  
23 *the Office of Management and Budget, the In-*  
24 *spector General for the Federal agency, and the*  
25 *appropriate committees of Congress a report in-*

1           *dicating why the Federal agency has not imple-*  
2           *mented the corrective measure or developed a*  
3           *mitigation plan; and*

4           “(3) after providing notice to the head of the af-  
5           *ected Federal agency, the Director may direct the iso-*  
6           *lation of any component of the agency information*  
7           *infrastructure, consistent with the contingency or con-*  
8           *tinuity of operation plans applicable to the agency*  
9           *information infrastructure, until corrective measures*  
10          *are taken or mitigation plans approved by the Direc-*  
11          *tor are put in place, if—*

12                   “(A) the head of the Federal agency has  
13                   *failed to comply with the corrective measures*  
14                   *prescribed under paragraph (1); and*

15                   “(B) the failure to comply presents a sig-  
16                   *nificant danger to the Federal information infra-*  
17                   *structure.*

18 **“SEC. 246. INFORMATION SHARING.**

19           “(a) *FEDERAL AGENCIES.—*

20                   “(1) *INFORMATION SHARING PROGRAM.—Con-*  
21                   *sistent with the responsibilities described in section*  
22                   *242 and 244, the Director, in consultation with the*  
23                   *other members of the Chief Information Officers*  
24                   *Council established under section 3603 of title 44,*  
25                   *United States Code, and the Federal Information Se-*

1        *curity Taskforce, shall establish a program for shar-*  
2        *ing information with and between the Center and*  
3        *other Federal agencies that includes processes and*  
4        *procedures, including standard operating proce-*  
5        *dures—*

6                *“(A) under which the Director regularly*  
7                *shares with each Federal agency—*

8                        *“(i) analysis and reports on the com-*  
9                        *posite security state of the Federal informa-*  
10                        *tion infrastructure and information infra-*  
11                        *structure that is owned, operated, con-*  
12                        *trolled, or licensed for use by, or on behalf*  
13                        *of, the Department of Defense, a military*  
14                        *department, or another element of the intel-*  
15                        *ligence community, which shall include in-*  
16                        *formation relating to threats,*  
17                        *vulnerabilities, incidents, or anomalous ac-*  
18                        *tivities;*

19                        *“(ii) any available analysis and re-*  
20                        *ports regarding the security of the agency*  
21                        *information infrastructure; and*

22                        *“(iii) means and methods of pre-*  
23                        *venting, responding to, mitigating, and re-*  
24                        *mediating vulnerabilities; and*

1           “(B) under which the Director may request  
2 information from Federal agencies concerning  
3 the security of the Federal information infra-  
4 structure, information infrastructure that is  
5 owned, operated, controlled, or licensed for use  
6 by, or on behalf of, the Department of Defense,  
7 a military department, or another element of the  
8 intelligence community, or the national informa-  
9 tion infrastructure necessary to carry out the du-  
10 ties of the Director under this subtitle or any  
11 other provision of law.

12           “(2) CONTENTS.—The program established under  
13 this section shall include—

14           “(A) timeframes for the sharing of informa-  
15 tion under paragraph (1);

16           “(B) guidance on what information shall be  
17 shared, including information regarding inci-  
18 dents;

19           “(C) a tiered structure that provides guid-  
20 ance for the sharing of urgent information; and

21           “(D) processes and procedures under which  
22 the Director or the head of a Federal agency may  
23 report noncompliance with the program to the  
24 Director of Cyberspace Policy.

1           “(3) *US-CERT.*—*The Director of the US-*  
2           *CERT shall ensure that the head of each Federal*  
3           *agency has continual access to data collected by the*  
4           *US-CERT regarding the agency information infra-*  
5           *structure of the Federal agency.*

6           “(4) *FEDERAL AGENCIES.*—

7           “(A) *IN GENERAL.*—*The head of a Federal*  
8           *agency shall comply with all processes and pro-*  
9           *cedures established under this subsection regard-*  
10           *ing notification to the Director relating to inci-*  
11           *dents.*

12           “(B) *IMMEDIATE NOTIFICATION RE-*  
13           *QUIRED.*—*Unless otherwise directed by the Presi-*  
14           *dent, any Federal agency with a national secu-*  
15           *rity system shall immediately notify the Director*  
16           *regarding any incident affecting the risk-based*  
17           *security of the national security system.*

18           “(b) *STATE AND LOCAL GOVERNMENTS, PRIVATE SEC-*  
19           *TOR, AND INTERNATIONAL PARTNERS.*—

20           “(1) *IN GENERAL.*—*The Director shall establish*  
21           *processes and procedures, including standard oper-*  
22           *ating procedures, to ensure bidirectional information*  
23           *sharing with State and local governments, private en-*  
24           *tities, and international partners of the United States*  
25           *on—*

1           “(A) threats, vulnerabilities, incidents, and  
2 anomalous activities affecting the national infor-  
3 mation infrastructure; and

4           “(B) means and methods of preventing, re-  
5 sponding to, and mitigating and remediating  
6 vulnerabilities.

7           “(2) CONTENTS.—The processes and procedures  
8 established under paragraph (1) shall include—

9           “(A) means or methods of accessing classi-  
10 fied or unclassified information, as appropriate  
11 and in accordance with applicable laws regard-  
12 ing trade secrets, that will provide situational  
13 awareness of the security of the Federal informa-  
14 tion infrastructure and the national information  
15 infrastructure relating to threats, vulnerabilities,  
16 traffic, trends, incidents, and other anomalous  
17 activities affecting the Federal information in-  
18 frastructure or the national information infra-  
19 structure;

20           “(B) a mechanism, established in consulta-  
21 tion with the heads of the relevant sector-specific  
22 agencies, sector coordinating councils, and infor-  
23 mation sharing and analysis centers, by which  
24 owners and operators of covered critical infra-  
25 structure shall report incidents in the informa-

1            *tion infrastructure for covered critical infra-*  
2            *structure under subsection (c)(1)(A);*

3            *“(C) guidance on the form, content, and*  
4            *priority of incident reports that shall be sub-*  
5            *mitted under subsection (c)(1)(A), which shall—*

6                    *“(i) include appropriate mechanisms*  
7                    *to protect—*

8                            *“(I) information in accordance*  
9                            *with section 251;*

10                           *“(II) personally identifiable infor-*  
11                           *mation; and*

12                           *“(III) trade secrets; and*

13                           *“(ii) prioritize the reporting of inci-*  
14                           *dents based on the risk the incident poses to*  
15                           *the disruption of the reliable operation of*  
16                           *the covered critical infrastructure;*

17            *“(D) a procedure for notifying an informa-*  
18            *tion technology provider if a vulnerability is de-*  
19            *tected in the product or service produced by the*  
20            *information technology provider and, where pos-*  
21            *sible, working with the information technology*  
22            *provider to remediate the vulnerability before*  
23            *any public disclosure of the vulnerability so as*  
24            *to minimize the opportunity for the vulnerability*  
25            *to be exploited; and*

1           “(E) an evaluation of the need to provide  
2           security clearances to employees of State and  
3           local governments, private entities, and inter-  
4           national partners to carry out this subsection.

5           “(3) *GUIDELINES.*—*The Director, in consulta-*  
6           *tion with the Attorney General, the Director of Na-*  
7           *tional Intelligence, and the Privacy Officer established*  
8           *under section 242(e), shall develop guidelines to pro-*  
9           *tect the privacy and civil liberties of United States*  
10          *persons and intelligence sources and methods, while*  
11          *carrying out this subsection.*

12          “(c) *INCIDENTS.*—

13                 “(1) *NON-FEDERAL ENTITIES.*—

14                         “(A) *IN GENERAL.*—

15                                 “(i) *MANDATORY REPORTING.*—*Subject*  
16                                 *to clause (ii), the owner or operator of cov-*  
17                                 *ered critical infrastructure shall report any*  
18                                 *incident affecting the information infra-*  
19                                 *structure of covered critical infrastructure*  
20                                 *to the extent the incident might indicate an*  
21                                 *actual or potential cyber risk, or exploi-*  
22                                 *tation of a cyber risk, in accordance with*  
23                                 *the policies and procedures for the mecha-*  
24                                 *nism established under subsection (b)(2)(B)*

1                   *and guidelines developed under subsection*  
2                   *(b)(3).*

3                   “(ii) *LIMITATION.*—*Clause (i) shall not*  
4                   *authorize the Director, the Center, the De-*  
5                   *partment, or any other Federal entity to—*

6                                 “(I) *compel the disclosure of infor-*  
7                                 *mation relating to an incident unless*  
8                                 *otherwise authorized by law; or*

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

1           “(B) *REPORTING PROCEDURES.*—*The Di-*  
2           *rector shall establish procedures that enable and*  
3           *encourage the owner or operator of national in-*  
4           *formation infrastructure to report to the Director*  
5           *regarding incidents affecting such information*  
6           *infrastructure.*

7           “(2) *INFORMATION PROTECTION.*—*Notwith-*  
8           *standing any other provision of law, information re-*  
9           *ported under paragraph (1) shall be protected from*  
10          *unauthorized disclosure, in accordance with section*  
11          *251.*

12          “(d) *ADDITIONAL RESPONSIBILITIES.*—*The Director*  
13          *shall—*

14                 “(1) *share data collected on the Federal informa-*  
15                 *tion infrastructure with the National Science Foun-*  
16                 *dition and other accredited research institutions for*  
17                 *the sole purpose of cybersecurity research in a manner*  
18                 *that protects privacy and civil liberties of United*  
19                 *States persons and intelligence sources and methods;*

20                 “(2) *establish a website to provide an oppor-*  
21                 *tunity for the public to provide—*

22                         “(A) *input about the operations of the Cen-*  
23                         *ter; and*

24                         “(B) *recommendations for improvements of*  
25                         *the Center; and*

1           “(3) *in coordination with the Secretary of De-*  
2           *fense, the Director of National Intelligence, the Sec-*  
3           *retary of State, and the Attorney General, develop in-*  
4           *formation sharing pilot programs with international*  
5           *partners of the United States.*

6   **“SEC. 247. PRIVATE SECTOR ASSISTANCE.**

7           “(a) *IN GENERAL.—The Director, in consultation with*  
8           *the Director of the National Institute of Standards and*  
9           *Technology, the Director of the National Security Agency,*  
10          *the head of any relevant sector-specific agency, the National*  
11          *Cybersecurity Advisory Council, State and local govern-*  
12          *ments, and any private entities the Director determines ap-*  
13          *propriate, shall establish a program to promote, and pro-*  
14          *vide technical assistance authorized under section*  
15          *242(f)(1)(S) relating to the implementation of, best prac-*  
16          *tices and related standards and guidelines for securing the*  
17          *national information infrastructure, including the costs*  
18          *and benefits associated with the implementation of the best*  
19          *practices and related standards and guidelines.*

20          “(b) *ANALYSIS AND IMPROVEMENT OF STANDARDS AND*  
21          *GUIDELINES.—For purposes of the program established*  
22          *under subsection (a), the Director shall—*

23                  “(1) *regularly assess and evaluate cybersecurity*  
24                  *standards and guidelines issued by private sector or-*  
25                  *ganizations, recognized international and domestic*

1       *standards setting organizations, and Federal agencies;*  
2       *and*

3               “(2) *in coordination with the National Institute*  
4       *of Standards and Technology, encourage the develop-*  
5       *ment of, and recommend changes to, the standards*  
6       *and guidelines described in paragraph (1) for secur-*  
7       *ing the national information infrastructure.*

8       “(c) *GUIDANCE AND TECHNICAL ASSISTANCE.—*

9               “(1) *IN GENERAL.—The Director shall promote*  
10       *best practices and related standards and guidelines to*  
11       *assist owners and operators of national information*  
12       *infrastructure in increasing the security of the na-*  
13       *tional information infrastructure and protecting*  
14       *against and mitigating or remediating known*  
15       *vulnerabilities.*

16               “(2) *REQUIREMENT.—Technical assistance pro-*  
17       *vided under section 242(f)(1)(S) and best practices*  
18       *promoted under this section shall be prioritized based*  
19       *on risk.*

20       “(d) *CRITERIA.—In promoting best practices or rec-*  
21       *ommending changes to standards and guidelines under this*  
22       *section, the Director shall ensure that best practices, and*  
23       *related standards and guidelines—*

24               “(1) *address cybersecurity in a comprehensive,*  
25       *risk-based manner;*

1           “(2) include consideration of the cost of imple-  
2           menting such best practices or of implementing rec-  
3           ommended changes to standards and guidelines;

4           “(3) increase the ability of the owners or opera-  
5           tors of national information infrastructure to protect  
6           against and mitigate or remediate known  
7           vulnerabilities;

8           “(4) are suitable, as appropriate, for implemen-  
9           tation by small business concerns;

10          “(5) as necessary and appropriate, are sector  
11          specific;

12          “(6) to the maximum extent possible, incorporate  
13          standards and guidelines established by private sector  
14          organizations, recognized international and domestic  
15          standards setting organizations, and Federal agencies;

16          “(7) consider voluntary programs by internet  
17          service providers to assist individuals using the inter-  
18          net service providers in the identification and mitiga-  
19          tion of cyber threats and vulnerabilities, with the con-  
20          sent of the individual users; and

21          “(8) provide sufficient flexibility to permit a  
22          range of security solutions.

23       **“SEC. 248. CYBER RISKS TO COVERED CRITICAL INFRA-**  
24       **STRUCTURE.**

25       “(a) *IDENTIFICATION OF CYBER RISKS.*—

1           “(1) *IN GENERAL.*—Based on the risk-based as-  
2           *sessments conducted under section 242(f)(1)(T)(i), the*  
3           *Director, in coordination with the head of the sector-*  
4           *specific agency with responsibility for covered critical*  
5           *infrastructure and the head of any Federal agency*  
6           *that is not a sector-specific agency with responsibil-*  
7           *ities for regulating the covered critical infrastructure,*  
8           *and in consultation with the National Cybersecurity*  
9           *Advisory Council and any private sector entity deter-*  
10          *mined appropriate by the Director, shall, on a contin-*  
11          *uous and sector-by-sector basis, identify and evaluate*  
12          *the cyber risks to covered critical infrastructure.*

13           “(2) *FACTORS TO BE CONSIDERED.*—In identi-  
14          *fying and evaluating cyber risks under paragraph*  
15          *(1), the Director shall consider—*

16                   “(A) *the actual or assessed threat, including*  
17                   *a consideration of adversary capabilities and in-*  
18                   *tent, preparedness, target attractiveness, and de-*  
19                   *terrence capabilities;*

20                   “(B) *the extent and likelihood of death, in-*  
21                   *jury, or serious adverse effects to human health*  
22                   *and safety caused by a disruption of the reliable*  
23                   *operation of covered critical infrastructure;*

1           “(C) *the threat to or impact on national se-*  
2 *curity caused by a disruption of the reliable op-*  
3 *eration of covered critical infrastructure;*

4           “(D) *the extent to which the disruption of*  
5 *the reliable operation of covered critical infra-*  
6 *structure will disrupt the reliable operation of*  
7 *other covered critical infrastructure;*

8           “(E) *the harm to the economy that would*  
9 *result from a disruption of the reliable operation*  
10 *of covered critical infrastructure; and*

11           “(F) *other risk-based security factors that*  
12 *the Director, in consultation with the head of the*  
13 *sector-specific agency with responsibility for the*  
14 *covered critical infrastructure and the head of*  
15 *any Federal agency that is not a sector-specific*  
16 *agency with responsibilities for regulating the*  
17 *covered critical infrastructure, determine to be*  
18 *appropriate and necessary to protect public*  
19 *health and safety, critical infrastructure, or na-*  
20 *tional and economic security.*

21           “(3) *REPORT.—*

22           “(A) *IN GENERAL.—Not later than 180*  
23 *days after the date of enactment of this subtitle,*  
24 *and annually thereafter, the Director, in coordi-*  
25 *nation with the head of the sector-specific agency*

1           with responsibility for the covered critical infra-  
2           structure and the head of any Federal agency  
3           that is not a sector-specific agency with respon-  
4           sibilities for regulating the covered critical infra-  
5           structure, shall submit to the appropriate com-  
6           mittees of Congress a report on the findings of  
7           the identification and evaluation of cyber risks  
8           under this subsection. Each report submitted  
9           under this paragraph shall be submitted in an  
10          unclassified form, but may include a classified  
11          annex.

12                   “(B) *INPUT.*—For purposes of the reports  
13                   required under subparagraph (A), the Director  
14                   shall create a process under which owners and  
15                   operators of covered critical infrastructure may  
16                   provide input on the findings of the reports.

17           “(b) *RISK-BASED SECURITY PERFORMANCE REQUIRE-*  
18          *MENTS.*—

19                   “(1) *IN GENERAL.*—Not later than 270 days  
20                   after the date of the enactment of this subtitle, in co-  
21                   ordination with the heads of the sector-specific agen-  
22                   cies with responsibility for covered critical infrastruc-  
23                   ture and the head of any Federal agency that is not  
24                   a sector-specific agency with responsibilities for regu-  
25                   lating the covered critical infrastructure, and in con-

1 *sultation with the National Cybersecurity Advisory*  
2 *Council and any private sector entity determined ap-*  
3 *propriate by the Director, the Director shall issue in-*  
4 *terim final regulations establishing risk-based secu-*  
5 *rity performance requirements to secure covered crit-*  
6 *ical infrastructure against cyber risks through the*  
7 *adoption of security measures that satisfy the security*  
8 *performance requirements identified by the Director.*

9 “(2) *PROCEDURES.*—*The regulations issued*  
10 *under this subsection shall—*

11 “(A) *include a process under which owners*  
12 *and operators of covered critical infrastructure*  
13 *are informed of identified cyber risks and secu-*  
14 *rity performance requirements designed to reme-*  
15 *diate or mitigate the cyber risks, in combination*  
16 *with best practices recommended under section*  
17 *247;*

18 “(B) *establish a process for owners and op-*  
19 *erators of covered critical infrastructure to select*  
20 *security measures, including any best practices*  
21 *recommended under section 247, that, in com-*  
22 *bination, satisfy the security performance re-*  
23 *quirements established by the Director under this*  
24 *subsection;*

1           “(C) establish a process for owners and op-  
2           erators of covered critical infrastructure to de-  
3           velop response plans for a national cyber emer-  
4           gency declared under section 249;

5           “(D) establish a process under which the  
6           Director—

7           “(i) is notified of the security measures  
8           selected by the owner or operator of covered  
9           critical infrastructure under subparagraph  
10          (B); and

11          “(ii) may determine whether the pro-  
12          posed security measures satisfy the security  
13          performance requirements established by the  
14          Director under this subsection; and

15          “(E) establish a process under which the  
16          Director—

17          “(i) identifies to owners and operators  
18          of covered critical infrastructure cyber risks  
19          that are not capable of effective remediation  
20          or mitigation using available best practices  
21          or security measures;

22          “(ii) provides owners and operators of  
23          covered critical infrastructure the oppor-  
24          tunity to develop best practices or security  
25          measures to remediate or mitigate the cyber

1           *risks identified in clause (i) without the*  
2           *prior approval of the Director and without*  
3           *affecting the compliance of the covered crit-*  
4           *ical infrastructure with the requirements*  
5           *under this section;*

6           *“(iii) in accordance with applicable*  
7           *law relating to the protection of trade se-*  
8           *crets, permits owners and operators of cov-*  
9           *ered critical infrastructure to report to the*  
10          *Center the development of effective best*  
11          *practices or security measures to remediate*  
12          *or mitigate the cyber risks identified under*  
13          *clause (i); and*

14          *“(iv) incorporates the best practices*  
15          *and security measures developed into the*  
16          *risk-based security performance require-*  
17          *ments under this section.*

18          “(3) *INTERNATIONAL COOPERATION ON SECUR-*  
19          *ING COVERED CRITICAL INFRASTRUCTURE.—*

20          “(A) *IN GENERAL.—The Director, in coordi-*  
21          *nation with the head of the sector-specific agency*  
22          *with responsibility for covered critical infra-*  
23          *structure and the head of any Federal agency*  
24          *that is not a sector-specific agency with respon-*

1           *sibilities for regulating the covered critical infra-*  
2           *structure, shall—*

3                     “(i) *consistent with the protection of*  
4                     *intelligence sources and methods and other*  
5                     *sensitive matters, inform the owner or oper-*  
6                     *ator of information infrastructure located*  
7                     *outside the United States the disruption of*  
8                     *which could result in national or regional*  
9                     *catastrophic damage in the United States*  
10                    *and the government of the country in which*  
11                    *the information infrastructure is located of*  
12                    *any cyber risks to the information infra-*  
13                    *structure; and*

14                    “(ii) *coordinate with the government of*  
15                    *the country in which the information infra-*  
16                    *structure is located and, as appropriate, the*  
17                    *owner or operator of the information infra-*  
18                    *structure, regarding the implementation of*  
19                    *security measures or other measures to the*  
20                    *information infrastructure to mitigate or*  
21                    *remediate cyber risks.*

22                    “(B) *INTERNATIONAL AGREEMENTS.—The*  
23                    *Director shall carry out this paragraph in a*  
24                    *manner consistent with applicable international*  
25                    *agreements.*

1           “(4) *RISK-BASED SECURITY PERFORMANCE RE-*  
2           *QUIREMENTS.*—

3           “(A) *IN GENERAL.*—*The security perform-*  
4           *ance requirements established by the Director*  
5           *under this subsection shall be—*

6                   “(i) *based on the factors listed in sub-*  
7                   *section (a)(2); and*

8                   “(ii) *designed to remediate or mitigate*  
9                   *identified cyber risks and any associated*  
10                   *consequences of an exploitation based on*  
11                   *such risks.*

12           “(B) *CONSULTATION.*—*In establishing secu-*  
13           *rity performance requirements under this sub-*  
14           *section, the Director shall, to the maximum ex-*  
15           *tent practicable, consult with—*

16                   “(i) *the Director of the National Secu-*  
17                   *rity Agency;*

18                   “(ii) *the Director of the National Insti-*  
19                   *tute of Standards and Technology;*

20                   “(iii) *the National Cybersecurity Advi-*  
21                   *sory Council;*

22                   “(iv) *the heads of sector-specific agen-*  
23                   *cies; and*

24                   “(v) *the heads of Federal agencies that*  
25                   *are not sector-specific agencies with respon-*

1           *sibilities for regulating the covered critical*  
2           *infrastructure.*

3           “(C) *ALTERNATIVE MEASURES.*—

4                   “(i) *IN GENERAL.*—*The owners and*  
5                   *operators of covered critical infrastructure*  
6                   *shall have flexibility to implement any secu-*  
7                   *rity measure, or combination thereof, to sat-*  
8                   *isfy the security performance requirements*  
9                   *described in subparagraph (A) and the Di-*  
10                   *rector may not disapprove under this sec-*  
11                   *tion any proposed security measures, or*  
12                   *combination thereof, based on the presence*  
13                   *or absence of any particular security meas-*  
14                   *ure if the proposed security measures, or*  
15                   *combination thereof, satisfy the security*  
16                   *performance requirements established by the*  
17                   *Director under this section or are consistent*  
18                   *with the process for addressing new or*  
19                   *evolving cyber risks established under para-*  
20                   *graph (2)(E).*

21                   “(ii) *RECOMMENDED SECURITY MEAS-*  
22                   *URES.*—*The Director may recommend to an*  
23                   *owner and operator of covered critical in-*  
24                   *frastructure a specific security measure, or*  
25                   *combination thereof, that will satisfy the se-*

1                    *curity performance requirements established*  
2                    *by the Director. The absence of the rec-*  
3                    *ommended security measures, or combina-*  
4                    *tion thereof, may not serve as the basis for*  
5                    *a disapproval of the security measure, or*  
6                    *combination thereof, proposed by the owner*  
7                    *or operator of covered critical infrastructure*  
8                    *if the proposed security measure, or com-*  
9                    *bination thereof, otherwise satisfies the secu-*  
10                   *urity performance requirements established*  
11                   *by the Director under this section.*

12 **“SEC. 249. NATIONAL CYBER EMERGENCIES.**

13                   *“(a) DECLARATION.—*

14                   *“(1) IN GENERAL.—The President may issue a*  
15                   *declaration of a national cyber emergency to covered*  
16                   *critical infrastructure if there is an ongoing or immi-*  
17                   *nent action by any individual or entity to exploit a*  
18                   *cyber risk in a manner that disrupts, attempts to dis-*  
19                   *rupt, or poses a significant risk of disruption to the*  
20                   *operation of the information infrastructure essential*  
21                   *to the reliable operation of covered critical infrastruc-*  
22                   *ture. Any declaration under this section shall specify*  
23                   *the covered critical infrastructure subject to the na-*  
24                   *tional cyber emergency.*

1           “(2) *NOTIFICATION.*—Upon issuing a declaration  
2           under paragraph (1), the President shall, consistent  
3           with the protection of intelligence sources and meth-  
4           ods, notify the owners and operators of the specified  
5           covered critical infrastructure and any other relevant  
6           private sector entity of the nature of the national  
7           cyber emergency.

