

111TH CONGRESS
2^D SESSION

S. 3480

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

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,*

3 **SECTION 1. SHORT TITLE.**

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

6 **SEC. 2. TABLE OF CONTENTS.**

7 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 COMMIT-
 4 TEES.—The term “appropriate congressional com-
 5 mittees” means—

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

1 (B) the Committee on Homeland Security
2 of the House of Representatives;

3 (C) the Committee on Oversight and Gov-
4 ernment Reform of the House of Representa-
5 tives; and

6 (D) any other congressional committee
7 with 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”
13 means the interdependent network of information in-
14 frastructure, and includes the Internet, tele-
15 communications networks, computer systems, and
16 embedded processors and controllers in critical in-
17 dustries.

18 (4) DIRECTOR.—The term “Director” means
19 the Director of Cyberspace Policy established under
20 section 101.

21 (5) FEDERAL AGENCY.—The term “Federal
22 agency”—

23 (A) means any executive department, Gov-
24 ernment corporation, Government controlled
25 corporation, or other establishment in the exec-

1 utive branch of the Government (including the
2 Executive Office of the President), or any inde-
3 pendent regulatory agency; and

4 (B) does not include the governments of
5 the District of Columbia and of the territories
6 and possessions of the United States and their
7 various subdivisions.

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

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

17 (B) does not include—

18 (i) a national security system; or

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

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

- 1 (A) actually or potentially jeopardizes—
2 (i) the information security of infor-
3 mation infrastructure; or
4 (ii) the information that information
5 infrastructure processes, stores, receives,
6 or transmits; or
7 (B) constitutes a violation or threat of vio-
8 lation of security policies, security procedures,
9 or acceptable use policies applicable to informa-
10 tion infrastructure.

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

18 (9) INFORMATION SECURITY.—The term “infor-
19 mation security” means protecting information and
20 information systems from disruption or unauthorized
21 access, use, disclosure, modification, or destruction
22 in order to provide—

- 23 (A) integrity, by guarding against im-
24 proper information modification or destruction,

1 including by ensuring information nonrepudi-
2 ation and authenticity;

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

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

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

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

17 (12) KEY RESOURCES.—The term “key re-
18 sources” has the meaning given that term in section
19 2 of the Homeland Security Act of 2002 (6 U.S.C.
20 101).

21 (13) NATIONAL CENTER FOR CYBERSECURITY
22 AND COMMUNICATIONS.—The term “National Cen-
23 ter for Cybersecurity and Communications” means
24 the National Center for Cybersecurity and Commu-
25 nications established under section 242(a) of the

1 Homeland Security Act of 2002, as added by this
2 Act.

3 (14) NATIONAL INFORMATION INFRASTRUC-
4 TURE.—The term “national information infrastruc-
5 ture” means information infrastructure—

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

8 (ii) if located outside the United States,
9 the disruption of which could result in national
10 or regional catastrophic damage in the United
11 States; and

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

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

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

22 (17) OFFICE.—The term “Office” means the
23 Office of Cyberspace Policy established under section
24 101.

1 (18) RISK.—The term “risk” means the poten-
2 tial for an unwanted outcome resulting from an inci-
3 dent, as determined by the likelihood of the occur-
4 rence of the incident and the associated con-
5 sequences, including potential for an adverse out-
6 come assessed as a function of threats,
7 vulnerabilities, and consequences associated with an
8 incident.

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

13 **TITLE I—OFFICE OF** 14 **CYBERSPACE POLICY**

15 **SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBER-** 16 **SPACE POLICY.**

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

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

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

4 (B) information assurance;

5 (C) protection of critical infrastructure and
6 key resources;

7 (D) research and development priorities;

8 (E) law enforcement;

9 (F) diplomacy;

10 (G) homeland security; and

11 (H) military and intelligence activities;

12 (2) oversee, coordinate, and integrate all poli-
13 cies and activities of the Federal Government across
14 all instruments of national power relating to ensur-
15 ing the security and resiliency of cyberspace, includ-
16 ing—

17 (A) diplomatic, economic, military, intel-
18 ligence, homeland security, and law enforcement
19 policies and activities within and among Federal
20 agencies; and

21 (B) offensive activities, defensive activities,
22 and other policies and activities necessary to en-
23 sure effective capabilities to operate in cyber-
24 space;

1 (3) ensure that all Federal agencies comply
2 with appropriate guidelines, policies, and directives
3 from the Department of Homeland Security, other
4 Federal agencies with responsibilities relating to
5 cyberspace security or resiliency, and the National
6 Center for Cybersecurity and Communications; and

7 (4) ensure that Federal agencies have access to,
8 receive, and appropriately disseminate law enforce-
9 ment information, intelligence information, terrorism
10 information, and any other information (including
11 information relating to incidents provided under sub-
12 sections (a)(4) and (c) of section 246 of the Home-
13 land Security Act of 2002, as added by this Act) rel-
14 evant to—

15 (A) the security of the Federal information
16 infrastructure or the national information infra-
17 structure; and

18 (B) the security of—

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

24 (ii) a national security system.

25 (b) DIRECTOR OF CYBERSPACE POLICY.—

1 (1) IN GENERAL.—There shall be a Director of
2 Cyberspace Policy, who shall be the head of the Of-
3 fice.

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

7 “Director of Cyberspace Policy.”.

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

10 (a) APPOINTMENT.—

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

14 (2) QUALIFICATIONS.—The President shall ap-
15 point the Director from among individuals who have
16 demonstrated ability and knowledge in information
17 technology, cybersecurity, and the operations, secu-
18 rity, and resiliency of communications networks.

19 (3) PROHIBITION.—No person shall serve as
20 Director while serving in any other position in the
21 Federal Government.

22 (b) RESPONSIBILITIES.—The Director shall—

23 (1) advise the President regarding the estab-
24 lishment of policies, goals, objectives, and priorities

1 for securing the information infrastructure of the
2 Nation;

3 (2) advise the President and other entities with-
4 in the Executive Office of the President regarding
5 mechanisms to build, and improve the resiliency and
6 efficiency of, the information and communication in-
7 dustry of the Nation, in collaboration with the pri-
8 vate sector, while promoting national economic inter-
9 ests;

10 (3) work with Federal agencies to—

11 (A) oversee, coordinate, and integrate the
12 implementation of the National Strategy, in-
13 cluding coordination with—

14 (i) the Department of Homeland Se-
15 curity;

16 (ii) the Department of Defense;

17 (iii) the Department of Commerce;

18 (iv) the Department of State;

19 (v) the Department of Justice;

20 (vi) the Department of Energy;

21 (vii) through the Director of National
22 Intelligence, the intelligence community;
23 and

1 (viii) and any other Federal agency
2 with responsibilities relating to the Na-
3 tional Strategy; and

4 (B) resolve any disputes that arise between
5 Federal agencies relating to the National Strat-
6 egy or other matters within the responsibility of
7 the Office;

8 (4) if the policies or activities of a Federal
9 agency are not in compliance with the responsibil-
10 ities of the Federal agency under the National Strat-
11 egy—

12 (A) notify the Federal agency;

13 (B) transmit a copy of each notification
14 under subparagraph (A) to the President and
15 the appropriate congressional committees; and

16 (C) coordinate the efforts to bring the
17 Federal agency into compliance;

18 (5) ensure the adequacy of protections for pri-
19 vacy and civil liberties in carrying out the respon-
20 sibilities of the Director under this title, including
21 through consultation with the Privacy and Civil Lib-
22 erties Oversight Board established under section
23 1061 of the National Security Intelligence Reform
24 Act of 2004 (42 U.S.C. 2000ee);

1 (6) upon reasonable request, appear before any
2 duly constituted committees of the Senate or of the
3 House of Representatives;

4 (7) recommend to the Office of Management
5 and Budget or the head of a Federal agency actions
6 (including requests to Congress relating to the re-
7 programming of funds) that the Director determines
8 are necessary to ensure risk-based security of—

9 (A) the Federal information infrastructure;

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

15 (C) a national security system;

16 (8) advise the Administrator of the Office of E-
17 Government and Information Technology and the
18 Administrator of the Office of Information and Reg-
19 ulatory Affairs on the development, and oversee the
20 implementation, of policies, principles, standards,
21 guidelines, and budget priorities for information
22 technology functions and activities of the Federal
23 Government;

24 (9) coordinate and ensure, to the maximum ex-
25 tent practicable, that the standards and guidelines