8           “(3) *AUTHORITIES.*—If the President issues a  
9           declaration under paragraph (1), the Director shall—

10           “(A) immediately direct the owners and op-  
11           erators of covered critical infrastructure subject  
12           to the declaration under paragraph (1) to imple-  
13           ment response plans required under section  
14           248(b)(2)(C);

15           “(B) develop and coordinate emergency  
16           measures or actions necessary to preserve the re-  
17           liable operation, and mitigate or remediate the  
18           consequences of the potential disruption, of cov-  
19           ered critical infrastructure;

20           “(C) ensure that emergency measures or ac-  
21           tions directed under this section represent the  
22           least disruptive means feasible to the operations  
23           of the covered critical infrastructure and to the  
24           national information infrastructure;

1           “(D) subject to subsection (g), direct actions  
2           by other Federal agencies to respond to the na-  
3           tional cyber emergency;

4           “(E) coordinate with officials of State and  
5           local governments, international partners of the  
6           United States, owners and operators of covered  
7           critical infrastructure specified in the declara-  
8           tion, and other relevant private section entities  
9           to respond to the national cyber emergency;

10           “(F) initiate a process under section 248 to  
11           address the cyber risk that may be exploited by  
12           the national cyber emergency; and

13           “(G) provide voluntary technical assistance,  
14           if requested, under section 242(f)(1)(S).

15           “(4) REIMBURSEMENT.—A Federal agency shall  
16           be reimbursed for expenditures under this section  
17           from funds appropriated for the purposes of this sec-  
18           tion. Any funds received by a Federal agency as reim-  
19           bursement for services or supplies furnished under the  
20           authority of this section shall be deposited to the cred-  
21           it of the appropriation or appropriations available on  
22           the date of the deposit for the services or supplies.

23           “(5) CONSULTATION.—In carrying out this sec-  
24           tion, the Director shall consult with the Secretary, the  
25           Secretary of Defense, the Director of the National Se-

1        *curity Agency, the Director of the National Institute*  
2        *of Standards and Technology, and any other official,*  
3        *as directed by the President.*

4            “(6) *PROHIBITED ACTIONS.*—*The authority to*  
5        *direct compliance with an emergency measure or ac-*  
6        *tion under this section shall not authorize the Direc-*  
7        *tor, the Center, the Department, or any other Federal*  
8        *entity to—*

9            “(A) *restrict or prohibit communications*  
10        *carried by, or over, covered critical infrastruc-*  
11        *ture and not specifically directed to or from the*  
12        *covered critical infrastructure unless the Director*  
13        *determines that no other emergency measure or*  
14        *action will preserve the reliable operation, and*  
15        *mitigate or remediate the consequences of the po-*  
16        *tential disruption, of the covered critical infra-*  
17        *structure or the national information infrastruc-*  
18        *ture;*

19            “(B) *control covered critical infrastructure;*

20            “(C) *compel the disclosure of information*  
21        *unless specifically authorized by law; or*

22            “(D) *intercept a wire, oral, or electronic*  
23        *communication (as those terms are defined in*  
24        *section 2510 of title 18, United States Code), ac-*  
25        *cess a stored electronic or wire communication,*

1           *install or use a pen register or trap and trace*  
2           *device, or conduct electronic surveillance (as de-*  
3           *defined in section 101 of the Foreign Intelligence*  
4           *Surveillance Act of 1978 (50 U.S.C.1801)) relat-*  
5           *ing to an incident unless otherwise authorized*  
6           *under chapter 119, chapter 121, or chapter 206*  
7           *of title 18, United States Code, the Foreign Intel-*  
8           *ligence Surveillance Act of 1978 (50 U.S.C. 1801*  
9           *et seq.).*

10           “(7) *PRIVACY.*—*In carrying out this section, the*  
11           *Director shall ensure that the privacy and civil lib-*  
12           *erties of United States persons are protected.*

13           “(b) *DISCONTINUANCE OF EMERGENCY MEASURES.*—

14           “(1) *IN GENERAL.*—*Any emergency measure or*  
15           *action developed under this section shall cease to have*  
16           *effect not later than 30 days after the date on which*  
17           *the President issued the declaration of a national*  
18           *cyber emergency, unless—*

19                   “(A) *the Director details in writing why the*  
20                   *emergency measure or action remains necessary*  
21                   *to address the identified national cyber emer-*  
22                   *gency; and*

23                   “(B) *the President issues a written order or*  
24                   *directive reaffirming the national cyber emer-*  
25                   *gency, the continuing nature of the national*

1           *cyber emergency, or the need to continue the*  
2           *adoption of the emergency measure or action.*

3           “(2) *EXTENSIONS.—An emergency measure or*  
4           *action extended in accordance with paragraph (1)*  
5           *may—*

6                   “(A) *remain in effect for not more than 30*  
7                   *days after the date on which the emergency*  
8                   *measure or action was to cease to have effect;*  
9                   *and*

10                   “(B) *unless a joint resolution described in*  
11                   *subsection (f)(1) is enacted, be extended for not*  
12                   *more than 3 additional 30-day periods, if the re-*  
13                   *quirements of paragraph (1) and subsection (d)*  
14                   *are met.*

15           “(c) *COMPLIANCE WITH EMERGENCY MEASURES.—*

16                   “(1) *IN GENERAL.—Subject to paragraph (2), the*  
17                   *owner or operator of covered critical infrastructure*  
18                   *shall immediately comply with any emergency meas-*  
19                   *ure or action developed by the Director under this sec-*  
20                   *tion during the pendency of any declaration by the*  
21                   *President under subsection (a)(1) or an extension*  
22                   *under subsection (b)(2).*

23                   “(2) *ALTERNATIVE MEASURES.—*

24                   “(A) *IN GENERAL.—If the Director deter-*  
25                   *mines that a proposed security measure, or any*

1 combination thereof, submitted by the owner or  
2 operator of covered critical infrastructure in ac-  
3 cordance with the process established under sec-  
4 tion 248(b)(2) will effectively mitigate or reme-  
5 diate the cyber risk associated with the national  
6 cyber emergency that is the subject of the dec-  
7 laration under this section, or effectively miti-  
8 gate or remediate the consequences of the poten-  
9 tial disruption of the covered critical infrastruc-  
10 ture based on the cyber risk at least as effectively  
11 as the emergency measures or actions directed by  
12 the Director under this section, the owner or op-  
13 erator may comply with paragraph (1) of this  
14 subsection by implementing the proposed security  
15 measure, or combination thereof, approved by the  
16 Director under the process established under sec-  
17 tion 248.

18 “(B) COMPLIANCE PENDING SUBMISSION OR  
19 APPROVAL.—Before submission of a proposed se-  
20 curity measure, or combination thereof, and dur-  
21 ing the pendency of any review by the Director  
22 under the process established under section 248,  
23 the owner or operator of covered critical infra-  
24 structure shall remain in compliance with any  
25 emergency measure or action developed by the

1           *Director under this section during the pendency*  
2           *of any declaration by the President under sub-*  
3           *section (a)(1) or an extension under subsection*  
4           *(b)(2), until such time as the Director has ap-*  
5           *proved an alternative proposed security measure,*  
6           *or combination thereof, under this paragraph.*

7           “(3) *INTERNATIONAL COOPERATION ON NATIONAL*  
8           *CYBER EMERGENCIES.—*

9                   “(A) *IN GENERAL.—The Director, in coordi-*  
10           *nation with the head of the sector-specific agency*  
11           *with responsibility for covered critical infra-*  
12           *structure and the head of any Federal agency*  
13           *that is not a sector-specific agency with respon-*  
14           *sibilities for regulating the covered critical infra-*  
15           *structure, shall—*

16                           “(i) *consistent with the protection of*  
17                           *intelligence sources and methods and other*  
18                           *sensitive matters, inform the owner or oper-*  
19                           *ator of information infrastructure located*  
20                           *outside the United States the disruption of*  
21                           *which could result in national or regional*  
22                           *catastrophic damage in the United States*  
23                           *and the government of the country in which*  
24                           *the information infrastructure is located of*  
25                           *any cyber risks to the information infra-*

1            *structure that led to the declaration of a na-*  
2            *tional cyber emergency; and*

3            *“(ii) coordinate with the government of*  
4            *the country in which the information infra-*  
5            *structure is located and, as appropriate, the*  
6            *owner or operator of the information infra-*  
7            *structure, regarding the implementation of*  
8            *emergency measures or actions necessary to*  
9            *preserve the reliable operation, and mitigate*  
10           *or remediate the consequences of the poten-*  
11           *tial disruption, of covered critical infra-*  
12           *structure that is the subject of the national*  
13           *cyber emergency.*

14           *“(B) INTERNATIONAL AGREEMENTS.—The*  
15           *Director shall carry out this paragraph in a*  
16           *manner consistent with applicable international*  
17           *agreements.*

18           *“(d) REPORTING.—*

19           *“(1) IN GENERAL.—Except as provided in para-*  
20           *graph (2), the President shall ensure that any dec-*  
21           *laration under subsection (a)(1) or any extension*  
22           *under subsection (b)(2) is reported to the appropriate*  
23           *committees of Congress before the Director mandates*  
24           *any emergency measure or actions under subsection*  
25           *(a)(3).*

1           “(2) *EXCEPTION.*—If notice cannot be given  
2           under paragraph (1) before mandating any emer-  
3           gency measure or actions under subsection (a)(3), the  
4           President shall provide the report required under  
5           paragraph (1) as soon as possible, along with a state-  
6           ment of the reasons for not providing notice in ac-  
7           cordance with paragraph (1).

8           “(3) *CONTENTS.*—Each report under this sub-  
9           section shall describe—

10           “(A) *the nature of the national cyber emer-*  
11           *gency;*

12           “(B) *the reasons that risk-based security re-*  
13           *quirements under section 248 are not sufficient*  
14           *to address the national cyber emergency;*

15           “(C) *the actions necessary to preserve the*  
16           *reliable operation and mitigate the consequences*  
17           *of the potential disruption of covered critical in-*  
18           *frastructure; and*

19           “(D) *in the case of an extension of a na-*  
20           *tional cyber emergency under subsection (b)(2)—*

21           “(i) *why the emergency measures or*  
22           *actions continue to be necessary to address*  
23           *the national cyber emergency; and*

24           “(ii) *when the President expects the*  
25           *national cyber emergency to abate.*

1           “(e) *STATUTORY DEFENSES AND CIVIL LIABILITY LIM-*  
2 *ITATIONS FOR COMPLIANCE WITH EMERGENCY MEAS-*  
3 *URES.*—

4           “(1) *DEFINITIONS.*—*In this subsection—*

5                   “(A) *the term ‘covered civil action’—*

6                           “(i) *means a civil action filed in a*  
7 *Federal or State court against a covered en-*  
8 *tity; and*

9                           “(ii) *does not include an action*  
10 *brought under section 2520 or 2707 of title*  
11 *18, United States Code, or section 110 or*  
12 *308 of the Foreign Intelligence Surveillance*  
13 *Act of 1978 (50 U.S.C. 1810 and 1828);*

14                   “(B) *the term ‘covered entity’ means any*  
15 *entity that owns or operates covered critical in-*  
16 *frastructure, including any owner, operator, offi-*  
17 *cer, employee, agent, landlord, custodian, pro-*  
18 *vider of information technology, or other person*  
19 *acting for or on behalf of that entity with respect*  
20 *to the covered critical infrastructure; and*

21                   “(C) *the term ‘noneconomic damages’ means*  
22 *damages for losses for physical and emotional*  
23 *pain, suffering, inconvenience, physical impair-*  
24 *ment, mental anguish, disfigurement, loss of en-*  
25 *joyment of life, loss of society and companion-*

1           *ship, loss of consortium, hedonic damages, injury*  
2           *to reputation, and any other nonpecuniary*  
3           *losses.*

4           “(2) *APPLICATION OF LIMITATIONS ON CIVIL LI-*  
5           *ABILITY.—The limitations on civil liability under*  
6           *paragraph (3) apply if—*

7                   “(A) *the President has issued a declaration*  
8                   *of national cyber emergency under subsection*  
9                   *(a)(1);*

10                   “(B) *the Director has—*

11                           “(i) *issued emergency measures or ac-*  
12                           *tions for which compliance is required*  
13                           *under subsection (c)(1); or*

14                           “(ii) *approved security measures under*  
15                           *subsection (c)(2);*

16                   “(C) *the covered entity is in compliance*  
17                   *with—*

18                           “(i) *the emergency measures or actions*  
19                           *required under subsection (c)(1); or*

20                           “(ii) *security measures which the Di-*  
21                           *rector has approved under subsection (c)(2);*  
22                           *and*

23                           “(D)(i) *the Director certifies to the court in*  
24                           *which the covered civil action is pending that the*  
25                           *actions taken by the covered entity during the*

1           *period covered by the declaration under sub-*  
2           *section (a)(1) were consistent with—*

3                   *“(I) emergency measures or actions for*  
4                   *which compliance is required under sub-*  
5                   *section (c)(1); or*

6                   *“(II) security measures which the Di-*  
7                   *rector has approved under subsection (c)(2);*  
8                   *or*

9                   *“(ii) notwithstanding the lack of a certifi-*  
10                  *cation, the covered entity demonstrates by a pre-*  
11                  *ponderance of the evidence that the actions taken*  
12                  *during the period covered by the declaration*  
13                  *under subsection (a)(1) are consistent with the*  
14                  *implementation of—*

15                  *“(I) emergency measures or actions for*  
16                  *which compliance is required under sub-*  
17                  *section (c)(1); or*

18                  *“(II) security measures which the Di-*  
19                  *rector has approved under subsection (c)(2).*

20                  *“(3) LIMITATIONS ON CIVIL LIABILITY.—In any*  
21                  *covered civil action that is related to any incident as-*  
22                  *sociated with a cyber risk covered by a declaration of*  
23                  *a national cyber emergency and for which Director*  
24                  *has issued emergency measures or actions for which*  
25                  *compliance is required under subsection (c)(1) or for*

1       *which the Director has approved security measures*  
2       *under subsection (c)(2), or that is the direct con-*  
3       *sequence of actions taken in good faith for the purpose*  
4       *of implementing security measures or actions which*  
5       *the Director has approved under subsection (c)(2)—*

6               “(A) *the covered entity shall not be liable*  
7               *for any punitive damages intended to punish or*  
8               *deter, exemplary damages, or other damages not*  
9               *intended to compensate a plaintiff for actual*  
10              *losses; and*

11              “(B) *noneconomic damages may be awarded*  
12              *against a defendant only in an amount directly*  
13              *proportional to the percentage of responsibility of*  
14              *such defendant for the harm to the plaintiff, and*  
15              *no plaintiff may recover noneconomic damages*  
16              *unless the plaintiff suffered physical harm.*

17              “(4) *CIVIL ACTIONS ARISING OUT OF IMPLEMEN-*  
18              *TATION OF EMERGENCY MEASURES OR ACTIONS.—A*  
19              *covered civil action may not be maintained against*  
20              *a covered entity that is the direct consequence of ac-*  
21              *tions taken in good faith for the purpose of imple-*  
22              *menting specific emergency measures or actions for*  
23              *which compliance is required under subsection (c)(1),*  
24              *if—*

1           “(A) the President has issued a declaration  
2 of national cyber emergency under subsection  
3 (a)(1) and the action was taken during the pe-  
4 riod covered by that declaration;

5           “(B) the Director has issued emergency  
6 measures or actions for which compliance is re-  
7 quired under subsection (c)(1) or that the Direc-  
8 tor has approved under subsection (c)(2);

9           “(C) the covered entity is in compliance  
10 with the emergency measures required under sub-  
11 section (c)(1) or that the Director has approved  
12 under subsection (c)(2); and

13           “(D)(i) the Director certifies to the court in  
14 which the covered civil action is pending that the  
15 actions taken by the entity during the period  
16 covered by the declaration under subsection  
17 (a)(1) were consistent with the implementation  
18 of emergency measures or actions for which com-  
19 pliance is required under subsection (c)(1) or  
20 that the Director has approved under subsection  
21 (c)(2); or

22           “(ii) notwithstanding the lack of a certifi-  
23 cation, the entity demonstrates by a preponder-  
24 ance of the evidence that the actions taken dur-  
25 ing the period covered by the declaration under

1            *subsection (a)(1) are consistent with the imple-*  
 2            *mentation of emergency measures or actions for*  
 3            *which compliance is required under subsection*  
 4            *(c)(1) or that the Director has approved under*  
 5            *subsection (c)(2).*

6            *“(5) CERTAIN ACTIONS NOT SUBJECT TO LIMITA-*  
 7            *TIONS ON LIABILITY.—*

8            *“(A) ADDITIONAL OR INTERVENING ACTS.—*  
 9            *Paragraphs (2) through (4) shall not apply to a*  
 10           *civil action relating to any additional or inter-*  
 11           *vening acts or omissions by any covered entity.*

12           *“(B) SERIOUS OR SUBSTANTIAL DAMAGE.—*  
 13           *Paragraph (4) shall not apply to any civil ac-*  
 14           *tion brought by an individual—*

15           *“(i) whose recovery is otherwise pre-*  
 16           *cluded by application of paragraph (4); and*

17           *“(ii) who has suffered—*

18           *“(I) serious physical injury or*  
 19           *death; or*

20           *“(II) substantial damage or de-*  
 21           *struction to his primary residence.*

22           *“(C) RULE OF CONSTRUCTION.—Recovery*  
 23           *available under subparagraph (B) shall be lim-*  
 24           *ited to those damages available under subpara-*  
 25           *graphs (A) and (B) of paragraph (3), except that*

1           *neither reasonable and necessary medical benefits*  
2           *nor lifetime total benefits for lost employment in-*  
3           *come due to permanent and total disability shall*  
4           *be limited herein.*

5           “(D) *INDEMNIFICATION.*—*In any civil ac-*  
6           *tion brought under subparagraph (B), the*  
7           *United States shall defend and indemnify any*  
8           *covered entity. Any covered entity defended and*  
9           *indemnified under this subparagraph shall fully*  
10          *cooperate with the United States in the defense*  
11          *by the United States in any proceeding and shall*  
12          *be reimbursed the reasonable costs associated*  
13          *with such cooperation.*

14          “(f) *JOINT RESOLUTION TO EXTEND CYBER EMER-*  
15          *GENCY.*—

16                 “(1) *IN GENERAL.*—*For purposes of subsection*  
17                 *(b)(2)(B), a joint resolution described in this para-*  
18                 *graph means only a joint resolution—*

19                         “(A) *the title of which is as follows: ‘Joint*  
20                         *resolution approving the extension of a cyber*  
21                         *emergency’; and*

22                         “(B) *the matter after the resolving clause of*  
23                         *which is as follows: ‘That Congress approves the*  
24                         *continuation of the emergency measure or action*  
25                         *issued by the Director of the National Center for*

1           *Cybersecurity and Communications on*  
2           \_\_\_\_\_ *for not longer than*  
3           *an additional 120-day period.*’, the blank space  
4           *being filled in with the date on which the emer-*  
5           *gency measure or action to which the joint reso-*  
6           *lution applies was issued.*

7           “(2) *PROCEDURE.*—

8                   “(A) *NO REFERRAL.*—*A joint resolution de-*  
9                   *scribed in paragraph (1) shall not be referred to*  
10                   *a committee in either House of Congress and*  
11                   *shall immediately be placed on the calendar.*

12                   “(B) *CONSIDERATION.*—

13                           “(i) *DEBATE LIMITATION.*—*A motion*  
14                           *to proceed to a joint resolution described in*  
15                           *paragraph (1) is highly privileged in the*  
16                           *House of Representatives and is privileged*  
17                           *in the Senate and is not debatable. The mo-*  
18                           *tion is not subject to a motion to postpone.*  
19                           *In the Senate, consideration of the joint res-*  
20                           *olution, and on all debatable motions and*  
21                           *appeals in connection therewith, shall be*  
22                           *limited to not more than 10 hours, which*  
23                           *shall be divided equally between the major-*  
24                           *ity leader and the minority leader, or their*  
25                           *designees. A motion further to limit debate*

1           *is in order and not debatable. All points of*  
2           *order against the joint resolution (and*  
3           *against consideration of the joint resolu-*  
4           *tion) are waived. An amendment to, or a*  
5           *motion to postpone, or a motion to proceed*  
6           *to the consideration of other business, or a*  
7           *motion to recommit the joint resolution is*  
8           *not in order.*

9           “(ii) *PASSAGE.*—*In the Senate, imme-*  
10          *diately following the conclusion of the de-*  
11          *bate on a joint resolution described in para-*  
12          *graph (1), and a single quorum call at the*  
13          *conclusion of the debate if requested in ac-*  
14          *cordance with the rules of the Senate, the*  
15          *vote on passage of the joint resolution shall*  
16          *occur.*

17          “(iii) *APPEALS.*—*Appeals from the de-*  
18          *isions of the Chair relating to the applica-*  
19          *tion of the rules of the Senate to the proce-*  
20          *dure relating to a joint resolution described*  
21          *in paragraph (1) shall be decided without*  
22          *debate.*

23          “(C) *OTHER HOUSE ACTS FIRST.*—*If, before*  
24          *the passage by 1 House of a joint resolution of*  
25          *that House described in paragraph (1), that*

1           *House receives from the other House a joint reso-*  
2           *lution described in paragraph (1)—*

3                     “(i) *the procedure in that House shall*  
4                     *be the same as if no joint resolution had*  
5                     *been received from the other House; and*

6                     “(ii) *the vote on final passage shall be*  
7                     *on the joint resolution of the other House.*

8                     “(D) *MAJORITY REQUIRED FOR ADOPTI-*  
9                     *ON.—A joint resolution considered under this*  
10                    *subsection shall require an affirmative vote of a*  
11                    *majority of the Members, duly chosen and sworn,*  
12                    *for adoption.*

13                    “(3) *RULEMAKING.—This subsection is enacted*  
14                    *by Congress—*

15                             “(A) *as an exercise of the rulemaking power*  
16                             *of the Senate and the House of Representatives,*  
17                             *respectively, and is deemed to be part of the rules*  
18                             *of each House, respectively but applicable only*  
19                             *with respect to the procedure to be followed in*  
20                             *that House in the case of a joint resolution de-*  
21                             *scribed in paragraph (1), and it supersedes other*  
22                             *rules only to the extent that it is inconsistent*  
23                             *with such rules; and*

24                             “(B) *with full recognition of the constitu-*  
25                             *tional right of either House to change the rules*

1           *(so far as they relate to the procedure of that*  
2           *House) at any time, in the same manner, and*  
3           *to the same extent as in the case of any other*  
4           *rule of that House.*

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

7                   “(1) *alter or supersede the authority of the Sec-*  
8                   *retary of Defense, the Attorney General, or the Direc-*  
9                   *tor of National Intelligence in responding to a na-*  
10                   *tional cyber emergency; or*

11                   “(2) *limit the authority of the Director under*  
12                   *section 248, after a declaration issued under this sec-*  
13                   *tion expires.*

14           **“SEC. 250. ENFORCEMENT.**

15                   “(a) *ANNUAL CERTIFICATION OF COMPLIANCE.*—

16                   “(1) *IN GENERAL.*—*Not later than 6 months*  
17                   *after the date on which the Director promulgates reg-*  
18                   *ulations under section 248(b), and every year there-*  
19                   *after, each owner or operator of covered critical infra-*  
20                   *structure shall certify in writing to the Director*  
21                   *whether the owner or operator has developed and im-*  
22                   *plemented, or is implementing, security measures ap-*  
23                   *proved by the Director under section 248 and any ap-*  
24                   *plicable emergency measures or actions required*

1        *under section 249 for any cyber risks and national*  
2        *cyber emergencies.*

3            “(2) *FAILURE TO COMPLY.—If an owner or oper-*  
4        *ator of covered critical infrastructure fails to submit*  
5        *a certification in accordance with paragraph (1), or*  
6        *if the certification indicates the owner or operator is*  
7        *not in compliance, the Director may issue an order*  
8        *requiring the owner or operator to submit proposed*  
9        *security measures under section 248 or comply with*  
10       *specific emergency measures or actions under section*  
11       *249.*

12       “(b) *RISK-BASED EVALUATIONS.—*

13            “(1) *IN GENERAL.—Consistent with the factors*  
14        *described in paragraph (3), the Director may perform*  
15        *an evaluation of the information infrastructure of*  
16        *any specific system or asset constituting covered crit-*  
17        *ical infrastructure to assess the validity of a certifi-*  
18        *cation of compliance submitted under subsection*  
19        *(a)(1).*

20            “(2) *DOCUMENT REVIEW AND INSPECTION.—An*  
21        *evaluation performed under paragraph (1) may in-*  
22        *clude—*

23            “(A) *a review of all documentation sub-*  
24        *mitted to justify an annual certification of com-*  
25        *pliance submitted under subsection (a)(1); and*

1           “(B) a physical or electronic inspection of  
2           relevant information infrastructure to which the  
3           security measures required under section 248 or  
4           the emergency measures or actions required  
5           under section 249 apply.

6           “(3) *EVALUATION SELECTION FACTORS.*—In de-  
7           termining whether sufficient risk exists to justify an  
8           evaluation under this subsection, the Director shall  
9           consider—

10           “(A) the specific cyber risks affecting or po-  
11           tentially affecting the information infrastructure  
12           of the specific system or asset constituting cov-  
13           ered critical infrastructure;

14           “(B) any reliable intelligence or other infor-  
15           mation indicating a cyber risk or credible na-  
16           tional cyber emergency to the information infra-  
17           structure of the specific system or asset consti-  
18           tuting covered critical infrastructure;

19           “(C) actual knowledge or reasonable sus-  
20           picion that the certification of compliance sub-  
21           mitted by a specific owner or operator of covered  
22           critical infrastructure is false or otherwise inac-  
23           curate;

1           “(D) a request by a specific owner or oper-  
2           ator of covered critical infrastructure for such an  
3           evaluation; and

4           “(E) such other risk-based factors as identi-  
5           fied by the Director.

6           “(4) *SECTOR-SPECIFIC AGENCIES.*—To carry out  
7           the risk-based evaluation authorized under this sub-  
8           section, the Director may use the resources of a sector-  
9           specific agency with responsibility for the covered  
10          critical infrastructure or any Federal agency that is  
11          not a sector-specific agency with responsibilities for  
12          regulating the covered critical infrastructure with the  
13          concurrence of the head of the agency.

14          “(5) *INFORMATION PROTECTION.*—Information  
15          provided to the Director during the course of an eval-  
16          uation under this subsection shall be protected from  
17          disclosure in accordance with section 251.

18          “(c) *CIVIL PENALTIES.*—

19                 “(1) *IN GENERAL.*—Any person who violates sec-  
20                 tion 248 or 249 shall be liable for a civil penalty.

21                 “(2) *NO PRIVATE RIGHT OF ACTION.*—Nothing in  
22                 this section confers upon any person, except the Di-  
23                 rector, a right of action against an owner or operator  
24                 of covered critical infrastructure to enforce any provi-  
25                 sion of this subtitle.

1 “(d) *LIMITATION ON CIVIL LIABILITY.*—

2 “(1) *DEFINITION.*—*In this subsection—*

3 “(A) *the term ‘covered civil action’—*

4 “(i) *means a civil action filed in a*  
5 *Federal or State court against a covered en-*  
6 *tity; and*

7 “(ii) *does not include an action*  
8 *brought under section 2520 or 2707 of title*  
9 *18, United States Code, or section 110 or*  
10 *308 of the Foreign Intelligence Surveillance*  
11 *Act of 1978 (50 U.S.C. 1810 and 1828);*

12 “(B) *the term ‘covered entity’ means any*  
13 *entity that owns or operates covered critical in-*  
14 *frastructure, including any owner, operator, offi-*  
15 *cer, employee, agent, landlord, custodian, pro-*  
16 *vider of information technology, or other person*  
17 *acting for or on behalf of that entity with respect*  
18 *to the covered critical infrastructure; and*

19 “(C) *the term ‘noneconomic damages’ means*  
20 *damages for losses for physical and emotional*  
21 *pain, suffering, inconvenience, physical impair-*  
22 *ment, mental anguish, disfigurement, loss of en-*  
23 *joyment of life, loss of society and companion-*  
24 *ship, loss of consortium, hedonic damages, injury*

1           to reputation, and any other nonpecuniary  
2           losses.

3           “(2) *LIMITATIONS ON CIVIL LIABILITY.*—If a cov-  
4           ered entity experiences an incident related to a cyber  
5           risk identified under section 248(a), in any covered  
6           civil action for damages directly caused by the inci-  
7           dent related to that cyber risk—

8                   “(A) the covered entity shall not be liable  
9                   for any punitive damages intended to punish or  
10                  deter, exemplary damages, or other damages not  
11                  intended to compensate a plaintiff for actual  
12                  losses; and

13                   “(B) noneconomic damages may be awarded  
14                   against a defendant only in an amount directly  
15                   proportional to the percentage of responsibility of  
16                   such defendant for the harm to the plaintiff, and  
17                   no plaintiff may recover noneconomic damages  
18                   unless the plaintiff suffered physical harm.

19           “(3) *APPLICATION.*—This subsection shall apply  
20           to claims made by any individual or nongovern-  
21           mental entity, including claims made by a State or  
22           local government agency on behalf of such individuals  
23           or nongovernmental entities, against a covered enti-  
24           ty—

1           “(A) whose proposed security measures, or  
2           combination thereof, satisfy the security perform-  
3           ance requirements established under subsection  
4           248(b) and have been approved by the Director;

5           “(B) that has been evaluated under sub-  
6           section (b) and has been found by the Director  
7           to have implemented the proposed security meas-  
8           ures approved under section 248; and

9           “(C) that is in actual compliance with the  
10          approved security measures at the time of the in-  
11          cident related to that cyber risk.

12          “(4) *LIMITATION.*—This subsection shall only  
13          apply to harm directly caused by the incident related  
14          to the cyber risk and shall not apply to damages  
15          caused by any additional or intervening acts or omis-  
16          sions by the covered entity.

17          “(5) *RULE OF CONSTRUCTION.*—Except as pro-  
18          vided under paragraph (3), nothing in this subsection  
19          shall be construed to abrogate or limit any right, rem-  
20          edy, or authority that the Federal Government or any  
21          State or local government, or any entity or agency  
22          thereof, may possess under any law, or that any indi-  
23          vidual is authorized by law to bring on behalf of the  
24          government.

1       “(e) *REPORT TO CONGRESS.*—*The Director shall sub-*  
 2 *mit an annual report to the appropriate committees of Con-*  
 3 *gress on the implementation and enforcement of the risk-*  
 4 *based performance requirements of covered critical infra-*  
 5 *structure under subsection 248(b) and this section includ-*  
 6 *ing—*

7               “(1) *the level of compliance of covered critical in-*  
 8 *frastructure with the risk-based security performance*  
 9 *requirements issued under section 248(b);*

10              “(2) *how frequently the evaluation authority*  
 11 *under subsection (b) was utilized and a summary of*  
 12 *the aggregate results of the evaluations; and*

13              “(3) *any civil penalties imposed on covered crit-*  
 14 *ical infrastructure.*

15 **“SEC. 251. PROTECTION OF INFORMATION.**

16       “(a) *DEFINITION.*—*In this section, the term ‘covered*  
 17 *information’—*

18              “(1) *means—*

19                      “(A) *any information required to be sub-*  
 20 *mitted under sections 246, 248, and 249 to the*  
 21 *Center by the owners and operators of covered*  
 22 *critical infrastructure; and*

23                      “(B) *any information submitted to the Cen-*  
 24 *ter under the processes and procedures estab-*  
 25 *lished under section 246 by State and local gov-*

1            *ernments, private entities, and international*  
2            *partners of the United States regarding threats,*  
3            *vulnerabilities, and incidents affecting—*

4                    *“(i) the Federal information infra-*  
5                    *structure;*

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

11                   *“(iii) the national information infra-*  
12                   *structure; and*

13                   *“(2) shall not include any information described*  
14                   *under paragraph (1), if that information is submitted*  
15                   *to—*

16                    *“(A) conceal violations of law, inefficiency,*  
17                    *or administrative error;*

18                    *“(B) prevent embarrassment to a person,*  
19                    *organization, or agency; or*

20                    *“(C) interfere with competition in the pri-*  
21                    *vate sector.*

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

1 214, except that the requirement of section 214 that the in-  
2 formation be voluntarily submitted, including the require-  
3 ment for an express statement, shall not be required for sub-  
4 missions of covered information.

5 “(c) *GUIDELINES.*—

6 “(1) *IN GENERAL.*—Subject to paragraph (2), the  
7 Director shall develop and issue guidelines, in con-  
8 sultation with the Secretary, Attorney General, and  
9 the National Cybersecurity Advisory Council, as nec-  
10 essary to implement this section.

11 “(2) *REQUIREMENTS.*—The guidelines developed  
12 under this section shall—

13 “(A) consistent with section 214(e)(2)(D)  
14 and (g) and the processes, procedures, and guide-  
15 lines developed under section 246(b), include pro-  
16 visions for information sharing among Federal,  
17 State, and local and officials, private entities, or  
18 international partners of the United States nec-  
19 essary to carry out the authorities and respon-  
20 sibilities of the Director;

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

1           to marking, safeguarding, dissemination and  
2           dispute resolution; and

3                   “(C) describe, with as much detail as pos-  
4                   sible, the categories and type of information enti-  
5                   ties should voluntarily submit under subsections  
6                   (b) and (c)(1)(B) of section 246.

7           “(d) *PROCESS FOR REPORTING SECURITY PROB-*  
8 *LEMS.—*

9                   “(1) *ESTABLISHMENT OF PROCESS.—The Direc-*  
10                  *tor shall establish through regulation, and provide in-*  
11                  *formation to the public regarding, a process by which*  
12                  *any person may submit a report to the Secretary re-*  
13                  *garding cybersecurity threats, vulnerabilities, and in-*  
14                  *cidents affecting—*

15                           “(A) *the Federal information infrastructure;*

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

21                           “(C) *national information infrastructure.*

22                   “(2) *ACKNOWLEDGMENT OF RECEIPT.—If a re-*  
23                  *port submitted under paragraph (1) identifies the*  
24                  *person making the report, the Director shall respond*

1       *promptly to such person and acknowledge receipt of*  
2       *the report.*

3           “(3) *STEPS TO ADDRESS PROBLEM.*—*The Direc-*  
4       *tor shall review and consider the information pro-*  
5       *vided in any report submitted under paragraph (1)*  
6       *and, at the sole, unreviewable discretion of the Direc-*  
7       *tor, determine what, if any, steps are necessary or ap-*  
8       *propriate to address any problems or deficiencies*  
9       *identified.*

10          “(4) *DISCLOSURE OF IDENTITY.*—

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

16           “(B) *REFERRAL TO THE ATTORNEY GEN-*  
17       *ERAL.*—*The Secretary shall disclose to the Attor-*  
18       *ney General the identity of a person described*  
19       *under subparagraph (A) if the matter is referred*  
20       *to the Attorney General for enforcement. The Di-*  
21       *rector shall provide reasonable advance notice to*  
22       *the affected person if disclosure of that person’s*  
23       *identity is to occur, unless such notice would risk*  
24       *compromising a criminal or civil enforcement*  
25       *investigation or proceeding.*

1       “(e) *RULES OF CONSTRUCTION.*—*Nothing in this sec-*  
2 *tion shall be construed to—*

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

7               “(2) *prevent the classification of information*  
8 *submitted under this section if that information meets*  
9 *the standards for classification under Executive Order*  
10 *12958 or any successor of that order or affect meas-*  
11 *ures and controls relating to the protection of classi-*  
12 *fied information as prescribed by Federal statute or*  
13 *under Executive Order 12958, or any successor of that*  
14 *order;*

15               “(3) *limit the right of an individual to make*  
16 *any disclosure—*

17                       “(A) *protected or authorized under section*  
18 *2302(b)(8) or 7211 of title 5, United States Code;*

19                       “(B) *to an appropriate official of informa-*  
20 *tion that the individual reasonably believes evi-*  
21 *dences a violation of any law, rule, or regula-*  
22 *tion, gross mismanagement, or substantial and*  
23 *specific danger to public health, safety, or secu-*  
24 *rity, and that is protected under any Federal or*  
25 *State law (other than those referenced in sub-*

1           *paragraph (A)) that shields the disclosing indi-*  
2           *vidual against retaliation or discrimination for*  
3           *having made the disclosure if such disclosure is*  
4           *not specifically prohibited by law and if such in-*  
5           *formation is not specifically required by Execu-*  
6           *tive order to be kept secret in the interest of na-*  
7           *tional defense or the conduct of foreign affairs; or*

8           *“(C) to the Special Counsel, the inspector*  
9           *general of an agency, or any other employee des-*  
10          *ignated by the head of an agency to receive simi-*  
11          *lar disclosures;*

12          *“(4) prevent the Director from using information*  
13          *required to be submitted under sections 246, 248, or*  
14          *249 for enforcement of this subtitle, including enforce-*  
15          *ment proceedings subject to appropriate safeguards;*

16          *“(5) authorize information to be withheld from*  
17          *Congress, the Government Accountability Office, or*  
18          *Inspector General of the Department;*

19          *“(6) affect protections afforded to trade secrets*  
20          *under any other provision of law; or*

21          *“(7) create a private right of action for enforce-*  
22          *ment of any provision of this section.*

23          *“(f) AUDIT.—*

24          *“(1) IN GENERAL.—Not later than 1 year after*  
25          *the date of enactment of the Protecting Cyberspace as*

1        *a National Asset Act of 2010, the Inspector General*  
2        *of the Department shall conduct an audit of the man-*  
3        *agement of information submitted under subsection*  
4        *(b) and report the findings to appropriate committees*  
5        *of Congress.*

6            *“(2) CONTENTS.—The audit under paragraph*  
7        *(1) shall include assessments of—*

8            *“(A) whether the information is adequately*  
9        *safeguarded against inappropriate disclosure;*

10           *“(B) the processes for marking and dissemi-*  
11        *inating the information and resolving any dis-*  
12        *putes;*

13           *“(C) how the information is used for the*  
14        *purposes of this section, and whether that use is*  
15        *effective;*

16           *“(D) whether information sharing has been*  
17        *effective to fulfill the purposes of this section;*

18           *“(E) whether the kinds of information sub-*  
19        *mitted have been appropriate and useful, or*  
20        *overbroad or overnarrow;*

21           *“(F) whether the information protections*  
22        *allow for adequate accountability and trans-*  
23        *parency of the regulatory, enforcement, and other*  
24        *aspects of implementing this subtitle; and*

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

3   **“SEC. 252. SECTOR-SPECIFIC AGENCIES.**

4           “(a) *IN GENERAL.*—The head of each sector-specific  
5 agency and the head of any Federal agency that is not a  
6 sector-specific agency with responsibilities for regulating  
7 covered critical infrastructure shall coordinate with the Di-  
8 rector on any activities of the sector-specific agency or Fed-  
9 eral agency that relate to the efforts of the agency regarding  
10 security or resiliency of the national information infra-  
11 structure, including critical infrastructure and covered crit-  
12 ical infrastructure, within or under the supervision of the  
13 agency.

14          “(b) *DUPLICATIVE REPORTING REQUIREMENTS.*—The  
15 head of each sector-specific agency and the head of any Fed-  
16 eral agency that is not a sector-specific agency with respon-  
17 sibilities for regulating covered critical infrastructure shall  
18 coordinate with the Director to eliminate and avoid the cre-  
19 ation of duplicate reporting or compliance requirements re-  
20 lating to the security or resiliency of the national informa-  
21 tion infrastructure, including critical infrastructure and  
22 covered critical infrastructure, within or under the super-  
23 vision of the agency.