1 developed for national security systems and the
2 standards and guidelines under section 20 of the
3 National Institute of Standards and Technology Act
4 (15 U.S.C. 278g–3) are complementary and unified;

5 (10) in consultation with the Administrator of
6 the Office of Information and Regulatory Affairs,
7 coordinate efforts of Federal agencies relating to the
8 development of regulations, rules, requirements, or
9 other actions applicable to the national information
10 infrastructure to ensure, to the maximum extent
11 practicable, that the efforts are complementary;

12 (11) coordinate the activities of the Office of
13 Science and Technology Policy, the National Eco-
14 nomic Council, the Office of Management and Budg-
15 et, the National Security Council, the Homeland Se-
16 curity Council, and the United States Trade Rep-
17 resentative related to the National Strategy and
18 other matters within the purview of the Office; and

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

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

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

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

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

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

4 “(iii) notwithstanding the exception
5 under subparagraph (A) (relating to an ap-
6 pointment made by the President, by and
7 with the advice and consent of the Senate),
8 the Director of Cyberspace Policy.”.

9 **SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET RE-**
10 **QUESTS RELATING TO THE NATIONAL STRAT-**
11 **EGY.**

12 (a) **IN GENERAL.**—For each fiscal year, the head of
13 each Federal agency shall transmit to the Director a copy
14 of any portion of the budget of the Federal agency in-
15 tended to implement the National Strategy at the same
16 time as that budget request is submitted to the Office of
17 Management and Budget in the preparation of the budget
18 of the President submitted to Congress under section
19 1105 (a) of title 31, United States Code.

20 (b) **TIMELY SUBMISSIONS.**—The head of each Fed-
21 eral agency shall ensure the timely development and sub-
22 mission to the Director of each proposed budget under this
23 section, in such format as may be designated by the Direc-
24 tor with the concurrence of the Director of the Office of
25 Management and Budget.

1 (c) ADEQUACY OF THE PROPOSED BUDGET RE-
2 QUESTS.—With the assistance of, and in coordination
3 with, the Office of E-Government and Information Tech-
4 nology and the National Center for Cybersecurity and
5 Communications, the Director shall review each budget
6 submission to assess the adequacy of the proposed request
7 with regard to implementation of the National Strategy.

8 (d) INADEQUATE BUDGET REQUESTS.—If the Direc-
9 tor concludes that a budget request submitted under sub-
10 section (a) is inadequate, in whole or in part, to implement
11 the objectives of the National Strategy, the Director shall
12 submit to the Director of the Office of Management and
13 Budget and the head of the Federal agency submitting
14 the budget request a written description of funding levels
15 and specific initiatives that would, in the determination
16 of the Director, make the request adequate.

17 **SEC. 105. ACCESS TO INTELLIGENCE.**

18 The Director shall have access to law enforcement in-
19 formation, intelligence information, terrorism information,
20 and any other information (including information relating
21 to incidents provided under subsections (a)(4) and (c) of
22 section 246 of the Homeland Security Act of 2002, as
23 added by this Act) that is obtained by, or in the possession
24 of, any Federal agency that the Director determines rel-
25 evant to the security of—

- 1 (1) the Federal information infrastructure;
- 2 (2) information infrastructure that is owned,
3 operated, controlled, or licensed for use by, or on be-
4 half of, the Department of Defense, a military de-
5 partment, or another element of the intelligence
6 community;
- 7 (3) a national security system; or
- 8 (4) national information infrastructure.

9 **SEC. 106. CONSULTATION.**

10 (a) IN GENERAL.—The Director may consult and ob-
11 tain recommendations from, as needed, such Presidential
12 and other advisory entities as the Director determines will
13 assist in carrying out the mission of the Office, includ-
14 ing—

- 15 (1) the National Security Telecommunications
16 Advisory Committee;
- 17 (2) the National Infrastructure Advisory Coun-
18 cil;
- 19 (3) the Privacy and Civil Liberties Oversight
20 Board;
- 21 (4) the President’s Intelligence Advisory Board;
- 22 (5) the Critical Infrastructure Partnership Ad-
23 visory Council; and

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

4 (b) NATIONAL STRATEGY.—In developing and updat-
5 ing the National Strategy the Director shall consult with
6 the National Cybersecurity Advisory Council and, as ap-
7 propriate, State and local governments and private enti-
8 ties.

9 **SEC. 107. REPORTS TO CONGRESS.**

10 (a) IN GENERAL.—The Director shall submit an an-
11 nual report to the appropriate congressional committees
12 describing the activities, ongoing projects, and plans of the
13 Federal Government designed to meet the goals and objec-
14 tives of the National Strategy.

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

18 (c) PUBLIC REPORT.—An unclassified version of
19 each report submitted under this section shall be made
20 available to the public.

1 **TITLE II—NATIONAL CENTER**
2 **FOR CYBERSECURITY AND**
3 **COMMUNICATIONS**

4 **SEC. 201. CYBERSECURITY.**

5 Title II of the Homeland Security Act of 2002 (6
6 U.S.C. 121 et seq.) is amended by adding at the end the
7 following:

8 **“Subtitle E—Cybersecurity**

9 **“SEC. 241. DEFINITIONS.**

10 “In this subtitle—

11 “(1) the term ‘agency information infrastruc-
12 ture’ means the Federal information infrastructure
13 of a particular Federal agency;

14 “(2) the term ‘appropriate committees of Con-
15 gress’ means the Committee on Homeland Security
16 and Governmental Affairs of the Senate and the
17 Committee on Homeland Security of the House of
18 Representatives;

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

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

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

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

6 “(ii) for which the national information in-
7 frastructure is essential to the reliable operation
8 of the system or asset;

9 “(5) the term ‘cyber vulnerability’ means any
10 security vulnerability that, if exploited, could pose a
11 significant risk of disruption to the operation of in-
12 formation infrastructure essential to the reliable op-
13 eration of covered critical infrastructure;

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

16 “(7) the term ‘Federal agency’—

17 “(A) means any executive department,
18 military department, Government corporation,
19 Government controlled corporation, or other es-
20 tablishment in the executive branch of the Gov-
21 ernment (including the Executive Office of the
22 President), or any independent regulatory agen-
23 cy; and

24 “(B) does not include the governments of
25 the District of Columbia and of the territories

1 and possessions of the United States and their
2 various subdivisions;

3 “(8) the term ‘Federal information infrastruc-
4 ture’—

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

11 “(B) does not include—

12 “(i) a national security system; or

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

18 “(9) the term ‘incident’ means an occurrence
19 that—

20 “(A) actually or potentially jeopardizes—

21 “(i) the information security of infor-
22 mation infrastructure; or

23 “(ii) the information that information
24 infrastructure processes, stores, receives,
25 or transmits; or

1 “(B) constitutes a violation or threat of
2 violation of security policies, security proce-
3 dures, or acceptable use policies applicable to
4 information infrastructure.

5 “(10) the term ‘information infrastructure’
6 means the underlying framework that information
7 systems and assets rely on to process, transmit, re-
8 ceive, or store information electronically, including—

9 “(A) programmable electronic devices and
10 communications networks; and

11 “(B) any associated hardware, software, or
12 data;

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

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

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

18 “(15) the term ‘management controls’ means
19 safeguards or countermeasures for an information
20 system that focus on the management of risk and
21 the management of information system security;

22 “(16) the term ‘National Cybersecurity Advi-
23 sory Council’ means the National Cybersecurity Ad-
24 visory Council established under section 239;

1 “(17) the term ‘national cyber emergency’
2 means an actual or imminent action by any indi-
3 vidual or entity to exploit a cyber vulnerability in a
4 manner that disrupts, attempts to disrupt, or poses
5 a significant risk of disruption to the operation of
6 the information infrastructure essential to the reli-
7 able operation of covered critical infrastructure;

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

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

12 “(ii) if located outside the United States,
13 the disruption of which could result in national
14 or regional catastrophic damage in the United
15 States; and

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

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

21 “(20) the term ‘operational controls’ means the
22 safeguards and countermeasures for an information
23 system that are primarily implemented and executed
24 by individuals not systems;

1 “(21) the term ‘sector-specific agency’ means
2 the relevant Federal agency responsible for infra-
3 structure protection activities in a designated critical
4 infrastructure sector or key resources category under
5 the National Infrastructure Protection Plan, or any
6 other appropriate Federal agency identified by the
7 President after the date of enactment of this sub-
8 title;