24          “(c) *REQUIREMENTS.*—

1           “(1) *IN GENERAL.*—*To the extent that the head*  
2 *of each sector-specific agency and the head of any*  
3 *Federal agency that is not a sector-specific agency*  
4 *with responsibilities for regulating covered critical in-*  
5 *frastructure has the authority to establish regulations,*  
6 *rules, or requirements or other required actions that*  
7 *are applicable to the security of national information*  
8 *infrastructure, including critical infrastructure and*  
9 *covered critical infrastructure, the head of that agency*  
10 *shall—*

11                   “(A) *notify the Director in a timely fashion*  
12 *of the intent to establish the regulations, rules,*  
13 *requirements, or other required actions;*

14                   “(B) *coordinate with the Director to ensure*  
15 *that the regulations, rules, requirements, or other*  
16 *required actions are consistent with, and do not*  
17 *conflict or impede, the activities of the Director*  
18 *under sections 247, 248, and 249; and*

19                   “(C) *in coordination with the Director, en-*  
20 *sure that the regulations, rules, requirements, or*  
21 *other required actions are implemented, as they*  
22 *relate to covered critical infrastructure, in ac-*  
23 *cordance with subsection (a).*

24           “(2) *COORDINATION.*—*Coordination under para-*  
25 *graph (1)(B) shall include the active participation of*

1       *the Director in the process for developing regulations,*  
2       *rules, requirements, or other required actions.*

3               “(3) *RULE OF CONSTRUCTION.*—*Nothing in this*  
4       *section shall be construed to provide additional au-*  
5       *thority for any sector-specific agency or any Federal*  
6       *agency that is not a sector-specific agency with re-*  
7       *sponsibilities for regulating national information in-*  
8       *frastructure, including critical infrastructure or cov-*  
9       *ered critical infrastructure, to establish standards or*  
10       *other measures that are applicable to the security of*  
11       *national information infrastructure not otherwise au-*  
12       *thorized by law.*

13       **“SEC. 253. STRATEGY FOR FEDERAL CYBERSECURITY SUP-**  
14               **PLY CHAIN MANAGEMENT.**

15               “(a) *IN GENERAL.*—*The Secretary, in consultation*  
16       *with the Director of Cyberspace Policy, the Director, the*  
17       *Secretary of Defense, the Secretary of Commerce, the Sec-*  
18       *retary of State, the Director of National Intelligence, the*  
19       *Administrator of General Services, the Administrator for*  
20       *Federal Procurement Policy, the other members of the Chief*  
21       *Information Officers Council established under section 3603*  
22       *of title 44, United States Code, the Chief Acquisition Offi-*  
23       *cers Council established under section 16A of the Office of*  
24       *Federal Procurement Policy Act (41 U.S.C. 414b), the Chief*  
25       *Financial Officers Council established under section 302 of*

1 *the Chief Financial Officers Act of 1990 (31 U.S.C. 901*  
2 *note), and the private sector, shall develop, periodically up-*  
3 *date, and implement a supply chain risk management*  
4 *strategy designed to ensure, based on mission criticality*  
5 *and cost effectiveness, the security of the Federal informa-*  
6 *tion infrastructure, including protection against unauthor-*  
7 *ized access to, alteration of information in, disruption of*  
8 *operations of, interruption of communications or services*  
9 *of, and insertion of malicious software, engineering*  
10 *vulnerabilities, or otherwise corrupting software, hardware,*  
11 *services, or products intended for use in Federal informa-*  
12 *tion infrastructure.*

13       “(b) *CONTENTS.—The supply chain risk management*  
14 *strategy developed under subsection (a) shall—*

15               “(1) *address risks in the supply chain during the*  
16 *entire life cycle of any part of the Federal informa-*  
17 *tion infrastructure;*

18               “(2) *place particular emphasis on—*

19                       “(A) *securing critical information systems*  
20 *and the Federal information infrastructure;*

21                       “(B) *developing processes that—*

22                               “(i) *incorporate all-source intelligence*  
23 *analysis into assessments of the supply*  
24 *chain for the Federal information infra-*  
25 *structure;*

1           “(ii) assess risks from potential sup-  
2 pliers providing critical components or  
3 services of the Federal information infra-  
4 structure;

5           “(iii) assess risks from individual com-  
6 ponents, including all subcomponents, or  
7 software used in or affecting the Federal in-  
8 formation infrastructure;

9           “(iv) manage the quality, configura-  
10 tion, and security of software, hardware,  
11 and systems of the Federal information in-  
12 frastructure throughout the life cycle of the  
13 software, hardware, or system, including  
14 components or subcomponents from sec-  
15 ondary and tertiary sources;

16           “(v) detect the occurrence, reduce the  
17 likelihood of occurrence, and mitigate or re-  
18 mediate the risks associated with products  
19 containing counterfeit components or mali-  
20 cious functions;

21           “(vi) enhance developmental and oper-  
22 ational test and evaluation capabilities, in-  
23 cluding software vulnerability detection  
24 methods and automated methods and tools  
25 that shall be integrated into acquisition pol-

1            *icy practices by Federal agencies and, where*  
2            *appropriate, make the capabilities available*  
3            *for use by the private sector; and*

4            *“(vii) protect the intellectual property*  
5            *and trade secrets of suppliers of information*  
6            *and communications technology products*  
7            *and services;*

8            *“(C) the use of internationally-recognized*  
9            *standards and standards developed by the pri-*  
10           *ivate sector and developing a process, with the*  
11           *National Institute for Standards and Tech-*  
12           *nology, to make recommendations for improve-*  
13           *ments of the standards;*

14           *“(D) identifying acquisition practices of*  
15           *Federal agencies that increase risks in the sup-*  
16           *ply chain and developing a process to provide*  
17           *recommendations for revisions to those processes;*  
18           *and*

19           *“(E) sharing with the private sector, to the*  
20           *fullest extent possible, the threats identified in*  
21           *the supply chain and working with the private*  
22           *sector to develop responses to those threats as*  
23           *identified; and*

24           *“(3) to the maximum extent practicable, promote*  
25           *the ability of Federal agencies to procure authentic*

1       *commercial off the shelf information and communica-*  
2       *tions technology products and services from a diverse*  
3       *pool of suppliers.*

4       “(c) *IMPLEMENTATION.*—*The Federal Acquisition Reg-*  
5       *ulatory Council established under section 25(a) of the Office*  
6       *of Federal Procurement Policy Act (41 U.S.C. 421(a))*  
7       *shall—*

8               “(1) *amend the Federal Acquisition Regulation*  
9       *issued under section 25 of that Act to—*

10                   “(A) *incorporate, where relevant, the supply*  
11       *chain risk management strategy developed under*  
12       *subsection (a) to improve security throughout the*  
13       *acquisition process; and*

14                   “(B) *direct that all software and hardware*  
15       *purchased by the Federal Government shall com-*  
16       *ply with standards developed or be interoperable*  
17       *with automated tools approved by the National*  
18       *Institute of Standards and Technology, to con-*  
19       *tinually enhance security; and*

20               “(2) *develop a clause or set of clauses for inclu-*  
21       *sion in solicitations, contracts, and task and delivery*  
22       *orders that sets forth the responsibility of the con-*  
23       *tractor under the Federal Acquisition Regulation pro-*  
24       *visions implemented under this subsection.*

1       “(d) *PREFERENCES FOR ACQUISITION OF COMMER-*  
 2 *CIAL ITEMS.—The strategy developed under this section,*  
 3 *and any actions taken under subsection (c), shall be con-*  
 4 *sistent with the preferences for the acquisition of commer-*  
 5 *cial items under section 2377 of title 10, United States*  
 6 *Code, and section 314B of the Federal Property and Admin-*  
 7 *istrative Services Act of 1949 (41 U.S.C. 264b).”.*

8       ***TITLE III—FEDERAL INFORMA-***  
 9       ***TION SECURITY MANAGE-***  
 10       ***MENT***

11       ***SEC. 301. COORDINATION OF FEDERAL INFORMATION POL-***  
 12       ***ICY.***

13       (a) *FINDINGS.—Congress finds that—*

14               (1) *since 2002 the Federal Government has experi-*  
 15 *enced multiple high-profile incidents that resulted*  
 16 *in the theft of sensitive information amounting to*  
 17 *more than the entire print collection contained in the*  
 18 *Library of Congress, including personally identifiable*  
 19 *information, advanced scientific research, and*  
 20 *prenegotiated United States diplomatic positions; and*

21               (2) *chapter 35 of title 44, United States Code,*  
 22 *must be amended to increase the coordination of Fed-*  
 23 *eral agency activities and to enhance situational*  
 24 *awareness throughout the Federal Government using*

1 *more effective enterprise-wide automated monitoring,*  
2 *detection, and response capabilities.*

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

6 *“SUBCHAPTER II—INFORMATION SECURITY*

7 *“§ 3550. Purposes*

8 *“The purposes of this subchapter are to—*

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

14 *“(2) recognize the highly networked nature of the*  
15 *current Federal information infrastructure and pro-*  
16 *vide effective Government-wide management and over-*  
17 *sight of the related information security risks, includ-*  
18 *ing coordination of information security efforts*  
19 *throughout the civilian, national security, and law*  
20 *enforcement communities;*

21 *“(3) provide for development and maintenance of*  
22 *prioritized and risk-based security controls required*  
23 *to protect Federal information infrastructure and in-*  
24 *formation systems; and*

1           “(4) provide a mechanism for improved oversight  
2 of Federal agency information security programs.

3           “(5) acknowledge that commercially developed  
4 information security products offer advanced, dy-  
5 namic, robust, and effective information security solu-  
6 tions, reflecting market solutions for the protection of  
7 critical information infrastructures important to the  
8 national defense and economic security of the Nation  
9 that are designed, built, and operated by the private  
10 sector; and

11           “(6) recognize that the selection of specific tech-  
12 nical hardware and software information security so-  
13 lutions should be left to individual agencies from  
14 among commercially developed products.

15 **“§ 3551. Definitions**

16           “(a) *IN GENERAL.*—Except as provided under sub-  
17 section (b), the definitions under section 3502 shall apply  
18 to this subchapter.

19           “(b) *ADDITIONAL DEFINITIONS.*—In this subchapter:

20           “(1) The term ‘agency information infrastruc-  
21 ture’—

22           “(A) means information infrastructure that  
23 is owned, operated, controlled, or licensed for use  
24 by, or on behalf of, an agency, including infor-

1            *mation systems used or operated by another enti-*  
2            *ty on behalf of the agency; and*

3            *“(B) does not include national security sys-*  
4            *tems.*

5            *“(2) The term ‘automated and continuous moni-*  
6            *toring’ means monitoring at a frequency and suffi-*  
7            *ciency such that the data exchange requires little to*  
8            *no human involvement and is not interrupted;*

9            *“(3) The term ‘incident’ means an occurrence*  
10          *that—*

11            *“(A) actually or imminently jeopardizes—*

12            *“(i) the information security of infor-*  
13            *mation infrastructure; or*

14            *“(ii) the information that information*  
15            *infrastructure processes, stores, receives, or*  
16            *transmits; or*

17            *“(B) constitutes a violation of security poli-*  
18            *cies, security procedures, or acceptable use poli-*  
19            *cies applicable to information infrastructure.*

20            *“(4) The term ‘information infrastructure’*  
21            *means the underlying framework that information*  
22            *systems and assets rely on to process, transmit, re-*  
23            *ceive, or store information electronically, including*  
24            *programmable electronic devices and communications*

1 *networks and any associated hardware, software, or*  
2 *data.*

3 “(5) *The term ‘information security’ means pro-*  
4 *tecting information and information systems from*  
5 *disruption or unauthorized access, use, disclosure,*  
6 *modification, or destruction in order to provide—*

7 “(A) *integrity, by guarding against im-*  
8 *proper information modification or destruction,*  
9 *including by ensuring information nonrepudi-*  
10 *ation and authenticity;*

11 “(B) *confidentiality, by preserving author-*  
12 *ized restrictions on access and disclosure, includ-*  
13 *ing means for protecting personal privacy and*  
14 *proprietary information; and*

15 “(C) *availability, by ensuring timely and*  
16 *reliable access to and use of information.*

17 “(6) *The term ‘information technology’ has the*  
18 *meaning given that term in section 11101 of title 40.*

19 “(7) *The term ‘management controls’ means safe-*  
20 *guards or countermeasures for an information system*  
21 *that focus on the management of risk and the man-*  
22 *agement of information system security.*

23 “(8)(A) *The term ‘national security system’*  
24 *means any information system (including any tele-*  
25 *communications system) used or operated by an agen-*

1 *cy or by a contractor of an agency, or other organiza-*  
2 *tion on behalf of an agency—*

3 *“(i) the function, operation, or use of*  
4 *which—*

5 *“(I) involves intelligence activities;*

6 *“(II) involves cryptologic activities re-*  
7 *lated to national security;*

8 *“(III) involves command and control*  
9 *of military forces;*

10 *“(IV) involves equipment that is an in-*  
11 *tegral part of a weapon or weapons system;*

12 *or*

13 *“(V) subject to subparagraph (B), is*  
14 *critical to the direct fulfillment of military*  
15 *or intelligence missions; or*

16 *“(ii) that is protected at all times by proce-*  
17 *dures established for information that have been*  
18 *specifically authorized under criteria established*  
19 *by an Executive order or an Act of Congress to*  
20 *be kept classified in the interest of national de-*  
21 *fense or foreign policy.*

22 *“(B) Subparagraph (A)(i)(V) does not include a*  
23 *system that is to be used for routine administrative*  
24 *and business applications (including payroll, finance,*  
25 *logistics, and personnel management applications).*

1           “(9) *The term ‘operational controls’ means the*  
2           *safeguards and countermeasures for an information*  
3           *system that are primarily implemented and executed*  
4           *by individuals, not systems.*

5           “(10) *The term ‘risk’ means the potential for an*  
6           *unwanted outcome resulting from an incident, as de-*  
7           *termined by the likelihood of the occurrence of the in-*  
8           *cident and the associated consequences, including po-*  
9           *tential for an adverse outcome assessed as a function*  
10          *of threats, vulnerabilities, and consequences associated*  
11          *with an incident*

12          “(11) *The term ‘risk-based security’ means secu-*  
13          *rity commensurate with the risk and magnitude of*  
14          *harm resulting from the loss, misuse, or unauthorized*  
15          *access to, or modification, of information, including*  
16          *assuring that systems and applications used by the*  
17          *agency operate effectively and provide appropriate*  
18          *confidentiality, integrity, and availability.*

19          “(12) *The term ‘security controls’ means the*  
20          *management, operational, and technical controls pre-*  
21          *scribed for an information system to protect the infor-*  
22          *mation security of the system.*

23          “(13) *The term ‘technical controls’ means the*  
24          *safeguards or countermeasures for an information*  
25          *system that are primarily implemented and executed*

1       *by the information system through mechanism con-*  
2       *tained in the hardware, software, or firmware compo-*  
3       *nents of the system.*

4       **“§ 3552. Authority and functions of the National Cen-**  
5                               **ter for Cybersecurity and Communications**

6       “(a) *IN GENERAL.*—*The Director of the National Cen-*  
7       *ter for Cybersecurity and Communications shall—*

8                       “(1) *develop, oversee the implementation of, and*  
9                       *enforce policies, principles, and guidelines on infor-*  
10                      *mation security, including through ensuring timely*  
11                      *agency adoption of and compliance with standards*  
12                      *developed under section 20 of the National Institute*  
13                      *of Standards and Technology Act (15 U.S.C. 278g–3)*  
14                      *and subtitle E of title II of the Homeland Security*  
15                      *Act of 2002;*

16                     “(2) *provide to agencies security controls that*  
17                     *agencies shall be required to be implemented to miti-*  
18                     *gate and remediate vulnerabilities, attacks, and ex-*  
19                     *ploitations discovered as a result of activities required*  
20                     *under this subchapter or subtitle E of title II of the*  
21                     *Homeland Security Act of 2002;*

22                     “(3) *to the extent practicable—*

23                               “(A) *prioritize the policies, principles,*  
24                               *standards, and guidelines promulgated under*  
25                               *section 20 of the National Institute of Standards*

1           *and Technology Act (15 U.S.C. 278g–3), para-*  
2           *graph (1), and subtitle E of title II of the Home-*  
3           *land Security Act of 2002, based upon the risk*  
4           *of an incident; and*

5           *“(B) develop guidance that requires agen-*  
6           *cies to monitor, including automated and contin-*  
7           *uous monitoring of, the effective implementation*  
8           *of policies, principles, standards, and guidelines*  
9           *developed under section 20 of the National Insti-*  
10          *tute of Standards and Technology Act (15 U.S.C.*  
11          *278g–3), paragraph (1), and subtitle E of title II*  
12          *of the Homeland Security Act of 2002;*

13          *“(C) ensure the effective operation of tech-*  
14          *nical capabilities within the National Center for*  
15          *Cybersecurity and Communications to enable*  
16          *automated and continuous monitoring of any in-*  
17          *formation collected as a result of the guidance*  
18          *developed under subparagraph (B) and use the*  
19          *information to enhance the risk-based security of*  
20          *the Federal information infrastructure; and*

21          *“(D) ensure the effective operation of a se-*  
22          *ecure system that satisfies information reporting*  
23          *requirements under sections 3553(c) and 3556(c);*

24          *“(4) require agencies, consistent with the stand-*  
25          *ards developed under section 20 of the National Insti-*

1 *tute of Standards and Technology Act (15 U.S.C.*  
2 *278g-3) or paragraph (1) and the requirements of*  
3 *this subchapter, to identify and provide information*  
4 *security protections commensurate with the risk re-*  
5 *sulting from the disruption or unauthorized access,*  
6 *use, disclosure, modification, or destruction of—*

7 *“(A) information collected or maintained by*  
8 *or on behalf of an agency; or*

9 *“(B) information systems used or operated*  
10 *by an agency or by a contractor of an agency or*  
11 *other organization on behalf of an agency;*

12 *“(5) oversee agency compliance with the require-*  
13 *ments of this subchapter, including coordinating with*  
14 *the Office of Management and Budget to use any au-*  
15 *thorized action under section 11303 of title 40 to en-*  
16 *force accountability for compliance with such require-*  
17 *ments;*

18 *“(6) review, at least annually, and approve or*  
19 *disapprove, agency information security programs re-*  
20 *quired under section 3553(b); and*

21 *“(7) coordinate information security policies and*  
22 *procedures with the Administrator for Electronic Gov-*  
23 *ernment and the Administrator for the Office of In-*  
24 *formation and Regulatory Affairs with related infor-*

1        *mation resources management policies and proce-*  
2        *dures.*

3        “(b) *NATIONAL SECURITY SYSTEMS.—The authorities*  
4        *of the Director of the National Center for Cybersecurity and*  
5        *Communications under this section shall not apply to na-*  
6        *tional security systems.*

7        **“§ 3553. Agency responsibilities**

8        “(a) *IN GENERAL.—The head of each agency shall—*  
9        *“(1) be responsible for—*

10                *“(A) providing information security protec-*  
11                *tions commensurate with the risk and magnitude*  
12                *of the harm resulting from unauthorized access,*  
13                *use, disclosure, disruption, modification, or de-*  
14                *struction of—*

15                        *“(i) information collected or main-*  
16                        *tained by or on behalf of the agency; and*

17                        *“(ii) agency information infrastruc-*  
18                        *ture;*

19                *“(B) complying with the requirements of*  
20                *this subchapter and related policies, procedures,*  
21                *standards, and guidelines, including—*

22                        *“(i) information security requirements,*  
23                        *including security controls, developed by the*  
24                        *Director of the National Center for Cyberse-*  
25                        *curity and Communications under section*

1                   3552, subtitle *E* of title II of the Homeland  
2                   Security Act of 2002, or any other provision  
3                   of law;

4                   “(ii) information security policies,  
5                   principles, standards, and guidelines pro-  
6                   mulgated under section 20 of the National  
7                   Institute of Standards and Technology Act  
8                   (15 U.S.C. 278g–3) and section 3552(a)(1);

9                   “(iii) information security standards  
10                  and guidelines for national security systems  
11                  issued in accordance with law and as di-  
12                  rected by the President; and

13                  “(iv) ensuring the standards imple-  
14                  mented for information systems and na-  
15                  tional security systems of the agency are  
16                  complementary and uniform, to the extent  
17                  practicable;

18                  “(C) ensuring that information security  
19                  management processes are integrated with agen-  
20                  cy strategic and operational planning and budg-  
21                  et processes, including policies, procedures, and  
22                  practices described in subsection (c)(1)(C);

23                  “(D) as appropriate, maintaining secure fa-  
24                  cilities that have the capability of accessing,

1           *sending, receiving, and storing classified infor-*  
2           *mation;*

3           “(E) *maintaining a sufficient number of*  
4           *personnel with security clearances, at the appro-*  
5           *propriate levels, to access, send, receive and analyze*  
6           *classified information to carry out the respon-*  
7           *sibilities of this subchapter; and*

8           “(F) *ensuring that information security*  
9           *performance indicators and measures are in-*  
10          *cluded in the annual performance evaluations of*  
11          *all managers, senior managers, senior executive*  
12          *service personnel, and political appointees;*

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

18                 “(A) *assessing the risk and magnitude of*  
19                 *the harm that could result from the disruption or*  
20                 *unauthorized access, use, disclosure, modifica-*  
21                 *tion, or destruction of such information or infor-*  
22                 *mation systems;*

23                 “(B) *determining the levels of information*  
24                 *security appropriate to protect such information*  
25                 *and information systems in accordance with*

1 *policies, principles, standards, and guidelines*  
2 *promulgated under section 20 of the National In-*  
3 *stitute of Standards and Technology Act (15*  
4 *U.S.C. 278g–3), section 3552(a)(1), and subtitle*  
5 *E of title II of the Homeland Security Act of*  
6 *2002, for information security categorizations*  
7 *and related requirements;*

8 *“(C) implementing policies and procedures*  
9 *to cost effectively reduce risks to an acceptable*  
10 *level;*

11 *“(D) periodically testing and evaluating in-*  
12 *formation security controls and techniques to en-*  
13 *sure that such controls and techniques are oper-*  
14 *ating effectively; and*

15 *“(E) withholding all bonus and cash*  
16 *awards to senior agency officials accountable for*  
17 *the operation of such agency information infra-*  
18 *structure that are recognized by the Chief Infor-*  
19 *mation Security Officer as impairing the risk-*  
20 *based security information, information system,*  
21 *or agency information infrastructure;*

22 *“(3) delegate to a senior agency officer des-*  
23 *ignated as the Chief Information Security Officer the*  
24 *authority and budget necessary to ensure and enforce*  
25 *compliance with the requirements imposed on the*

1        *agency under this subchapter, subtitle E of title II of*  
2        *the Homeland Security Act of 2002, or any other pro-*  
3        *vision of law, including—*

4                *“(A) overseeing the establishment, mainte-*  
5                *nance, and management of a security operations*  
6                *center that has technical capabilities that can,*  
7                *through automated and continuous monitoring—*

8                        *“(i) detect, report, respond to, contain,*  
9                        *remediate, and mitigate incidents that im-*  
10                        *pair risk-based security of the information,*  
11                        *information systems, and agency informa-*  
12                        *tion infrastructure, in accordance with pol-*  
13                        *icy provided by the Director of the National*  
14                        *Center for Cybersecurity and Communica-*  
15                        *tions;*

16                        *“(ii) monitor and, on a risk-based*  
17                        *basis, mitigate and remediate the*  
18                        *vulnerabilities of every information system*  
19                        *within the agency information infrastruc-*  
20                        *ture;*

21                        *“(iii) continually evaluate risks posed*  
22                        *to information collected or maintained by*  
23                        *or on behalf of the agency and information*  
24                        *systems and hold senior agency officials ac-*  
25                        *countable for ensuring the risk-based secu-*

1            *rity of such information and information*  
2            *systems;*

3            *“(iv) collaborate with the Director of*  
4            *the National Center for Cybersecurity and*  
5            *Communications and appropriate public*  
6            *and private sector security operations cen-*  
7            *ters to address incidents that impact the se-*  
8            *curity of information and information sys-*  
9            *tems that extend beyond the control of the*  
10           *agency; and*

11           *“(v) report any incident described*  
12           *under clauses (i) and (ii), as directed by the*  
13           *policy of the Director of the National Center*  
14           *for Cybersecurity and Communications and*  
15           *the Inspector General of the agency;*

16           *“(B) collaborating with the Administrator*  
17           *for E–Government and the Chief Information Of-*  
18           *ficer to establish, maintain, and update an en-*  
19           *terprise network, system, storage, and security*  
20           *architecture, that can be accessed by the National*  
21           *Cybersecurity Communications Center and in-*  
22           *cludes—*

23           *“(i) information on how security con-*  
24           *trols are implemented throughout the agen-*  
25           *cy information infrastructure; and*

1           “(ii) information on how the controls  
2           described under subparagraph (A) maintain  
3           the appropriate level of confidentiality, in-  
4           tegrity, and availability of information and  
5           information systems based on—

6                   “(I) the policy of the Director of  
7                   the National Center for Cybersecurity  
8                   and Communications; and

9                   “(II) the standards or guidance  
10                  developed by the National Institute of  
11                  Standards and Technology;

12                  “(C) developing, maintaining, and over-  
13                  seeing an agency-wide information security pro-  
14                  gram as required by subsection (b);

15                  “(D) developing, maintaining, and over-  
16                  seeing information security policies, procedures,  
17                  and control techniques to address all applicable  
18                  requirements, including those issued under sec-  
19                  tion 3552;

20                  “(E) training, consistent with the require-  
21                  ments of section 406 of the Protecting Cyberspace  
22                  as a National Asset Act of 2010, and overseeing  
23                  personnel with significant responsibilities for in-  
24                  formation security with respect to such respon-  
25                  sibilities; and

1           “(F) assisting senior agency officers con-  
2           cerning their responsibilities under paragraph  
3           (2);

4           “(4) ensure that the Chief Information Security  
5           Officer has a sufficient number of cleared and trained  
6           personnel with technical skills identified by the Direc-  
7           tor of the National Center for Cybersecurity and Com-  
8           munications as critical to maintaining the risk-based  
9           security of agency information infrastructure as re-  
10          quired by the subchapter and other applicable laws;

11          “(5) ensure that the agency Chief Information  
12          Security Officer, in coordination with appropriate  
13          senior agency officials, reports not less than annually  
14          to the head of the agency on the effectiveness of the  
15          agency information security program, including  
16          progress of remedial actions;

17          “(6) ensure that the Chief Information Security  
18          Officer—

19                 “(A) possesses necessary qualifications, in-  
20                 cluding education, professional certifications,  
21                 training, experience, and the security clearance  
22                 required to administer the functions described  
23                 under this subchapter; and

24                 “(B) has information security duties as the  
25                 primary duty of that officer; and

1           “(7) ensure that components of that agency es-  
2           tablish and maintain an automated reporting mecha-  
3           nism that allows the Chief Information Security Offi-  
4           cer with responsibility for the entire agency, and all  
5           components thereof, to implement, monitor, and hold  
6           senior agency officers accountable for the implementa-  
7           tion of appropriate security policies, procedures, and  
8           controls of agency components.