9 “(22) the term ‘sector coordinating councils’
10 means self-governed councils that are composed of
11 representatives of key stakeholders within a specific
12 sector of critical infrastructure that serve as the
13 principal private sector policy coordination and plan-
14 ning entities with the Federal Government relating
15 to the security and resiliency of the critical infra-
16 structure that comprise that sector;

17 “(23) the term ‘security controls’ means the
18 management, operational, and technical controls pre-
19 scribed for an information system to protect the in-
20 formation security of the system;

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

24 “(25) the term ‘technical controls’ means the
25 safeguards or countermeasures for an information

1 system that are primarily implemented and executed
2 by the information system through mechanisms con-
3 tained in the hardware, software, or firmware com-
4 ponents of the system;

5 “(26) the term ‘terrorism information’ has the
6 meaning given that term in section 1016 of the In-
7 telligence Reform and Terrorism Prevention Act of
8 2004 (6 U.S.C. 485);

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

13 “(28) the term ‘US–CERT’ means the United
14 States Computer Readiness Team established under
15 section 244.

16 **“SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND**
17 **COMMUNICATIONS.**

18 “(a) ESTABLISHMENT.—

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

22 “(2) OPERATIONAL ENTITY.—The Center
23 may—

1 “(A) enter into contracts for the procure-
2 ment of property and services for the Center;
3 and

4 “(B) appoint employees of the Center in
5 accordance with the civil service laws of the
6 United States.

7 “(b) DIRECTOR.—

8 “(1) IN GENERAL.—The Center shall be headed
9 by a Director, who shall be appointed by the Presi-
10 dent, by and with the advice and consent of the Sen-
11 ate.

12 “(2) REPORTING TO SECRETARY.—The Direc-
13 tor shall report directly to the Secretary and serve
14 as the principal advisor to the Secretary on cyberse-
15 curity and the operations, security, and resiliency of
16 the communications infrastructure of the United
17 States.

18 “(3) PRESIDENTIAL ADVICE.—The Director
19 shall regularly advise the President on the exercise
20 of the authorities provided under this subtitle or any
21 other provision of law relating to the security of the
22 Federal information infrastructure or an agency in-
23 formation infrastructure.

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

1 “(A) a demonstrated ability in and knowl-
2 edge of information technology, cybersecurity,
3 and the operations, security and resiliency of
4 communications networks; and

5 “(B) significant executive leadership and
6 management experience in the public or private
7 sector.

8 “(5) LIMITATION ON SERVICE.—

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

15 “(B) EXCEPTION.—The Director may
16 serve on any commission, board, council, or
17 similar entity with responsibilities or duties re-
18 lating to cybersecurity or the operations, secu-
19 rity, and resiliency of the communications infra-
20 structure of the United States at the direction
21 of the President or as otherwise provided by
22 law.

23 “(c) DEPUTY DIRECTORS.—

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

4 “(2) INFRASTRUCTURE PROTECTION.—

5 “(A) APPOINTMENT.—There shall be a
6 Deputy Director appointed by the Secretary,
7 who shall have expertise in infrastructure pro-
8 tection.

9 “(B) RESPONSIBILITIES.—The Deputy Di-
10 rector appointed under subparagraph (A)
11 shall—

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

23 “(ii) review the budget for the Center
24 and the Office of Infrastructure Protection
25 before submission of the budget to the Sec-

1 retary to ensure that activities are appro-
2 priately coordinated;

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

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

18 “(v) perform such other duties as the
19 Director may assign.

20 “(C) ANNUAL EVALUATION.—The Assist-
21 ant Secretary for Infrastructure Protection
22 shall submit annually to the Director an evalua-
23 tion of the performance of the Deputy Director
24 appointed under subparagraph (A).

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

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

21 “(e) PRIVACY OFFICER.—

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

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

6 “(f) DUTIES OF DIRECTOR.—

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

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

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

18 “(C) provide dynamic, comprehensive, and
19 continuous situational awareness of the security
20 status of the Federal information infrastruc-
21 ture, national information infrastructure, and
22 information infrastructure that is owned, oper-
23 ated, controlled, or licensed for use by, or on
24 behalf of, the Department of Defense, a mili-
25 tary department, or another element of the in-

1 intelligence community by sharing and inte-
2 grating classified and unclassified information,
3 including information relating to threats,
4 vulnerabilities, traffic, trends, incidents, and
5 other anomalous activities affecting the infra-
6 structure or systems, on a routine and contin-
7 uous basis with—

8 “(i) the National Threat Operations
9 Center of the National Security Agency;

10 “(ii) the United States Cyber Com-
11 mand, including the Joint Task Force-
12 Global Network Operations;

13 “(iii) the Cyber Crime Center of the
14 Department of Defense;

15 “(iv) the National Cyber Investigative
16 Joint Task Force;

17 “(v) the Intelligence Community Inci-
18 dent Response Center;

19 “(vi) any other Federal agency, or
20 component thereof, identified by the Direc-
21 tor; and

22 “(vii) any non-Federal entity, includ-
23 ing, where appropriate, information shar-
24 ing and analysis centers, identified by the
25 Director, with the concurrence of the

1 owner or operator of that entity and con-
2 sistent with applicable law;

3 “(D) work with the entities described in
4 subparagraph (C) to establish policies and pro-
5 cedures that enable information sharing be-
6 tween and among the entities;

7 “(E) develop, in coordination with the As-
8 sistant 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 “(F) conduct risk-based assessments of the
17 Federal information infrastructure with respect
18 to acts of terrorism, natural disasters, and
19 other large-scale disruptions and provide the re-
20 sults of the assessments to the Director of
21 Cyberspace Policy;

22 “(G) develop, oversee the implementation
23 of, and enforce policies, principles, and guide-
24 lines on information security for the Federal in-
25 formation infrastructure, including timely adop-

1 tion of and compliance with standards devel-
2 oped by the National Institute of Standards
3 and Technology under section 20 of the Na-
4 tional Institute of Standards and Technology
5 Act (15 U.S.C. 278g-3);

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

11 “(I) provide to Federal agencies manda-
12 tory security controls to mitigate and remediate
13 vulnerabilities of and incidents affecting the
14 Federal information infrastructure;

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

21 “(K) in accordance with section 253, de-
22 velop, periodically update, and implement a
23 supply chain risk management strategy to en-
24 hance, in a risk-based and cost-effective man-
25 ner, the security of the communications and in-

1 formation technology products and services pur-
2 chased by the Federal Government;

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

13 “(M) consult, in coordination with the Di-
14 rector of Cyberspace Policy, with appropriate
15 international partners to enhance the security
16 of the Federal information infrastructure and
17 national information infrastructure;

18 “(N)(i) coordinate and integrate informa-
19 tion to analyze the composite security state of
20 the Federal information infrastructure and in-
21 formation infrastructure that is owned, oper-
22 ated, controlled, or licensed for use by, or on
23 behalf of, the Department of Defense, a mili-
24 tary department, or another element of the in-
25 telligence community;

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

14 “(iii) in conjunction with the quadrennial
15 homeland security review required under section
16 707, and at such other times determined appro-
17 priate by the Director, analyze the composite
18 security state of the national information infra-
19 structure and submit to the President, Con-
20 gress, and the Secretary a report regarding ac-
21 tions necessary to enhance the composite secu-
22 rity state of the national information infrastruc-
23 ture based on the analysis; and

24 “(iv) foster collaboration and serve as the
25 primary contact between the Federal Govern-

1 ment, State and local governments, and private
2 entities on matters relating to the security of
3 the Federal information infrastructure and the
4 national information infrastructure;

5 “(O) oversee the development, implementa-
6 tion, and management of security requirements
7 for Federal agencies relating to the external ac-
8 cess points to or from the Federal information
9 infrastructure;

10 “(P) establish, develop, and oversee the ca-
11 pabilities and operations within the US-CERT
12 as required by section 244;

13 “(Q) oversee the operations of the National
14 Communications System, as described in Execu-
15 tive Order 12472 (49 Fed. Reg. 13471; relating
16 to the assignment of national security and
17 emergency preparedness telecommunications
18 functions), as amended by Executive Order
19 13286 (68 Fed. Reg. 10619) and Executive
20 Order 13407 (71 Fed. Reg. 36975), or any suc-
21 cessor thereto, including planning for and pro-
22 viding communications for the Federal Govern-
23 ment under all circumstances, including crises,
24 emergencies, attacks, recoveries, and reconstitu-
25 tions;

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

10 “(S) subject to the availability of re-
11 sources, and at the discretion of the Director,
12 provide voluntary technical assistance—