9           “(b) *AGENCY-WIDE INFORMATION SECURITY PRO-*  
10 *GRAM.—Each agency shall develop, document, and imple-*  
11 *ment an agency-wide information security program, ap-*  
12 *proved by the Director of the National Center for Cybersecu-*  
13 *rity and Communications under section 3552(a)(6) and*  
14 *consistent with components across and within agencies, to*  
15 *provide information security for the information and infor-*  
16 *mation systems that support the operations and assets of*  
17 *the agency, including those provided or managed by another*  
18 *agency, contractor, or other source, that includes—*

19           “(1) frequent assessments, at least twice each  
20           month—

21           “(A) of the risk and magnitude of the harm  
22           that could result from the disruption or unau-  
23           thorized access, use, disclosure, modification, or  
24           destruction of information and information sys-

1           *tems that support the operations and assets of*  
2           *the agency; and*

3                   *“(B) that assess whether information or in-*  
4                   *formation systems should be removed or migrated*  
5                   *to more secure networks or standards and make*  
6                   *recommendations to the head of the agency and*  
7                   *the Director of the National Center for Cyberse-*  
8                   *curity and Communications based on that as-*  
9                   *essment;*

10                   *“(2) consistent with guidance developed under*  
11                   *section 3554, vulnerability assessments and penetra-*  
12                   *tion tests commensurate with the risk posed to an*  
13                   *agency information infrastructure;*

14                   *“(3) ensure that information security*  
15                   *vulnerabilities are remediated or mitigated based on*  
16                   *the risk posed to the agency;*

17                   *“(4) policies and procedures that—*

18                           *“(A) are informed and revised by the assess-*  
19                           *ments required under paragraphs (1) and (2);*

20                           *“(B) cost effectively reduce information se-*  
21                           *curity risks to an acceptable level;*

22                           *“(C) ensure that information security is ad-*  
23                           *dressed throughout the life cycle of each agency*  
24                           *information system; and*

25                           *“(D) ensure compliance with—*

1           “(i) the requirements of this sub-  
2           chapter;

3           “(ii) policies and procedures prescribed  
4           by the Director of the National Center for  
5           Cybersecurity and Communications;

6           “(iii) minimally acceptable system  
7           configuration requirements, as determined  
8           by the Director of the National Center for  
9           Cybersecurity and Communications; and

10          “(iv) any other applicable require-  
11          ments, including standards and guidelines  
12          for national security systems issued in ac-  
13          cordance with law and as directed by the  
14          President;

15          “(5) subordinate plans for providing risk-based  
16          information security for networks, facilities, and sys-  
17          tems or groups of information systems, as appro-  
18          priate;

19          “(6) role-based security awareness training, con-  
20          sistent with the requirements of section 406 of the  
21          Protecting Cyberspace as a National Asset Act of  
22          2010, to inform personnel with access to the agency  
23          network, including contractors and other users of in-  
24          formation systems that support the operations and as-  
25          sets of the agency, of—

1           “(A) information security risks associated  
2           with agency activities; and

3           “(B) agency responsibilities in complying  
4           with agency policies and procedures designed to  
5           reduce those risks;

6           “(7) periodic testing and evaluation of the effec-  
7           tiveness of information security policies, procedures,  
8           and practices, to be performed with a rigor and fre-  
9           quency depending on risk, which shall include—

10           “(A) testing and evaluation not less than  
11           twice each year of security controls of informa-  
12           tion collected or maintained by or on behalf of  
13           the agency and every information system identi-  
14           fied in the inventory required under section  
15           3505(c);

16           “(B) the effectiveness of ongoing monitoring,  
17           including automated and continuous monitoring,  
18           vulnerability scanning, and intrusion detection  
19           and prevention of incidents posed to the risk-  
20           based security of information and information  
21           systems as required under subsection (a)(3); and

22           “(C) testing relied on in—

23           “(i) an operational evaluation under  
24           section 3554;

1                   “(ii) an independent assessment under  
2                   section 3556; or

3                   “(iii) another evaluation, to the extent  
4                   specified by the Director of the National  
5                   Center for Cybersecurity and Communica-  
6                   tions;

7                   “(8) a process for planning, implementing, eval-  
8                   uating, and documenting remedial action to address  
9                   any deficiencies in the information security policies,  
10                  procedures, and practices of the agency;

11                  “(9) procedures for detecting, reporting, and re-  
12                  sponding to incidents, consistent with requirements  
13                  issued under section 3552, that include—

14                         “(A) to the extent practicable, automated  
15                         and continuous monitoring of the use of infor-  
16                         mation and information systems;

17                         “(B) requirements for mitigating risks and  
18                         remediating vulnerabilities associated with such  
19                         incidents systemically within the agency infor-  
20                         mation infrastructure before substantial damage  
21                         is done; and

22                         “(C) notifying and coordinating with the  
23                         Director of the National Center for Cybersecurity  
24                         and Communications, as required by this sub-  
25                         chapter, subtitle E of title II of the Homeland

1           *Security Act of 2002, and any other provision of*  
2           *law; and*

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

6           “(c) *AGENCY REPORTING.*—

7           “(1) *IN GENERAL.*—*Each agency shall—*

8                   “(A) *ensure that information relating to the*  
9                   *adequacy and effectiveness of information secu-*  
10                   *rity policies, procedures, and practices, is avail-*  
11                   *able to the entities identified under paragraph*  
12                   *(2) through the system developed under section*  
13                   *3552(a)(3), including information relating to—*

14                           “(i) *compliance with the requirements*  
15                           *of this subchapter;*

16                           “(ii) *the effectiveness of the informa-*  
17                           *tion security policies, procedures, and prac-*  
18                           *tices of the agency based on a determination*  
19                           *of the aggregate effect of identified defi-*  
20                           *ciencies and vulnerabilities;*

21                           “(iii) *an identification and analysis of*  
22                           *any significant deficiencies identified in*  
23                           *such policies, procedures, and practices;*

24                           “(iv) *an identification of any vulner-*  
25                           *ability that could impair the risk-based se-*

1           *curity of the agency information infrastruc-*  
2           *ture; and*

3           *“(v) results of any operational evalua-*  
4           *tion conducted under section 3554 and*  
5           *plans of action to address the deficiencies*  
6           *and vulnerabilities identified as a result of*  
7           *such operational evaluation;*

8           *“(B) follow the policy, guidance, and stand-*  
9           *ards of the Director of the National Center for*  
10          *Cybersecurity and Communications, in consulta-*  
11          *tion with the Federal Information Security*  
12          *Taskforce, to continually update, and ensure the*  
13          *electronic availability of both a classified and*  
14          *unclassified version of the information required*  
15          *under subparagraph (A);*

16          *“(C) ensure the information under subpara-*  
17          *graph (A) addresses the adequacy and effective-*  
18          *ness of information security policies, procedures,*  
19          *and practices in plans and reports relating to—*

20                  *“(i) annual agency budgets;*

21                  *“(ii) information resources manage-*  
22                  *ment of this subchapter;*

23                  *“(iii) information technology manage-*  
24                  *ment and procurement under this chapter*  
25                  *or any other applicable provision of law;*

1                   “(iv) subtitle E of title II of the Home-  
2                   land Security Act of 2002;

3                   “(v) program performance under sec-  
4                   tions 1105 and 1115 through 1119 of title  
5                   31, and sections 2801 and 2805 of title 39;

6                   “(vi) financial management under  
7                   chapter 9 of title 31, and the Chief Finan-  
8                   cial Officers Act of 1990 (31 U.S.C. 501  
9                   note; Public Law 101–576) (and the amend-  
10                  ments made by that Act);

11                  “(vii) financial management systems  
12                  under the Federal Financial Management  
13                  Improvement Act (31 U.S.C. 3512 note);

14                  “(viii) internal accounting and admin-  
15                  istrative controls under section 3512 of title  
16                  31; and

17                  “(ix) performance ratings, salaries,  
18                  and bonuses provided to the senior man-  
19                  agers and supporting personnel taking into  
20                  account program performance as it relates  
21                  to complying with this subchapter; and

22                  “(D) report any significant deficiency in a  
23                  policy, procedure, or practice identified under  
24                  subparagraph (A) or (B)—

1           “(i) as a material weakness in report-  
2           ing under section 3512 of title 31; and

3           “(ii) if relating to financial manage-  
4           ment systems, as an instance of a lack of  
5           substantial compliance under the Federal  
6           Financial Management Improvement Act  
7           (31 U.S.C. 3512 note).

8           “(2) ADEQUACY AND EFFECTIVENESS INFORMA-  
9           TION.—Information required under paragraph (1)(A)  
10          shall, to the extent possible and in accordance with  
11          applicable law, policy, guidance, and standards, be  
12          available on an automated and continuous basis to—

13               “(A) the Director of the National Center for  
14               Cybersecurity and Communications;

15               “(B) the Office of Management and Budget;

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

18               “(D) the Committee on Government Over-  
19               sight and Reform of the House of Representa-  
20               tives;

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

23               “(F) other appropriate authorization and  
24               appropriations committees of Congress;

1                   “(G) *the Inspector General of the Federal*  
2                   *agency; and*

3                   “(H) *the Comptroller General.*

4                   “(d) *INCLUSIONS IN PERFORMANCE PLANS.—*

5                   “(1) *IN GENERAL.—In addition to the require-*  
6                   *ments of subsection (c), each agency, in consultation*  
7                   *with the Director of the National Center for Cyberse-*  
8                   *curity and Communications, shall include as part of*  
9                   *the performance plan required under section 1115 of*  
10                  *title 31 a description of the time periods the resources,*  
11                  *including budget, staffing, and training, that are nec-*  
12                  *essary to implement the program required under sub-*  
13                  *section (b).*

14                  “(2) *RISK ASSESSMENTS.—The description*  
15                  *under paragraph (1) shall be based on the risk and*  
16                  *vulnerability assessments required under subsection*  
17                  *(b) and evaluations required under section 3554.*

18                  “(e) *NOTICE AND COMMENT.—Each agency shall pro-*  
19                  *vide the public with timely notice and opportunities for*  
20                  *comment on proposed information security policies and*  
21                  *procedures to the extent that such policies and procedures*  
22                  *affect communication with the public.*

23                  “(f) *MORE STRINGENT STANDARDS.—The head of an*  
24                  *agency may employ standards for the cost effective informa-*  
25                  *tion security for information systems within or under the*

1 *supervision of that agency that are more stringent than the*  
2 *standards the Director of the National Center for Cybersecu-*  
3 *rity and Communications prescribes under this subchapter,*  
4 *subtitle E of title II of the Homeland Security Act of 2002,*  
5 *or any other provision of law, if the more stringent stand-*  
6 *ards—*

7           “(1) *contain at least the applicable standards*  
8           *made compulsory and binding by the Director of the*  
9           *National Center for Cybersecurity and Communica-*  
10          *tions; and*

11           “(2) *are otherwise consistent with policies and*  
12          *guidelines issued under section 3552.*

13 **“§ 3554. Annual operational evaluation**

14          “(a) *GUIDANCE.—*

15           “(1) *IN GENERAL.—Not later than 1 year after*  
16          *the date of enactment of the Protecting Cyberspace as*  
17          *a National Asset Act of 2010 and each year there-*  
18          *after, the Director of the National Center for Cyberse-*  
19          *curity and Communications shall oversee, coordinate,*  
20          *and develop guidance for the effective implementation*  
21          *of operational evaluations of the Federal information*  
22          *infrastructure and agency information security pro-*  
23          *grams and practices to determine the effectiveness of*  
24          *such program and practices.*

1           “(2) *COLLABORATION IN DEVELOPMENT.*—*In de-*  
2           *veloping guidance for the operational evaluations de-*  
3           *scribed under this section, the Director of the Na-*  
4           *tional Center for Cybersecurity and Communications*  
5           *shall collaborate with the Federal Information Secu-*  
6           *rity Taskforce and the Council of Inspectors General*  
7           *on Integrity and Efficiency, and other agencies as*  
8           *necessary, to develop and update risk-based perform-*  
9           *ance indicators and measures that assess the ade-*  
10           *quacy and effectiveness of information security of an*  
11           *agency and the Federal information infrastructure.*

12           “(3) *CONTENTS OF OPERATIONAL EVALUATION.*—  
13           *Each operational evaluation under this section—*

14                   “(A) *shall be prioritized based on risk; and*

15                   “(B) *shall—*

16                           “(i) *test the effectiveness of agency in-*  
17                           *formation security policies, procedures, and*  
18                           *practices of the information systems of the*  
19                           *agency, or a representative subset of those*  
20                           *information systems;*

21                           “(ii) *assess (based on the results of the*  
22                           *testing) compliance with—*

23                                   “(I) *the requirements of this sub-*  
24                                   *chapter; and*

1           “(II) related information security  
2 policies, procedures, standards, and  
3 guidelines;

4           “(iii) evaluate whether agencies—

5                 “(I) effectively monitor, detect,  
6 analyze, protect, report, and respond to  
7 vulnerabilities and incidents;

8                 “(II) report to and collaborate  
9 with the appropriate public and pri-  
10 vate security operation centers, the Di-  
11 rector of the National Center for Cyber-  
12 security and Communications, and law  
13 enforcement agencies; and

14                 “(III) remediate or mitigate the  
15 risk posed by attacks and exploitations  
16 in a timely fashion in order to prevent  
17 future vulnerabilities and incidents;  
18 and

19                 “(iv) identify deficiencies of agency in-  
20 formation security policies, procedures, and  
21 controls on the agency information infra-  
22 structure.

23           “(b) CONDUCT AN OPERATIONAL EVALUATION.—

24                 “(1) IN GENERAL.—Except as provided under  
25 paragraph (2), and in consultation with the Chief In-

1 *formation Officer and senior officials responsible for*  
2 *the affected systems, the Chief Information Security*  
3 *Officer of each agency shall not less than annually—*

4 *“(A) conduct an operational evaluation of*  
5 *the agency information infrastructure for*  
6 *vulnerabilities, attacks, and exploitations of the*  
7 *agency information infrastructure;*

8 *“(B) evaluate the ability of the agency to*  
9 *monitor, detect, correlate, analyze, report, and*  
10 *respond to incidents; and*

11 *“(C) report to the head of the agency, the*  
12 *Director of the National Center for Cybersecurity*  
13 *and Communications, the Chief Information Of-*  
14 *ficer, and the Inspector General for the agency*  
15 *the findings of the operational evaluation.*

16 *“(2) SATISFACTION OF REQUIREMENTS BY*  
17 *OTHER EVALUATION.—Unless otherwise specified by*  
18 *the Director of the National Center for Cybersecurity*  
19 *and Communications, if the Director of the National*  
20 *Center for Cybersecurity and Communications con-*  
21 *ducts an operational evaluation of the agency infor-*  
22 *mation infrastructure under section 245(b)(2)(A) of*  
23 *the Homeland Security Act of 2002, the Chief Infor-*  
24 *mation Security Officer may deem the requirements*  
25 *of paragraph (1) satisfied for the year in which the*

1        *operational evaluation described under this para-*  
2        *graph is conducted.*

3        “(c) *CORRECTIVE MEASURES MITIGATION AND REME-*  
4        *DIATION PLANS.—*

5                “(1) *IN GENERAL.—In consultation with the Di-*  
6        *rector of the National Center for Cybersecurity and*  
7        *Communications and the Chief Information Officer,*  
8        *Chief Information Security Officers shall remediate or*  
9        *mitigate vulnerabilities in accordance with this sub-*  
10        *section.*

11                “(2) *RISK-BASED PLAN.—After an operational*  
12        *evaluation is conducted under this section or under*  
13        *section 245(b) of the Homeland Security Act of 2002,*  
14        *the agency shall submit to the Director of the Na-*  
15        *tional Center for Cybersecurity and Communications*  
16        *in a timely fashion a risk-based plan for addressing*  
17        *recommendations and mitigating and remediating*  
18        *vulnerabilities identified as a result of such oper-*  
19        *ational evaluation, including a timeline and budget*  
20        *for implementing such plan.*

21                “(3) *APPROVAL OR DISAPPROVAL.—Not later*  
22        *than 15 days after receiving a plan submitted under*  
23        *paragraph (2), the Director of the National Center for*  
24        *Cybersecurity and Communications shall—*

1           “(A) approve or disprove the agency plan;  
2           and

3           “(B) comment on the adequacy and effec-  
4           tiveness of the plan.

5           “(4) ISOLATION FROM INFRASTRUCTURE.—

6           “(A) IN GENERAL.—The Director of the Na-  
7           tional Center for Cybersecurity and Communica-  
8           tions may, consistent with the contingency or  
9           continuity of operation plans applicable to such  
10          agency information infrastructure, order the iso-  
11          lation of any component of the Federal informa-  
12          tion infrastructure from any other Federal infor-  
13          mation infrastructure, if—

14                 “(i) an agency does not implement  
15                 measures in a risk-based plan approved  
16                 under this subsection; and

17                 “(ii) the failure to comply presents a  
18                 significant danger to the Federal informa-  
19                 tion infrastructure.

20          “(B) DURATION.—An isolation under sub-  
21          paragraph (A) shall remain in effect until—

22                 “(i) the Director of the National Center  
23                 for Cybersecurity and Communications de-  
24                 termines that corrective measures have been  
25                 implemented; or

1                   “(ii) an updated risk-based plan is ap-  
2                   proved by the Director of the National Cen-  
3                   ter for Cybersecurity and Communications  
4                   and implemented by the agency.

5           “(d) OPERATIONAL GUIDANCE.—The Director of the  
6 National Center for Cybersecurity and Communications  
7 shall—

8                   “(1) not later than 180 days after the date of en-  
9                   actment of the Protecting Cyberspace as a National  
10                  Asset Act of 2010, develop operational guidance for  
11                  operational evaluations as required under this section  
12                  that are risk-based and cost effective; and

13                  “(2) periodically evaluate and ensure informa-  
14                  tion is available on an automated and continuous  
15                  basis through the system required under section  
16                  3552(a)(3)(D) to Congress on—

17                         “(A) the adequacy and effectiveness of the  
18                         operational evaluations conducted under this sec-  
19                         tion or section 245(b) of the Homeland Security  
20                         Act of 2002; and

21                         “(B) possible executive and legislative ac-  
22                         tions for cost-effectively managing the risks to  
23                         the Federal information infrastructure.