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

21 “(ii) at the request of the owner or
22 operator of national information infra-
23 structure that is not covered critical infra-
24 structure, and based on risk, to assist the
25 owner or operator in implementing best

1 practices, and related standards and guide-
2 lines, recommended under section 247 and
3 other measures necessary to mitigate or re-
4 mediate vulnerabilities of the information
5 infrastructure and the consequences of ef-
6 forts to exploit the vulnerabilities;

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

19 “(ii) coordinate and evaluate the mitigation
20 or remediation of cyber vulnerabilities and con-
21 sequences identified under clause (i);

22 “(U) regularly evaluate and assess tech-
23 nologies designed to enhance the protection of
24 the Federal information infrastructure and na-
25 tional information infrastructure, including an

1 assessment of the cost-effectiveness of the tech-
2 nologies;

3 “(V) promote the use of the best practices
4 recommended under section 247 to State and
5 local governments and the private sector;

6 “(W) develop and implement outreach and
7 awareness programs on cybersecurity, includ-
8 ing—

9 “(i) a public education campaign to
10 increase the awareness of cybersecurity,
11 cyber safety, and cyber ethics, which shall
12 include use of the Internet, social media,
13 entertainment, and other media to reach
14 the public;

15 “(ii) an education campaign to in-
16 crease the understanding of State and local
17 governments and private sector entities of
18 the costs of failing to ensure effective secu-
19 rity of information infrastructure and cost-
20 effective methods to mitigate and reme-
21 diate vulnerabilities; and

22 “(iii) outcome-based performance
23 measures to determine the success of the
24 programs;

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

3 “(i) the participation of State and
4 local governments, international partners
5 of the United States, and the private sec-
6 tor; and

7 “(ii) an after action report analyzing
8 lessons learned from exercises and identi-
9 fying vulnerabilities to be remediated or
10 mitigated;

11 “(Y) coordinate with the Assistant Sec-
12 retary for Infrastructure Protection to ensure
13 that—

14 “(i) cybersecurity is appropriately ad-
15 dressed in carrying out the infrastructure
16 protection responsibilities described in sec-
17 tion 201(d); and

18 “(ii) the operations of the Center and
19 the Office of Infrastructure Protection
20 avoid duplication and use, to the maximum
21 extent practicable, joint mechanisms for in-
22 formation sharing and coordination with
23 the private sector;

1 “(Z) oversee the activities of the Office of
2 Emergency Communications established under
3 section 1801; and

4 “(AA) perform such other duties as the
5 Secretary may direct relating to the security
6 and resiliency of the information and commu-
7 nications infrastructure of the United States.

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

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

17 “(B) may make recommendations to the
18 Director of the Office of Management and
19 Budget and the Director of Cyberspace Policy
20 regarding the budget for each Federal agency
21 to ensure that adequate funding is devoted to
22 securing the Federal information infrastructure,
23 in accordance with policies, principles, and
24 guidelines established by the Director under
25 this subtitle; and

1 “(C) shall provide copies of any rec-
2 ommendations made under subparagraph (B)
3 to—

4 “(i) the Committee on Appropriations
5 of the Senate;

6 “(ii) the Committee on Appropriations
7 of the House of Representatives; and

8 “(iii) the appropriate committees of
9 Congress.

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

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

19 “(h) SUFFICIENCY OF RESOURCES PLAN.—

20 “(1) REPORT.—Not later than 120 days after
21 the date of enactment of this subtitle, the Director
22 of the Office of Management and Budget shall sub-
23 mit to the appropriate committees of Congress and
24 the Comptroller General of the United States a re-

1 port on the resources and staff necessary to carry
2 out fully the responsibilities under this subtitle.

3 “(2) COMPTROLLER GENERAL REVIEW.—

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

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

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

21 **“SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COL-**
22 **LABORATION.**

23 “(a) IN GENERAL.—The Director and the Assistant
24 Secretary for Infrastructure Protection shall coordinate
25 the information, communications, and physical infrastruc-

1 ture protection responsibilities and activities of the Center
2 and the Office of Infrastructure Protection.

3 “(b) OVERSIGHT.—The Secretary shall ensure that
4 the coordination described in subsection (a) occurs.

5 **“SEC. 244. UNITED STATES COMPUTER EMERGENCY READI-**
6 **NESS TEAM.**

7 “(a) ESTABLISHMENT OF OFFICE.—There is estab-
8 lished within the Center, the United States Computer
9 Emergency Readiness Team, which shall be headed by a
10 Director, who shall be selected from the Senior Executive
11 Service by the Secretary.