1 **“§ 3555. Federal Information Security Taskforce**

2       “(a) *ESTABLISHMENT.*—*There is established in the ex-*  
3 *ecutive branch a Federal Information Security Taskforce.*

4       “(b) *MEMBERSHIP.*—*The members of the Federal In-*  
5 *formation Security Taskforce shall be full-time senior Gov-*  
6 *ernment employees and shall be as follows:*

7               “(1) *The Director of the National Center for Cy-*  
8 *bersecurity and Communications.*

9               “(2) *The Administrator of the Office of Elec-*  
10 *tronic Government of the Office of Management and*  
11 *Budget.*

12               “(3) *The Chief Information Security Officer of*  
13 *each agency described under section 901(b) of title 31.*

14               “(4) *The Chief Information Security Officer of*  
15 *the Department of the Army, the Department of the*  
16 *Navy, and the Department of the Air Force.*

17               “(5) *A representative from the Office of Cyber-*  
18 *space Policy.*

19               “(6) *A representative from the Office of the Di-*  
20 *rector of National Intelligence.*

21               “(7) *A representative from the United States*  
22 *Cyber Command.*

23               “(8) *A representative from the National Security*  
24 *Agency.*

25               “(9) *A representative from the United States*  
26 *Computer Emergency Readiness Team.*

1           “(10) *A representative from the Intelligence*  
2           *Community Incident Response Center.*

3           “(11) *A representative from the Committee on*  
4           *National Security Systems.*

5           “(12) *A representative from the National Insti-*  
6           *tute for Standards and Technology.*

7           “(13) *A representative from the Council of In-*  
8           *spectors General on Integrity and Efficiency.*

9           “(14) *A representative from State and local gov-*  
10          *ernment.*

11          “(15) *Any other officer or employee of the United*  
12          *States designated by the chairperson.*

13          “(c) *CHAIRPERSON AND VICE-CHAIRPERSON.—*

14                 “(1) *CHAIRPERSON.—The Director of the Na-*  
15                 *tional Center for Cybersecurity and Communications*  
16                 *shall act as chairperson of the Federal Information*  
17                 *Security Taskforce.*

18                 “(2) *VICE-CHAIRPERSON.—The vice chairperson*  
19                 *of the Federal Information Security Taskforce shall—*

20                         “(A) *be selected by the Federal Information*  
21                         *Security Taskforce from among its members;*

22                         “(B) *serve a 1-year term and may serve*  
23                         *multiple terms; and*

24                         “(C) *serve as a liaison to the Chief Informa-*  
25                         *tion Officer, Council of the Inspectors General on*

1           *Integrity and Efficiency, Committee on National*  
2           *Security Systems, and other councils or commit-*  
3           *tees as appointed by the chairperson.*

4           “(d) *FUNCTIONS.—The Federal Information Security*  
5 *Taskforce shall—*

6           “(1) *be the principal interagency forum for col-*  
7 *laboration regarding best practices and recommenda-*  
8 *tions for agency information security and the security*  
9 *of the Federal information infrastructure;*

10          “(2) *assist in the development of and annually*  
11 *evaluate guidance to fulfill the requirements under*  
12 *sections 3554 and 3556;*

13          “(3) *share experiences and innovative ap-*  
14 *proaches relating to threats against the Federal infor-*  
15 *mation infrastructure, information sharing and in-*  
16 *formation security best practices, penetration testing*  
17 *regimes, and incident response, mitigation, and reme-*  
18 *diation;*

19          “(4) *promote the development and use of stand-*  
20 *ard performance indicators and measures for agency*  
21 *information security that—*

22                  “(A) *are outcome-based;*

23                  “(B) *focus on risk management;*

24                  “(C) *align with the business and program*  
25 *goals of the agency;*

1           “(D) measure improvements in the agency  
2 security posture over time; and

3           “(E) reduce burdensome and inefficient per-  
4 formance indicators and measures;

5           “(5) recommend to the Office of Personnel Man-  
6 agement the necessary qualifications to be established  
7 for Chief Information Security Officers to be capable  
8 of administering the functions described under this  
9 subchapter including education, training, and experi-  
10 ence;

11           “(6) enhance information system processes by es-  
12 tablishing a prioritized baseline of information secu-  
13 rity measures and controls that can be continuously  
14 monitored through automated mechanisms; and

15           “(7) evaluate the effectiveness and efficiency of  
16 any reporting and compliance requirements that are  
17 required by law related to the information security of  
18 Federal information infrastructure; and

19           “(8) submit proposed enhancements developed  
20 under paragraphs (1) through (7) to the Director of  
21 the National Center for Cybersecurity and Commu-  
22 nications.

23           “(e) TERMINATION.—

24           “(1) IN GENERAL.—Except as provided under  
25 paragraph (2), the Federal Information Security

1 *Taskforce shall terminate 4 years after the date of en-*  
 2 *actment of the Protecting Cyberspace as a National*  
 3 *Asset Act of 2010.*

4 “(2) *EXTENSION.*—*The President may—*

5 “(A) *extend the Federal Information Secu-*  
 6 *rity Taskforce by executive order; and*

7 “(B) *make more than 1 extension under this*  
 8 *paragraph for any period as the President may*  
 9 *determine.*

10 **“§ 3556. *Independent Assessments***

11 “(a) *IN GENERAL.*—

12 “(1) *INSPECTORS GENERAL ASSESSMENTS.*—*Not*  
 13 *less than every 2 years, each agency with an Inspec-*  
 14 *tor General appointed under the Inspector General*  
 15 *Act of 1978 (5 U.S.C. App.) or any other law shall*  
 16 *assess the adequacy and effectiveness of the informa-*  
 17 *tion security program developed under section*  
 18 *3553(b) and (c), and evaluations conducted under sec-*  
 19 *tion 3554.*

20 “(2) *INDEPENDENT ASSESSMENTS.*—*For each*  
 21 *agency to which paragraph (1) does not apply, the*  
 22 *head of the agency shall engage an independent exter-*  
 23 *nal auditor to perform the assessment.*

24 “(b) *STANDARDS.*—*The assessments required under*  
 25 *subsection (a) shall be performed in accordance with stand-*

1 ards developed by the Government Accountability Office, in  
2 collaboration with the Council of Inspectors General on In-  
3 tegrity and Efficiency and with assistance from the Federal  
4 Information Security Taskforce.

5 “(c) *EXISTING ASSESSMENTS.*—The assessments re-  
6 quired under this section may be based in whole or in part  
7 on an audit, evaluation, or report relating to programs or  
8 practices of the applicable agency.

9 “(d) *REPORTING OF INFORMATION.*—

10 “(1) *INSPECTORS GENERAL REPORTING.*—Each  
11 Inspector General shall ensure information obtained  
12 as a result of the assessment required under this sec-  
13 tion, or any other relevant information, is—

14 “(A) provided to the head of the agency, the  
15 agency Chief Information Security Officer, and  
16 the agency Chief Information Officer; and

17 “(B) available through the system required  
18 under section 3552(a)(3)(D) to Congress and the  
19 Director of the National Center for Cybersecurity  
20 and Communications.

21 “(2) *HEADS OF AGENCIES REPORTING.*—If an  
22 assessment described under subsection (a)(2) is per-  
23 formed, the head of the agency shall comply with the  
24 requirements of paragraph (1)(A) and (B).

1 **“§ 3557. Protection of Information**

2       *“In complying with this subchapter, agencies, eval-*  
3 *uators, and Inspectors General shall take appropriate ac-*  
4 *tions to ensure the protection of information which, if dis-*  
5 *closed, may adversely affect information security. Protec-*  
6 *tions under this chapter shall be commensurate with the*  
7 *risk and comply with all applicable laws and regulations.*

8 **“§ 3558. Department of Defense and Central Intel-**  
9 **ligence Agency systems**

10       *“(a) IN GENERAL.—The authorities of the Director of*  
11 *the National Center for Cybersecurity and Communications*  
12 *under this subchapter shall be delegated to—*

13               *“(1) the Secretary of Defense in the case of sys-*  
14 *tems described under subsection (b); and*

15               *“(2) the Director of the Central Intelligence*  
16 *Agency in the case of systems described under sub-*  
17 *section (c).*

18       *“(b) DEPARTMENT OF DEFENSE SYSTEMS.—The sys-*  
19 *tems described under this subsection are systems that are*  
20 *operated by the Department of Defense, a contractor of the*  
21 *Department of Defense, or another entity on behalf of the*  
22 *Department of Defense that processes any information the*  
23 *unauthorized access, use, disclosure, disruption, modifica-*  
24 *tion, or destruction of which would have a debilitating im-*  
25  *pact on the mission of the Department of Defense.*

1           “(c) *CENTRAL INTELLIGENCE AGENCY SYSTEMS.*—*The*  
 2 *systems described under this subsection are systems that are*  
 3 *operated by the Central Intelligence Agency, a contractor*  
 4 *of the Central Intelligence Agency, or another entity on be-*  
 5 *half of the Central Intelligence Agency that processes any*  
 6 *information the unauthorized access, use, disclosure, dis-*  
 7 *ruption, modification, or destruction of which would have*  
 8 *a debilitating impact on the mission of the Central Intel-*  
 9 *ligence Agency.*”.

10           (c) *TECHNICAL AND CONFORMING AMENDMENTS.*—

11           (1) *TABLE OF SECTIONS.*—*The table of sections*  
 12 *for chapter 35 of title 44, United States Code, is*  
 13 *amended by striking the matter relating to sub-*  
 14 *chapters II and III and inserting the following:*

“SUBCHAPTER II—INFORMATION SECURITY

“3550. *Purposes.*

“3551. *Definitions.*

“3552. *Authority and functions of the National Center for Cybersecurity and*  
*Communications.*

“3553. *Agency responsibilities.*

“3554. *Annual operational evaluation.*

“3555. *Federal Information Security Taskforce.*

“3556. *Independent assessments.*

“3557. *Protection of information.*

“3558. *Department of Defense and Central Intelligence Agency systems.*”.

15           (2) *OTHER REFERENCES.*—

16           (A) *Section 1001(c)(1)(A) of the Homeland*  
 17 *Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is*  
 18 *amended by striking “section 3532(3)” and in-*  
 19 *serting “section 3551(b)”.*

1           (B) Section 2222(j)(6) of title 10, United  
2 States Code, is amended by striking “section  
3 3542(b)(2))” and inserting “section 3551(b)”.

4           (C) Section 2223(c)(3) of title 10, United  
5 States Code, is amended, by striking “section  
6 3542(b)(2))” and inserting “section 3551(b)”.

7           (D) Section 2315 of title 10, United States  
8 Code, is amended by striking “section  
9 3542(b)(2))” and inserting “section 3551(b)”.

10           (E) Section 20(a)(2) of the National Insti-  
11 tute of Standards and Technology Act (15 U.S.C.  
12 278g-3) is amended by striking “section  
13 3532(b)(2)” and inserting “section 3551(b)”.

14           (F) Section 21(b)(2) of the National Insti-  
15 tute of Standards and Technology Act (15 U.S.C.  
16 278g-4(b)(2)) is amended by striking “Institute  
17 and” and inserting “Institute, the Director of the  
18 National Center on Cybersecurity and Commu-  
19 nications, and”.

20           (G) Section 21(b)(3) of the National Insti-  
21 tute of Standards and Technology Act (15 U.S.C.  
22 278g-4(b)(3)) is amended by inserting “the Di-  
23 rector of the National Center on Cybersecurity  
24 and Communications,” after “the Director of the  
25 National Security Agency,”.

1           (H) Section 8(d)(1) of the Cyber Security  
2           Research and Development Act (15 U.S.C.  
3           7406(d)(1)) is amended by striking “section  
4           3534(b)” and inserting “section 3553(b)”.

5           (3) *HOMELAND SECURITY ACT OF 2002.*—

6           (A) *TITLE X.*—*The Homeland Security Act*  
7           *of 2002 (6 U.S.C. 101 et seq.) is amended by*  
8           *striking title X.*

9           (B) *TABLE OF CONTENTS.*—*The table of*  
10          *contents in section 1(b) of the Homeland Secu-*  
11          *rity Act of 2002 (6 U.S.C. 101 et seq.) is amend-*  
12          *ed by striking the matter relating to title X.*

13          (d) *REPEAL OF OTHER STANDARDS.*—

14          (1) *IN GENERAL.*—*Section 11331 of title 40,*  
15          *United States Code, is repealed.*

16          (2) *TECHNICAL AND CONFORMING AMEND-*  
17          *MENTS.*—

18          (A) Section 20(c)(3) of the National Insti-  
19          tute of Standards and Technology Act (15 U.S.C.  
20          278g–3(c)(3)) is amended by striking “under sec-  
21          tion 11331 of title 40, United States Code”.

22          (B) Section 20(d)(1) of the National Insti-  
23          tute of Standards and Technology Act (15 U.S.C.  
24          278g–3(d)(1)) is amended by striking “the Direc-  
25          tor of the Office of Management and Budget for

1           *promulgation under section 11331 of title 40,*  
2           *United States Code” and inserting “the Sec-*  
3           *retary of Commerce for promulgation”.*

4           *(C) Section 11302(d) of title 40, United*  
5           *States Code, is amended by striking “under sec-*  
6           *tion 11331 of this title and”.*

7           *(D) Section 1874A (e)(2)(A)(ii) of the So-*  
8           *cial Security Act (42 U.S.C.1395kk-1*  
9           *(e)(2)(A)(ii)) is amended by striking “section*  
10           *11331 of title 40, United States Code” and in-*  
11           *serting “section 3552 of title 44, United States*  
12           *Code”.*

13           *(E) Section 3504(g)(2) of title 44, United*  
14           *States Code, is amended by striking “section*  
15           *11331 of title 40” and inserting “section 3552 of*  
16           *title 44”.*

17           *(F) Section 3504(h)(1) of title 44, United*  
18           *States Code, is amended by inserting “, the Di-*  
19           *rector of the National Center for Cybersecurity*  
20           *and Communications,” after “the National Insti-*  
21           *tute of Standards and Technology”.*

22           *(G) Section 3504(h)(1)(B) of title 44,*  
23           *United States Code, is amended by striking*  
24           *“under section 11331 of title 40” and inserting*  
25           *“section 3552 of title 44”.*

1           (H) Section 3518(d) of title 44, United  
 2 States Code, is amended by striking “sections  
 3 11331 and 11332” and inserting “section  
 4 11332”.

5           (I) Section 3602(f)(8) of title 44, United  
 6 States Code, is amended by striking “under sec-  
 7 tion 11331 of title 40.

8           (J) Section 3603(f)(5) of title 44, United  
 9 States Code, is amended by striking “and pro-  
 10 mulgated under section 11331 of title 40,”.

11       **TITLE IV—RECRUITMENT AND**  
 12       **PROFESSIONAL DEVELOPMENT**

13       **SEC. 401. DEFINITIONS.**

14       *In this title:*

15           (1) **CYBERSECURITY MISSION.**—The term “cyber-  
 16 security mission” means the activities of the Federal  
 17 Government that encompass the full range of threat  
 18 reduction, vulnerability reduction, deterrence, inter-  
 19 national engagement, incident response, resiliency,  
 20 and recovery policies and activities, including com-  
 21 puter network operations, information assurance, law  
 22 enforcement, diplomacy, military, and intelligence  
 23 missions as such activities relate to the security and  
 24 stability of cyberspace.

1           (2) *FEDERAL AGENCY'S CYBERSECURITY MIS-*  
2           *SION.—The term “Federal agency’s cybersecurity mis-*  
3           *sion” means, with respect to any Federal agency, the*  
4           *portion of the cybersecurity mission that is the re-*  
5           *sponsibility of the Federal agency.*

6 **SEC. 402. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

7           (a) *IN GENERAL.—The Director of the Office of Per-*  
8           *sonnel Management and the Director shall assess the readi-*  
9           *ness and capacity of the Federal workforce to meet the needs*  
10          *of the cybersecurity mission of the Federal Government.*

11          (b) *STRATEGY.—*

12                 (1) *IN GENERAL.—The Director of the Office of*  
13                 *Personnel Management, in consultation with the Di-*  
14                 *rector and the Director of the Office of Management*  
15                 *and Budget, shall develop a comprehensive workforce*  
16                 *strategy that enhances the readiness, capacity, train-*  
17                 *ing, and recruitment and retention of Federal cyber-*  
18                 *security personnel.*

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

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

23                         (B) *10-year and 20-year projections of*  
24                         *workforce needs.*

1           (3) *DATES FOR COMPLETION.*—*The strategy*  
2           *under this subsection shall be—*

3                   (A) *completed not later than 180 days after*  
4                   *the date of enactment of this Act; and*

5                   (B) *updated as needed.*

6 **SEC. 403. STRATEGIC CYBERSECURITY WORKFORCE PLAN-**  
7                   **NING.**

8           (a) *FEDERAL AGENCY DEVELOPMENT OF STRATEGIC*  
9           *CYBERSECURITY WORKFORCE PLANS.*—*Not later than 180*  
10           *days after the date of enactment of this Act and in every*  
11           *subsequent year, and subject to subsection (c)(2), the head*  
12           *of each Federal agency shall develop a strategic cybersecu-*  
13           *rity workforce plan as part of the Federal agency perform-*  
14           *ance plan required under section 1115 of title 31, United*  
15           *States Code.*

16           (b) *BASIS AND GUIDANCE FOR PLANS.*—*Each Federal*  
17           *agency shall develop a plan prepared under subsection (a)*  
18           *on the basis of the assessment developed under section 402*  
19           *and any subsequent guidance issued by the Director of the*  
20           *Office of Personnel Management, in consultation with the*  
21           *Director and the Director of the Office of Management and*  
22           *Budget.*

23           (c) *CONTENTS OF THE PLAN.*—

1           (1) *IN GENERAL.*—Subject to paragraph (2),  
2           each plan prepared under subsection (a) shall in-  
3           clude—

4                   (A) a description of the Federal agency’s cy-  
5                   bersecurity mission;

6                   (B) a description and analysis, relating to  
7                   the specialized workforce needed by the Federal  
8                   agency to fulfill the Federal agency’s cybersecu-  
9                   rity mission, including—

10                           (i) the workforce needs of the Federal  
11                           agency on the date of the report, and 10-  
12                           year and 20-year projections of workforce  
13                           needs;

14                           (ii) hiring projections to meet work-  
15                           force needs, including, for at least a 2-year  
16                           period, specific occupation and grade levels;

17                           (iii) long-term and short-term strategic  
18                           goals to address critical skills deficiencies,  
19                           including analysis of the numbers of and  
20                           reasons for attrition of employees;

21                           (iv) recruitment strategies, including  
22                           the use of student internships, part-time  
23                           employment, student loan reimbursement,  
24                           and telework, to attract highly qualified

1 candidates from diverse backgrounds and  
2 geographic locations;

3 (v) an assessment of the sources and  
4 availability of individuals with needed ex-  
5 pertise;

6 (vi) ways to streamline the hiring  
7 process;

8 (vii) the barriers to recruiting and hir-  
9 ing individuals qualified in cybersecurity  
10 and recommendations to overcome the bar-  
11 riers; and

12 (viii) a training and development  
13 plan, consistent with the curriculum devel-  
14 oped under section 406, to enhance and im-  
15 prove the knowledge of employees.

16 (2) *FEDERAL AGENCIES WITH SMALL SPECIAL-*  
17 *IZED WORKFORCE.*—*In accordance with guidance*  
18 *issued under subsection (b), a Federal agency that*  
19 *needs only a small specialized workforce to fulfill the*  
20 *Federal agency’s cybersecurity mission may, in lieu*  
21 *of developing a separate strategic cybersecurity work-*  
22 *force plan, present the workforce plan component re-*  
23 *ferred to in paragraph (1)(A) and those components*  
24 *referred to in paragraph (1)(B) that are relevant and*  
25 *appropriate to the circumstances of the agency as*

1        *part of the Federal agency performance plan required*  
2        *under section 1115 of title 31, United States Code.*

3        **SEC. 404. CYBERSECURITY OCCUPATION CLASSIFICATIONS.**

4        *(a) IN GENERAL.—Not later than 1 year after the date*  
5        *of enactment of this Act, the Director of the Office of Per-*  
6        *sonnel Management, in coordination with the Director,*  
7        *shall develop and issue comprehensive occupation classifica-*  
8        *tions for Federal employees engaged in cybersecurity mis-*  
9        *sions.*

10        *(b) APPLICABILITY OF CLASSIFICATIONS.—The Direc-*  
11        *tor of the Office of Personnel Management shall ensure that*  
12        *the comprehensive occupation classifications issued under*  
13        *subsection (a) may be used throughout the Federal Govern-*  
14        *ment.*

15        **SEC. 405. MEASURES OF CYBERSECURITY HIRING EFFEC-**  
16        **TIVENESS.**

17        *(a) IN GENERAL.—The head of each Federal agency*  
18        *shall measure, and collect information on, indicators of the*  
19        *effectiveness of the recruitment and hiring by the Federal*  
20        *agency of a workforce needed to fulfill the Federal agency's*  
21        *cybersecurity mission.*

22        *(b) TYPES OF INFORMATION.—The indicators of effec-*  
23        *tiveness measured and subject to collection of information*  
24        *under subsection (a) shall include indicators with respect*  
25        *to the following:*

1           (1) *RECRUITING AND HIRING.*—*In relation to re-*  
2           *cruiting and hiring by the Federal agency—*

3                   (A) *the ability to reach and recruit well-*  
4                   *qualified individuals from diverse talent pools;*

5                   (B) *the use and impact of special hiring au-*  
6                   *thorities and flexibilities to recruit the most*  
7                   *qualified applicants, including the use of student*  
8                   *internship and scholarship programs for perma-*  
9                   *nent hires;*

10                  (C) *the use and impact of special hiring au-*  
11                  *thorities and flexibilities to recruit diverse can-*  
12                  *didates, including criteria such as the veteran*  
13                  *status, race, ethnicity, gender, disability, or na-*  
14                  *tional origin of the candidates; and*

15                  (D) *the educational level, and source of ap-*  
16                  *plicants.*

17           (2) *SUPERVISORS.*—*In relation to the super-*  
18           *visors of the positions being filled—*

19                   (A) *satisfaction with the quality of the ap-*  
20                   *plicants interviewed and hired;*

21                   (B) *satisfaction with the match between the*  
22                   *skills of the individuals and the needs of the Fed-*  
23                   *eral agency;*

24                   (C) *satisfaction of the supervisors with the*  
25                   *hiring process and hiring outcomes;*

1           (D) whether any mission-critical defi-  
2           ciencies were addressed by the individuals and  
3           the connection between the deficiencies and the  
4           performance of the Federal agency; and

5           (E) the satisfaction of the supervisors with  
6           the period of time elapsed to fill the positions.

7           (3) *APPLICANTS.*—The satisfaction of applicants  
8           with the hiring process, including clarity of job an-  
9           nouncements, any reasons for withdrawal of an ap-  
10          plication, the user-friendliness of the application  
11          process, communication regarding status of applica-  
12          tions, and the timeliness of offers of employment.

13          (4) *HIRED INDIVIDUALS.*—In relation to the in-  
14          dividuals hired—

15               (A) satisfaction with the hiring process;

16               (B) satisfaction with the process of starting  
17               employment in the position for which the indi-  
18               vidual was hired;

19               (C) attrition; and

20               (D) the results of exit interviews.

21          (c) *REPORTS.*—

22               (1) *IN GENERAL.*—The head of each Federal  
23               agency shall submit the information collected under  
24               this section to the Director of the Office of Personnel

1        *Management on an annual basis and in accordance*  
2        *with the regulations issued under subsection (d).*

3                (2) *AVAILABILITY OF RECRUITING AND HIRING*  
4        *INFORMATION.—*

5                (A) *IN GENERAL.—The Director of the Of-*  
6        *fice of Personnel Management shall prepare an*  
7        *annual report containing the information re-*  
8        *ceived under paragraph (1) in a consistent for-*  
9        *mat to allow for a comparison of hiring effective-*  
10       *ness and experience across demographic groups*  
11       *and Federal agencies.*

12               (B) *SUBMISSION.—The Director of the Of-*  
13       *fice of Personnel Management shall—*

14               (i) *not later than 90 days after the re-*  
15       *ceipt of all information required to be sub-*  
16       *mitted under paragraph (1), make the re-*  
17       *port prepared under subparagraph (A) pub-*  
18       *licly available, including on the website of*  
19       *the Office of Personnel Management; and*

20               (ii) *before the date on which the report*  
21       *prepared under subparagraph (A) is made*  
22       *publicly available, submit the report to*  
23       *Congress.*

24        (d) *REGULATIONS.—*

1           (1) *IN GENERAL.*—Not later than 180 days after  
2           the date of enactment of this Act, the Director of the  
3           Office of Personnel Management shall issue regula-  
4           tions establishing the methodology, timing, and re-  
5           porting of the data required to be submitted under  
6           this section.

7           (2) *SCOPE AND DETAIL OF REQUIRED INFORMA-*  
8           *TION.*—The regulations under paragraph (1) shall de-  
9           limit the scope and detail of the information that a  
10          Federal agency is required to collect and submit  
11          under this section, taking account of the size and  
12          complexity of the workforce that the Federal agency  
13          needs to fulfill the Federal agency’s cybersecurity mis-  
14          sion.

15 **SEC. 406. TRAINING AND EDUCATION.**

16          (a) *TRAINING.*—

17               (1) *FEDERAL GOVERNMENT EMPLOYEES AND*  
18               *FEDERAL CONTRACTORS.*—The Director of the Office  
19               of Personnel Management, in conjunction with the  
20               Director of the National Center for Cybersecurity and  
21               Communications, the Director of National Intel-  
22               ligence, the Secretary of Defense, and the Chief Infor-  
23               mation Officers Council established under section  
24               3603 of title 44, United States Code, shall establish a  
25               cybersecurity awareness and education curriculum

1        *that shall be required for all Federal employees and*  
2        *contractors engaged in the design, development, or op-*  
3        *eration of agency information infrastructure, as de-*  
4        *efined under section 3551 of title 44, United States*  
5        *Code.*

6            (2) *CONTENTS.—The curriculum established*  
7        *under paragraph (1) may include—*

8            (A) *role-based security awareness training;*

9            (B) *recommended cybersecurity practices;*

10          (C) *cybersecurity recommendations for trav-*  
11        *eling abroad;*

12          (D) *unclassified counterintelligence infor-*  
13        *mation;*

14          (E) *information regarding industrial espio-*  
15        *nage;*

16          (F) *information regarding malicious activ-*  
17        *ity online;*

18          (G) *information regarding cybersecurity*  
19        *and law enforcement;*

20          (H) *identity management information;*

21          (I) *information regarding supply chain se-*  
22        *curity;*

23          (J) *information security risks associated*  
24        *with the activities of Federal employees; and*

1                   (K) the responsibilities of Federal employees  
2                   in complying with policies and procedures de-  
3                   signed to reduce information security risks iden-  
4                   tified under subparagraph (J).

5                   (3) FEDERAL CYBERSECURITY PROFES-  
6                   SIONALS.—The Director of the Office of Personnel  
7                   Management in conjunction with the Director of the  
8                   National Center for Cybersecurity and Communica-  
9                   tions, the Director of National Intelligence, the Sec-  
10                  retary of Defense, the Director of the Office of Man-  
11                  agement and Budget, and, as appropriate, colleges,  
12                  universities, and nonprofit organizations with cyber-  
13                  security training expertise, shall develop a program,  
14                  to provide training to improve and enhance the skills  
15                  and capabilities of Federal employees engaged in the  
16                  cybersecurity mission, including training specific to  
17                  the acquisition workforce.

18                  (4) HEADS OF FEDERAL AGENCIES.—Not later  
19                  than 30 days after the date on which an individual  
20                  is appointed to a position at level I or II of the Exec-  
21                  utive Schedule, the Director of the National Center for  
22                  Cybersecurity and Communications and the Director  
23                  of National Intelligence, or their designees, shall pro-  
24                  vide that individual with a cybersecurity threat brief-  
25                  ing.

1           (5) *CERTIFICATION.*—*The head of each Federal*  
2 *agency shall include in the annual report required*  
3 *under section 3553(c) of title 44, United States Code,*  
4 *a certification regarding whether all officers, employ-*  
5 *ees, and contractors of the Federal agency have com-*  
6 *pleted the training required under this subsection.*

7           (b) *EDUCATION.*—

8           (1) *FEDERAL EMPLOYEES.*—*The Director of the*  
9 *Office of Personnel Management, in coordination with*  
10 *the Secretary of Education, the Director of the Na-*  
11 *tional Science Foundation, and the Director, shall de-*  
12 *velop and implement a strategy to provide Federal*  
13 *employees who work in cybersecurity missions with*  
14 *the opportunity to obtain additional education.*

15           (2) *K THROUGH 12.*—*The Secretary of Edu-*  
16 *cation, in coordination with the Director of the Na-*  
17 *tional Center for Cybersecurity and Communications*  
18 *and State and local governments, shall develop cur-*  
19 *riculum standards, guidelines, and recommended*  
20 *courses to address cyber safety, cybersecurity, and*  
21 *cyber ethics for students in kindergarten through*  
22 *grade 12.*

23           (3) *UNDERGRADUATE, GRADUATE, VOCATIONAL,*  
24 *AND TECHNICAL INSTITUTIONS.*—

1           (A) *SECRETARY OF EDUCATION.*—*The Sec-*  
2           *retary of Education, in coordination with the*  
3           *Director of the National Center for Cybersecurity*  
4           *and Communications, shall—*

5                   (i) *develop curriculum standards and*  
6                   *guidelines to address cyber safety, cybersecu-*  
7                   *rity, and cyber ethics for all students en-*  
8                   *rolled in undergraduate, graduate, voca-*  
9                   *tional, and technical institutions in the*  
10                  *United States; and*

11                  (ii) *analyze and develop recommended*  
12                  *courses for students interested in pursuing*  
13                  *careers in information technology, commu-*  
14                  *nications, computer science, engineering,*  
15                  *math, and science, as those subjects relate to*  
16                  *cybersecurity.*

17           (B) *OFFICE OF PERSONNEL MANAGE-*  
18           *MENT.*—*The Director of the Office of Personnel*  
19           *Management, in coordination with the Director,*  
20           *shall develop strategies and programs—*

21                   (i) *to recruit students from under-*  
22                   *graduate, graduate, vocational, and tech-*  
23                   *nical institutions in the United States to*  
24                   *serve as Federal employees engaged in cyber*  
25                   *missions; and*

1                   (ii) that provide internship and part-  
2                   time work opportunities with the Federal  
3                   Government for students at the under-  
4                   graduate, graduate, vocational, and tech-  
5                   nical institutions in the United States.

6           (c) *CYBER TALENT COMPETITIONS AND CHAL-*  
7 *LENGES.—*

8                   (1) *IN GENERAL.—The Director of the National*  
9                   *Center for Cybersecurity and Communications shall*  
10                   *establish a program to ensure the effective operation*  
11                   *of national and statewide competitions and challenges*  
12                   *that seek to identify, develop, and recruit talented in-*  
13                   *dividuals to work in Federal agencies, State and local*  
14                   *government agencies, and the private sector to per-*  
15                   *form duties relating to the security of the Federal in-*  
16                   *formation infrastructure or the national information*  
17                   *infrastructure.*

18                   (2) *GROUPS AND INDIVIDUALS.—The program*  
19                   *under this subsection shall include—*

20                           (A) *high school students;*

21                           (B) *undergraduate students;*

22                           (C) *graduate students;*

23                           (D) *academic and research institutions;*

24                           (E) *veterans; and*

1           (F) other groups or individuals as the Di-  
2           rector may determine.

3           (3) *SUPPORT OF OTHER COMPETITIONS AND*  
4           *CHALLENGES.*—The program under this subsection  
5           may support other competitions and challenges not es-  
6           tablished under this subsection through affiliation and  
7           cooperative agreements with—

8                   (A) Federal agencies;

9                   (B) regional, State, or community school  
10                  programs supporting the development of cyber  
11                  professionals; or

12                  (C) other private sector organizations.

13           (4) *AREAS OF TALENT.*—The program under this  
14           subsection shall seek to identify, develop, and recruit  
15           exceptional talent relating to—

16                   (A) ethical hacking;

17                   (B) penetration testing;

18                   (C) vulnerability Assessment;

19                   (D) continuity of system operations;

20                   (E) cyber forensics; and

21                   (F) offensive and defensive cyber operations.

22 **SEC. 407. CYBERSECURITY INCENTIVES.**

23           (a) *AWARDS.*—In making cash awards under chapter  
24 45 of title 5, United States Code, the President or the head  
25 of a Federal agency, in consultation with the Director, shall

1 *consider the success of an employee in fulfilling the objec-*  
2 *tives of the National Strategy, in a manner consistent with*  
3 *any policies, guidelines, procedures, instructions, or stand-*  
4 *ards established by the President.*

5 (b) *OTHER INCENTIVES.*—*The head of each Federal*  
6 *agency shall adopt best practices, developed by the Director*  
7 *of the National Center for Cybersecurity and Communica-*  
8 *tions and the Office of Management and Budget, regarding*  
9 *effective ways to educate and motivate employees of the Fed-*  
10 *eral Government to demonstrate leadership in cybersecu-*  
11 *arity, including—*

12 (1) *promotions and other nonmonetary awards;*  
13 *and*

14 (2) *publicizing information sharing accomplish-*  
15 *ments by individual employees and, if appropriate,*  
16 *the tangible benefits that resulted.*

17 **SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR**  
18 **THE NATIONAL CENTER FOR CYBERSECURITY**  
19 **AND COMMUNICATIONS.**

20 (a) *DEFINITIONS.*—*In this section:*

21 (1) *CENTER.*—*The term “Center” means the Na-*  
22 *tional Center for Cybersecurity and Communications.*

23 (2) *DEPARTMENT.*—*The term “Department”*  
24 *means the Department of Homeland Security.*

1           (3) *DIRECTOR.*—*The term “Director” means the*  
2 *Director of the Center.*

3           (4) *ENTRY LEVEL POSITION.*—*The term “entry*  
4 *level position” means a position that—*

5                   (A) *is established by the Director in the*  
6 *Center; and*

7                   (B) *is classified at GS-7, GS-8, or GS-9 of*  
8 *the General Schedule.*

9           (5) *SECRETARY.*—*The term “Secretary” means*  
10 *the Secretary of Homeland Security.*

11           (6) *SENIOR POSITION.*—*The term “senior posi-*  
12 *tion” means a position that—*

13                   (A) *is established by the Director in the*  
14 *Center; and*

15                   (B) *is not established under section 5108 of*  
16 *title 5, United States Code, but is similar in du-*  
17 *ties and responsibilities for positions established*  
18 *under that section.*

19           (b) *RECRUITMENT AND RETENTION PROGRAM.*—

20                   (1) *ESTABLISHMENT.*—*The Director may estab-*  
21 *lish a program to assist in the recruitment and reten-*  
22 *tion of highly skilled personnel to carry out the func-*  
23 *tions of the Center.*

1           (2) *CONSULTATION AND CONSIDERATIONS.*—*In*  
2 *establishing a program under this section, the Direc-*  
3 *tor shall—*

4                   (A) *consult with the Secretary; and*

5                   (B) *consider—*

6                           (i) *national and local employment*  
7 *trends;*

8                           (ii) *the availability and quality of*  
9 *candidates;*

10                           (iii) *any specialized education or cer-*  
11 *tifications required for positions;*

12                           (iv) *whether there is a shortage of cer-*  
13 *tain skills; and*

14                           (v) *such other factors as the Director*  
15 *determines appropriate.*

16       (c) *HIRING AND SPECIAL PAY AUTHORITIES.*—

17                   (1) *DIRECT HIRE AUTHORITY.*—*Without regard*  
18 *to the civil service laws (other than sections 3303 and*  
19 *3328 of title 5, United States Code), the Director may*  
20 *appoint not more than 500 employees under this sub-*  
21 *section to carry out the functions of the Center.*

22                   (2) *RATES OF PAY.*—

23                           (A) *ENTRY LEVEL POSITIONS.*—*The Direc-*  
24 *tor may fix the pay of the employees appointed*  
25 *to entry level positions under this subsection*

1           *without regard to chapter 51 and subchapter III*  
2           *of chapter 53 of title 5, United States Code, re-*  
3           *lating to classification of positions and General*  
4           *Schedule pay rates, except that the rate of pay*  
5           *for any such employee may not exceed the max-*  
6           *imum rate of basic pay payable for a position*  
7           *at GS-10 of the General Schedule while that em-*  
8           *ployee is in an entry level position.*

9           *(B) SENIOR POSITIONS.—*

10           *(i) IN GENERAL.—The Director may*  
11           *fix the pay of the employees appointed to*  
12           *senior positions under this subsection with-*  
13           *out regard to chapter 51 and subchapter III*  
14           *of chapter 53 of title 5, United States Code,*  
15           *relating to classification of positions and*  
16           *General Schedule pay rates, except that the*  
17           *rate of pay for any such employee may not*  
18           *exceed the maximum rate of basic pay pay-*  
19           *able under section 5376 of title 5, United*  
20           *States Code.*

21           *(ii) HIGHER MAXIMUM RATES.—*

22           *(I) IN GENERAL.—Notwith-*  
23           *standing the limitation on rates of pay*  
24           *under clause (i)—*

1           (aa) not more than 20 em-  
2           ployees, identified by the Director,  
3           may be paid at a rate of pay not  
4           to exceed the maximum rate of  
5           basic pay payable for a position  
6           at level I of the Executive Sched-  
7           ule under section 5312 of title 5,  
8           United States Code; and

9           (bb) not more than 5 employ-  
10          ees, identified by the Director  
11          with the approval of the Sec-  
12          retary, may be paid at a rate of  
13          pay not to exceed the maximum  
14          rate of basic pay payable for the  
15          Vice President under section 104  
16          of title 3, United States Code.

17           (II) NONDELEGATION OF AUTHOR-  
18          ITY.—The Secretary or the Director  
19          may not delegate any authority under  
20          this clause.

21          (d) CONVERSION TO COMPETITIVE SERVICE.—

22           (1) DEFINITION.—In this subsection, the term  
23          “qualified employee” means any individual ap-  
24          pointed to an excepted service position in the Depart-  
25          ment who performs functions relating to the security

1 *of the Federal information infrastructure or national*  
2 *information infrastructure.*

3 (2) *COMPETITIVE CIVIL SERVICE STATUS.—In*  
4 *consultation with the Director, the Secretary may*  
5 *grant competitive civil service status to a qualified*  
6 *employee if that employee is —*

7 (A) *employed in the Center; or*

8 (B) *transferring to the Center.*

9 (e) *RETENTION BONUSES.—*

10 (1) *AUTHORITY.—Notwithstanding section 5754*  
11 *of title 5, United States Code, the Director may—*

12 (A) *pay a retention bonus under that sec-*  
13 *tion to any individual appointed under this sub-*  
14 *section, if the Director determines that, in the*  
15 *absence of a retention bonus, there is a high risk*  
16 *that the individual would likely leave employ-*  
17 *ment with the Department; and*

18 (B) *exercise the authorities of the Office of*  
19 *Personnel Management and the head of an agen-*  
20 *cy under that section with respect to retention*  
21 *bonuses paid under this subsection.*

22 (2) *LIMITATIONS ON AMOUNT OF ANNUAL BO-*  
23 *NUSES.—*

24 (A) *DEFINITIONS.—In this paragraph:*

1                   (i) *MAXIMUM TOTAL PAY.*—The term  
2 “maximum total pay” means—

3                   (I) *in the case of an employee de-*  
4 *scribed under subsection(c)(2)(B)(i),*  
5 *the total amount of pay paid in a cal-*  
6 *endar year at the maximum rate of*  
7 *basic pay payable for a position at*  
8 *level I of the Executive Schedule under*  
9 *section 5312 of title 5, United States*  
10 *Code;*

11                   (II) *in the case of an employee de-*  
12 *scribed under sub-*  
13 *section(c)(2)(B)(ii)(I)(aa), the total*  
14 *amount of pay paid in a calendar year*  
15 *at the maximum rate of basic pay*  
16 *payable for a position at level I of the*  
17 *Executive Schedule under section 5312*  
18 *of title 5, United States Code; and*

19                   (III) *in the case of an employee*  
20 *described under sub-*  
21 *section(c)(2)(B)(ii)(I)(bb), the total*  
22 *amount of pay paid in a calendar year*  
23 *at the maximum rate of basic pay*  
24 *payable for the Vice President under*

1                    *section 104 of title 3, United States*  
2                    *Code.*

3                    *(ii) TOTAL COMPENSATION.—The term*  
4                    *“total compensation” means—*

5                    *(I) the amount of pay paid to an*  
6                    *employee in any calendar year; and*

7                    *(II) the amount of all retention*  
8                    *bonuses paid to an employee in any*  
9                    *calendar year.*

10                  *(B) LIMITATION.—The Director may not*  
11                  *pay a retention bonus under this subsection to*  
12                  *an employee that would result in the total com-*  
13                  *ensation of that employee exceeding maximum*  
14                  *total pay.*

15                  *(f) TERMINATION OF AUTHORITY.—The authority to*  
16                  *make appointments and pay retention bonuses under this*  
17                  *section shall terminate 3 years after the date of enactment*  
18                  *of this Act.*

19                  *(g) REPORTS.—*

20                  *(1) PLAN FOR EXECUTION OF AUTHORITIES.—*  
21                  *Not later than 120 days of enactment of this Act, the*  
22                  *Director shall submit a report to the appropriate*  
23                  *committees of Congress with a plan for the execution*  
24                  *of the authorities provided under this section.*

1           (2) *ANNUAL REPORT.*—Not later than 6 months  
2 after the date of enactment of this Act, and every year  
3 thereafter, the Director shall submit to the appro-  
4 priate committees of Congress a detailed report that—

5                   (A) discusses how the actions taken during  
6 the period of the report are fulfilling the critical  
7 hiring needs of the Center;

8                   (B) assesses metrics relating to individuals  
9 hired under the authority of this section, includ-  
10 ing—

11                           (i) the numbers of individuals hired;

12                           (ii) the turnover in relevant positions;

13                           (iii) with respect to each individual  
14 hired—

15                                   (I) the position for which hired;

16                                   (II) the salary paid;

17                                   (III) any retention bonus paid  
18 and the amount of the bonus;

19                                   (IV) the geographic location from  
20 which hired;

21                                   (V) the immediate past salary;  
22 and

23                                   (VI) whether the individual was a  
24 noncareer appointee in the Senior Ex-  
25 ecutive Service or an appointee to a

- 1                    *position of a confidential or policy-de-*  
2                    *termining character under schedule C*  
3                    *of subpart C of part 213 of title 5 of*  
4                    *the Code of Federal Regulations before*  
5                    *the hiring; and*
- 6                    *(iv) whether public notice for recruit-*  
7                    *ment was made, and if so—*
- 8                    *(I) the total number of qualified*  
9                    *applicants;*
- 10                    *(II) the number of veteran pref-*  
11                    *erence eligible candidates who applied;*
- 12                    *(III) the time from posting to job*  
13                    *offer; and*
- 14                    *(IV) statistics on diversity, in-*  
15                    *cluding age, disability, race, gender,*  
16                    *and national origin, of individuals*  
17                    *hired under the authority of this sec-*  
18                    *tion to the extent such statistics are*  
19                    *available; and*
- 20                    *(C) includes rates of pay set in accordance*  
21                    *with subsection (c).*

1     **TITLE V—OTHER PROVISIONS**

2     **SEC. 501. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

3             *Subtitle D of title II of the Homeland Security Act*  
 4 *of 2002 (6 U.S.C. 161 et seq.) is amended by adding at*  
 5 *the end the following:*

6     **“SEC. 238. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

7             “(a) *ESTABLISHMENT OF RESEARCH AND DEVELOP-*  
 8 *MENT PROGRAM.—The Under Secretary for Science and*  
 9 *Technology, in coordination with the Director of the Na-*  
 10 *tional Center for Cybersecurity and Communications, shall*  
 11 *carry out a research and development program for the pur-*  
 12 *pose of improving the security of information infrastruc-*  
 13 *ture.*

14            “(b) *ELIGIBLE PROJECTS.—The research and develop-*  
 15 *ment program carried out under subsection (a) may include*  
 16 *projects to—*

17                 “(1) *advance the development and accelerate the*  
 18 *deployment of more secure versions of fundamental*  
 19 *Internet protocols and architectures, including for the*  
 20 *secure domain name addressing system and routing*  
 21 *security;*

22                 “(2) *improve and create technologies for detect-*  
 23 *ing and analyzing attacks or intrusions, including*  
 24 *analysis of malicious software;*

1           “(3) improve and create mitigation and recovery  
2           methodologies, including techniques for containment  
3           of attacks and development of resilient networks and  
4           systems;

5           “(4) develop and support infrastructure and  
6           tools to support cybersecurity research and develop-  
7           ment efforts, including modeling, testbeds, and data  
8           sets for assessment of new cybersecurity technologies;

9           “(5) assist the development and support of tech-  
10          nologies to reduce vulnerabilities in process control  
11          systems;

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

14          “(7) test, evaluate, and facilitate, with appro-  
15          priate protections for any proprietary information  
16          concerning the technologies, the transfer of tech-  
17          nologies associated with the engineering of less vulner-  
18          able software and securing the information technology  
19          software development lifecycle;

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

22          “(9) assist the development of technologies de-  
23          signed to increase the security and resiliency of tele-  
24          communications networks;

1           “(10) advance the protection of privacy and civil  
2           liberties in cybersecurity technology and practices;  
3           and

4           “(11) address other risks identified by the Direc-  
5           tor of the National Center for Cybersecurity and Com-  
6           munications.

7           “(c) COORDINATION WITH OTHER RESEARCH INITIA-  
8           TIVES.—The Under Secretary—

9           “(1) shall ensure that the research and develop-  
10          ment program carried out under subsection (a) is  
11          consistent with the national strategy to increase the  
12          security and resilience of cyberspace developed by the  
13          Director of Cyberspace Policy under section 101 of the  
14          Protecting Cyberspace as a National Asset Act of  
15          2010, or any succeeding strategy;

16          “(2) shall, to the extent practicable, coordinate  
17          the research and development activities of the Depart-  
18          ment with other ongoing research and development se-  
19          curity-related initiatives, including research being  
20          conducted by—

21                  “(A) the National Institute of Standards  
22                  and Technology;

23                  “(B) the National Science Foundation;

24                  “(C) the National Academy of Sciences;

1           “(D) other Federal agencies, as defined  
2           under section 241;

3           “(E) other Federal and private research lab-  
4           oratories, research entities, and universities and  
5           institutions of higher education, and relevant  
6           nonprofit organizations; and

7           “(F) international partners of the United  
8           States;

9           “(3) shall carry out any research and develop-  
10          ment project under subsection (a) through a reimburs-  
11          able agreement with an appropriate Federal agency,  
12          as defined under section 241, if the Federal agency—

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

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

17           “(4) may make grants to, or enter into coopera-  
18          tive agreements, contracts, other transactions, or re-  
19          imbursable agreements with, the entities described in  
20          paragraph (2); and

21           “(5) shall submit a report to the appropriate  
22          committees of Congress on a review of the cybersecu-  
23          rity activities, and the capacity, of the national lab-  
24          oratories and other research entities available to the  
25          Department to determine if the establishment of a na-

1        *tional laboratory dedicated to cybersecurity research*  
2        *and development is necessary.*

3        “(d) *PRIVACY AND CIVIL RIGHTS AND CIVIL LIB-*  
4        *ERTIES ISSUES.—*

5                “(1) *CONSULTATION.—In carrying out research*  
6        *and development projects under subsection (a), the*  
7        *Under Secretary shall consult with the Privacy Offi-*  
8        *cer appointed under section 222 and the Officer for*  
9        *Civil Rights and Civil Liberties of the Department*  
10        *appointed under section 705.*

11                “(2) *PRIVACY IMPACT ASSESSMENTS.—In accord-*  
12        *ance with sections 222 and 705, the Privacy Officer*  
13        *shall conduct privacy impact assessments and the Of-*  
14        *ficer for Civil Rights and Civil Liberties shall conduct*  
15        *reviews, as appropriate, for research and development*  
16        *projects carried out under subsection (a) that the*  
17        *Under Secretary determines could have an impact on*  
18        *privacy, civil rights, or civil liberties.*

19        “**SEC. 239. NATIONAL CYBERSECURITY ADVISORY COUNCIL.**

20                “(a) *ESTABLISHMENT.—Not later than 90 days after*  
21        *the date of enactment of this section, the Secretary shall*  
22        *establish an advisory committee under section 871 on pri-*  
23        *vate sector cybersecurity, to be known as the National Cy-*  
24        *bersecurity Advisory Council (in this section referred to as*  
25        *the ‘Council’).*

1       “(b) *RESPONSIBILITIES.*—

2               “(1) *IN GENERAL.*—*The Council shall advise the*  
3       *Director of the National Center for Cybersecurity and*  
4       *Communications on the implementation of the cyber-*  
5       *security provisions affecting the private sector under*  
6       *this subtitle and subtitle E.*

7               “(2) *INCENTIVES AND REGULATIONS.*—*The*  
8       *Council shall advise the Director of the National Cen-*  
9       *ter for Cybersecurity and Communications and ap-*  
10       *propriate committees of Congress (as defined in sec-*  
11       *tion 241) and any other congressional committee with*  
12       *jurisdiction over the particular matter regarding how*  
13       *market incentives and regulations may be imple-*  
14       *mented to enhance the cybersecurity and economic se-*  
15       *curity of the Nation.*

16       “(c) *MEMBERSHIP.*—

17               “(1) *IN GENERAL.*—*The members of the Council*  
18       *shall be appointed the Director of the National Center*  
19       *for Cybersecurity and Communications and shall, to*  
20       *the extent practicable, represent a geographic and*  
21       *substantive cross-section of owners and operators of*  
22       *critical infrastructure and others with expertise in cy-*  
23       *bersecurity, including, as appropriate—*

24                       “(A) *representatives of covered critical in-*  
25       *frastructure (as defined under section 241);*

1           “(B) academic institutions with expertise in  
2 cybersecurity;

3           “(C) Federal, State, and local government  
4 agencies with expertise in cybersecurity;

5           “(D) a representative of the National Secu-  
6 rity Telecommunications Advisory Council, as  
7 established by Executive Order 12382 (47 Fed.  
8 Reg. 40531; relating to the establishment of the  
9 advisory council), as amended by Executive  
10 Order 13286 (68 Fed. Reg. 10619), as in effect  
11 on August 3, 2009, or any successor entity;

12           “(E) a representative of the Communica-  
13 tions Sector Coordinating Council, or any suc-  
14 cessor entity;

15           “(F) a representative of the Information  
16 Technology Sector Coordinating Council, or any  
17 successor entity;

18           “(G) individuals, acting in their personal  
19 capacity, with demonstrated technical expertise  
20 in cybersecurity; and

21           “(H) such other individuals as the Director  
22 determines to be appropriate, including owners  
23 of small business concerns (as defined under sec-  
24 tion 3 of the Small Business Act (15 U.S.C.  
25 632)).

1           “(2) *TERM.*—*The members of the Council shall*  
 2           *be appointed for 2 year terms and may be appointed*  
 3           *to consecutive terms.*

4           “(3) *LEADERSHIP.*—*The Chairperson and Vice-*  
 5           *Chairperson of the Council shall be selected by mem-*  
 6           *bers of the Council from among the members of the*  
 7           *Council and shall serve 2-year terms.*

8           “(d) *APPLICABILITY OF FEDERAL ADVISORY COM-*  
 9           *MITTEE ACT.*—*The Federal Advisory Committee Act (5*  
 10           *U.S.C. App.) shall not apply to the Council.”.*

11   **SEC. 502. PRIORITIZED CRITICAL INFORMATION INFRA-**  
 12                                   **STRUCTURE.**

13           (a) *IN GENERAL.*—*Section 210E(a)(2) of the Home-*  
 14           *land Security Act of 2002 (6 U.S.C. 1241(a)(2)) is amend-*  
 15           *ed—*

16                   (1) *by striking “In accordance” and inserting*  
 17           *the following:*

18                                   “(A) *IN GENERAL.*—*In accordance”;* and

19                   (2) *by adding at the end the following:*

20                                   “(B) *CONSIDERATIONS.*—*In establishing*  
 21                                   *and maintaining a list under subparagraph (A),*  
 22                                   *the Secretary, in coordination with the Director*  
 23                                   *of the National Center for Cybersecurity and*  
 24                                   *Communications, shall consider cyber risks and*  
 25                                   *consequences by sector, including—*

1                   “(i) the factors listed in section  
2                   248(a)(2);

3                   “(ii) interdependencies between compo-  
4                   nents of covered critical infrastructure (as  
5                   defined under section 241); and

6                   “(iii) the potential for the destruction  
7                   or disruption of the system or asset to  
8                   cause—

9                   “(I) a mass casualty event which  
10                  includes an extraordinary number of  
11                  fatalities;

12                  “(II) severe economic con-  
13                  sequences;

14                  “(III) mass evacuations with a  
15                  prolonged absence; or

16                  “(IV) severe degradation of na-  
17                  tional security capabilities, including  
18                  intelligence and defense functions.”.

19                  **(b) COVERED CRITICAL INFRASTRUCTURE.**—Title II of  
20 *the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)*  
21 *(as amended by section 201 of this Act)* is further amended  
22 *by adding at the end the following:*

23 **“SEC. 254. COVERED CRITICAL INFRASTRUCTURE.**

24                  **“(a) IDENTIFICATION OF COVERED CRITICAL INFRA-**  
25 **STRUCTURE.**—

1           “(1) *IN GENERAL.*—Subject to paragraphs (2)  
2           and (3), the Secretary, in coordination with sector-  
3           specific agencies and in consultation with the Na-  
4           tional Cybersecurity Advisory Council and other ap-  
5           propriate representatives of State and local govern-  
6           ments and the private sector, shall establish and  
7           maintain a list of systems or assets that constitute  
8           covered critical infrastructure for purposes of this  
9           subtitle.

10           “(2) *REQUIREMENTS.*—

11           “(A) *IN GENERAL.*—A system or asset may  
12           not be identified as covered critical infrastruc-  
13           ture under this section unless such system or  
14           asset meets each of the requirements under sub-  
15           paragraph (B)(i), (ii), and (iii).

16           “(B) *REQUIREMENTS.*—The requirements  
17           referred to under subparagraph (A) are that—

18           “(i) the destruction or the disruption of  
19           the reliable operation of the system or asset  
20           would cause national or regional cata-  
21           strophic effects identified under section  
22           210E(a)(2)(B)(iii);

23           “(ii) the system or asset is on the  
24           prioritized critical infrastructure list estab-

1           lished by the Secretary under section  
2           210E(a)(2); and

3           “(iii)(I) the system or asset is a com-  
4           ponent of the national information infra-  
5           structure; or

6           “(II) the national information infra-  
7           structure is essential to the reliable oper-  
8           ation of the system or asset.

9           “(3) *LIMITATION.*—A system or asset may not be  
10          identified as covered critical infrastructure under this  
11          section based solely on activities protected by the first  
12          amendment to the United States Constitution.

13          “(b) *NOTIFICATION.*—

14                 “(1) *IDENTIFICATION OF SYSTEM OR ASSET.*—If  
15          the Secretary identifies any system or asset as covered  
16          critical infrastructure under subsection (a), the Sec-  
17          retary shall promptly notify the owner or operator of  
18          that system or asset of that identification.

19                 “(2) *SYSTEM OR ASSET NO LONGER COVERED*  
20          *CRITICAL INFRASTRUCTURE.*—If the Secretary deter-  
21          mines that any system or asset that was identified as  
22          covered critical infrastructure under subsection (a) no  
23          longer constitutes covered critical infrastructure, the  
24          Secretary shall promptly notify the owner or operator  
25          of that system or asset of that determination.

1       “(c) *REDRESS.*—

2               “(1) *IN GENERAL.*—Subject to paragraphs (2),  
3       (3), and (4), the Secretary shall develop a mechanism,  
4       consistent with subchapter II of chapter 5 of title 5,  
5       United States Code, for an owner or operator notified  
6       under subsection (b)(1) to appeal the identification of  
7       a system or asset as covered critical infrastructure  
8       under this section.

9               “(2) *COMPLIANCE.*—The owner or operator of a  
10       system or asset identified as covered critical infra-  
11       structure shall comply with any requirement of this  
12       subtitle relating to covered critical infrastructure  
13       until such time as the system or asset is no longer  
14       identified as covered critical infrastructure by the  
15       Secretary, based on—

16                       “(A) an appeal under this subsection; or

17                       “(B) a determination of the Secretary unre-  
18       lated to an appeal.

19               “(3) *ABUSE OF DISCRETION.*—In order to pre-  
20       vail in any appeal under this subsection, the owner  
21       or operator of the system or asset identified as covered  
22       critical infrastructure shall be required to dem-  
23       onstrate an abuse of discretion by the Secretary.

1           “(4) *FINAL APPEAL.*—*A final decision in any*  
2 *appeal under this subsection shall be a final agency*  
3 *action that shall not be subject to judicial review.*

4           “(d) *ADDITION OF SYSTEMS OR ASSETS.*—

5           “(1) *IN GENERAL.*—*The Secretary shall develop*  
6 *a process under which any owner or operator of a*  
7 *system or asset that may constitute covered critical*  
8 *infrastructure may—*

9           “(A) *request that such system or asset be*  
10 *identified by the Secretary as covered critical in-*  
11 *frastructure under this section; and*

12           “(B) *submit material supporting such a re-*  
13 *quest to the Director of the Center for consider-*  
14 *ation by the Secretary in carrying out this sec-*  
15 *tion.*

16           “(2) *FINAL DECISION.*—*A decision to identify*  
17 *any system or asset as covered critical infrastructure*  
18 *based on a request submitted under this subsection—*

19           “(A) *is committed to the sole, unreviewable*  
20 *discretion of the Secretary; and*

21           “(B) *shall not be subject to—*

22           “(i) *an appeal under subsection (c); or*

23           “(ii) *judicial review.*”.

1 **SEC. 503. NATIONAL CENTER FOR CYBERSECURITY AND**  
2 **COMMUNICATIONS ACQUISITION AUTHORI-**  
3 **TIES.**

4 (a) *IN GENERAL.*—*The National Center for Cybersecu-*  
5 *rity and Communications is authorized to use the authori-*  
6 *ties under subsections (c)(1) and (d)(1)(B) of section 2304*  
7 *of title 10, United States Code, instead of the authorities*  
8 *under subsections (c)(1) and (d)(1)(B) of section 303 of the*  
9 *Federal Property and Administrative Services Act of 1949*  
10 *(41 U.S.C. 253), subject to all other requirements of section*  
11 *303 of the Federal Property and Administrative Services*  
12 *Act of 1949.*

13 (b) *GUIDELINES.*—*Not later than 90 days after the*  
14 *date of enactment of this Act, the chief procurement officer*  
15 *of the Department of Homeland Security shall issue guide-*  
16 *lines for use of the authority under subsection (a).*

17 (c) *TERMINATION.*—*The National Center for Cyberse-*  
18 *curity and Communications may not use the authority*  
19 *under subsection (a) on and after the date that is 3 years*  
20 *after the date of enactment of this Act.*

21 (d) *REPORTING.*—

22 (1) *IN GENERAL.*—*On a semiannual basis, the*  
23 *Director of the National Center for Cybersecurity and*  
24 *Communications shall submit a report on use of the*  
25 *authority granted by subsection (a) to—*

1           (A) *the Committee on Homeland Security*  
2           *and Governmental Affairs of the Senate; and*

3           (B) *the Committee on Homeland Security of*  
4           *the House of Representatives.*

5           (2) *CONTENTS.—Each report submitted under*  
6           *paragraph (1) shall include, at a minimum—*

7           (A) *the number of contract actions taken*  
8           *under the authority under subsection (a) during*  
9           *the period covered by the report; and*

10          (B) *for each contract action described in*  
11          *subparagraph (A)—*

12               (i) *the total dollar value of the contract*  
13               *action;*

14               (ii) *a summary of the market research*  
15               *conducted by the National Center for Cyber-*  
16               *security and Communications, including a*  
17               *list of all offerors who were considered and*  
18               *those who actually submitted bids, in order*  
19               *to determine that use of the authority was*  
20               *appropriate; and*

21               (iii) *a copy of the justification and ap-*  
22               *proval documents required by section 303(f)*  
23               *of the Federal Property and Administrative*  
24               *Services Act of 1949 (41 U.S.C. 253(f)).*

1           (3) *CLASSIFIED ANNEX.*—A report submitted  
2           under this subsection shall be submitted in an unclas-  
3           sified form, but may include a classified annex, if  
4           necessary.

5 **SEC. 504. EVALUATION OF THE EFFECTIVE IMPLEMENTA-**  
6                           **TION OF OFFICE OF MANAGEMENT AND**  
7                           **BUDGET INFORMATION SECURITY RELATED**  
8                           **POLICIES AND DIRECTIVES.**

9           (a) *IN GENERAL.*—The Administrator for Electronic  
10          Government and Information Technology, in coordination  
11          with the Chief Information Officers Council, the Federal In-  
12          formation Security Taskforce, and Council on Inspectors  
13          General on Integrity and Efficiency, shall evaluate agency  
14          adoption and effective implementation of appropriate infor-  
15          mation security related policies, memoranda, and directives  
16          issued by the Office of Management and Budget including—

17                 (1) *OMB Memorandum M–10–15, FY 2010 Re-*  
18                 *porting Instructions for the Federal Information Se-*  
19                 *curity Management Act and Agency Privacy Manage-*  
20                 *ment, issued April 21, 2010;*

21                 (2) *OMB Memorandum M–09–32, Update on the*  
22                 *Trusted Internet Connections Initiative, issued Sep-*  
23                 *tember 17, 2009;*

1           (3) *OMB Memorandum M-09-02, Information*  
2           *Technology Management Structure and Governance*  
3           *Framework, issued October 21, 2008;*

4           (4) *OMB Memorandum M-08-23, Securing the*  
5           *Federal Government’s Domain Name System Infra-*  
6           *structure, issued April 22, 2008;*

7           (5) *OMB Memorandum M-08-22, Guidance on*  
8           *the Federal Desktop Core Configuration (FDCC),*  
9           *issued August 11, 2008;*

10          (6) *OMB Memorandum M-07-16, Safeguarding*  
11          *Against and Responding to the Breach of Personally*  
12          *Identifiable Information, issued May 22, 2007;*

13          (7) *OMB Memorandum M-07-06, Validating*  
14          *and Monitoring Agency Issuance of Personal Identity*  
15          *Verification Credentials, issued January 11, 2007;*

16          (8) *OMB Memorandum M-04-26, Personal Use*  
17          *Policies and “File Sharing” Technology, issued Sep-*  
18          *tember 8, 2004; and*

19          (9) *OMB Memorandum M-03-22, OMB Guid-*  
20          *ance for Implementing the Privacy Provisions of the*  
21          *E-Government Act of 2002, issued September 26,*  
22          *2003.*

23          (b) *REPORT.—Not later than 1 year after the date of*  
24          *enactment of this Act, the Office of Management and Budget*  
25          *shall submit a report on the evaluation required under sub-*

1 *section (a) to the appropriate congressional committees*  
2 *which shall include—*

3           (1) *an examination of whether Federal agencies*  
4 *have effectively implemented information security*  
5 *policies;*

6           (2) *identification of and reasons why Federal*  
7 *agencies are not in compliance with information secu-*  
8 *rity policies;*

9           (3) *the extent to which contractors working on*  
10 *behalf of Federal agencies are in compliance and ef-*  
11 *fectively implementing information security policies;*  
12 *and*

13           (4) *recommended legislative and executive branch*  
14 *actions.*

15 **SEC. 505. TECHNICAL AND CONFORMING AMENDMENTS.**

16           (a) *ELIMINATION OF ASSISTANT SECRETARY FOR CY-*  
17 *BERSECURITY AND COMMUNICATIONS.—The Homeland Se-*  
18 *curity Act of 2002 (6 U.S.C. 101 et seq.) is amended—*

19           (1) *in section 103(a)(8) (6 U.S.C. 113(a)(8)), by*  
20 *striking “, cybersecurity,”;*

21           (2) *in section 514 (6 U.S.C. 321c)—*

22                   (A) *by striking subsection (b); and*

23                   (B) *by redesignating subsection (c) as sub-*  
24 *section (b); and*

1           (3) *in section 1801(b) (6 U.S.C. 571(b)), by*  
2           *striking “shall report to the Assistant Secretary for*  
3           *Cybersecurity and Communications” and inserting*  
4           *“shall report to the Director of the National Center*  
5           *for Cybersecurity and Communications”.*

6           (b) *CIO COUNCIL.—Section 3603(b) of title 44, United*  
7           *States Code, is amended—*

8           (1) *by redesignating paragraph (7) as para-*  
9           *graph (8); and*

10          (2) *by inserting after paragraph (6) the fol-*  
11          *lowing:*

12                 *“(7) The Director of the National Center for Cy-*  
13                 *bersecurity and Communications.”.*

14          (c) *REPEAL.—The Homeland Security Act of 2002 (6*  
15          *U.S.C. 101 et seq) is amended—*

16                 (1) *by striking section 223 (6 U.S.C. 143); and*

17                 (2) *by redesignating sections 224 and 225 (6*  
18                 *U.S.C. 144 and 145) as sections 223 and 224, respec-*  
19                 *tively.*

20          (d) *TECHNICAL CORRECTION.—Section 1802(a) of the*  
21          *Homeland Security Act of 2002 (6 U.S.C. 572(a)) is*  
22          *amended in the matter preceding paragraph (1) by striking*  
23          *“Department of”.*

1       (e) *EXECUTIVE SCHEDULE POSITION.*—Section 5313  
 2 of title 5, United States Code, is amended by adding at  
 3 the end the following:

4       “Director of the National Center for Cybersecurity and  
 5 Communications.”.

6       (f) *TABLE OF CONTENTS.*—The table of contents in sec-  
 7 tion 1(b) of the Homeland Security Act of 2002 (6 U.S.C.  
 8 101 et seq.) is amended—

9               (1) by striking the items relating to sections 223,  
 10       224, and 225 and inserting the following:

“Sec. 223. NET guard.

“Sec. 224. Cyber Security Enhancements Act of 2002.”; and

11               (2) by inserting after the item relating to section  
 12       237 the following:

“Sec. 238. Cybersecurity research and development.

“Sec. 239. National Cybersecurity Advisory Council.

“Subtitle E—Cybersecurity

“Sec. 241. Definitions.

“Sec. 242. National Center for Cybersecurity and Communications.

“Sec. 243. Physical and cyber infrastructure collaboration.

“Sec. 244. United States Computer Emergency Readiness Team.

“Sec. 245. Additional authorities of the Director of the National Center for Cyber-  
 security and Communications.

“Sec. 246. Information sharing.

“Sec. 247. Private sector assistance.

“Sec. 248. Cyber risks to covered critical infrastructure.

“Sec. 249. National cyber emergencies..

“Sec. 250. Enforcement.

“Sec. 251. Protection of information.

“Sec. 252. Sector-specific agencies.

“Sec. 253. Strategy for Federal cybersecurity supply chain management.

“Sec. 254. Covered critical infrastructure.”.



Calendar No. 698

111<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

**S. 3480**

[Report No. 111-368]

---

---

## **A BILL**

To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

---

---

DECEMBER 15, 2010

Reported with an amendment