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

13 “(1) collect, coordinate, and disseminate infor-
14 mation on—

15 “(A) risks to the Federal information in-
16 frastructure, 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
20 the intelligence community, or the national in-
21 formation infrastructure; and

22 “(B) security controls to enhance the secu-
23 rity of the Federal information infrastructure
24 or the national information infrastructure

1 against the risks identified in subparagraph
2 (A); and

3 “(2) establish a mechanism for engagement
4 with 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 in-
11 formation infrastructure;

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

20 “(C) warn Federal agencies of threats,
21 vulnerabilities, incidents, and anomalous activi-
22 ties that could affect the Federal information
23 infrastructure;

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
16 owners or operators of national information in-
17 frastructure regarding, threats, vulnerabilities,
18 and incidents, affecting the national informa-
19 tion infrastructure, including providing—

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

23 “(ii) recommended security controls to
24 mitigate or remediate vulnerabilities; and

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

5 “(i) isolate, mitigate, or remediate in-
6 cidents;

7 “(ii) recover from damages and miti-
8 gate or remediate vulnerabilities; and

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

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

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

23 “(A) in conjunction with the Inspector
24 General of the Department, conduct an inde-

1 pendent audit or review of the activities of the
2 US–CERT under paragraph (1)(B); and

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

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

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

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

20 “(1) maintain communication;

21 “(2) ensure cooperative engagement and infor-
22 mation sharing; and

23 “(3) respond to inquiries or requests.

24 “(g) REQUESTS FOR INFORMATION OR PHYSICAL AC-
25 CESS.—

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

13 “(2) PHYSICAL ACCESS.—Upon request of the
14 Director, and in consultation with the head of a
15 Federal agency, the Federal agency shall provide
16 physical access to any facility of the Federal agency
17 necessary to determine whether the Federal agency
18 is in compliance with any policies, principles, and
19 guidelines established by the Director under this
20 subtitle, or otherwise necessary to carry out the du-
21 ties, responsibilities, and authorities of the Director
22 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 (c) 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 “(c) 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 sements 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 (c)(1); or

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

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

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

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

12 “(II) security measures which the Di-
13 rector has approved under subsection
14 (c)(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 (c)(1); or

1 “(II) security measures which the Di-
2 rector has approved under subsection
3 (c)(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 (c)(1) or for which the Director has approved secu-
11 rity measures under subsection (c)(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 (c)(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 (c)(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 (c)(1);

18 “(C) the covered entity is in compliance
19 with the emergency measures required under
20 subsection (c)(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 (c)(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 (c)(1).

12 “(5) CERTAIN ACTIONS NOT SUBJECT TO LIM-
13 ITATIONS 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 (c)(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 “(e) 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 “(c) 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(c) and
15 3556(c);

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 (c)(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 cluded 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(c);

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 “(c) 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 “(c) 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 “(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
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.

1 “(b) EXISTING ASSESSMENTS.—The assessments re-
 2 quired by this section may be based in whole or in part
 3 on an audit, evaluation, or report relating to programs or
 4 practices of the applicable agency.

5 “(c) INSPECTORS GENERAL REPORTING.—Inspectors
 6 General shall ensure information obtained as a result of
 7 the assessment required under this section, or any other
 8 relevant information, is available through the system re-
 9 quired under section 3552(a)(3)(D) to Congress and the
 10 National Center for Cybersecurity and Communications.

11 **“§ 3557. Protection of Information**

12 “In complying with this subchapter, agencies, eval-
 13 uators, and Inspectors General shall take appropriate ac-
 14 tions to ensure the protection of information which, if dis-
 15 closed, may adversely affect information security. Protec-
 16 tions under this chapter shall be commensurate with the
 17 risk and comply with all applicable laws and regulations.”.

18 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

19 (1) TABLE OF SECTIONS.—The table of sections
 20 for chapter 35 of title 44, United States Code, is
 21 amended by striking the matter relating to sub-
 22 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.”.

1 (2) OTHER REFERENCES.—

2 (A) Section 1001(c)(1)(A) of the Home-
3 land Security Act of 2002 (6 U.S.C.
4 511(c)(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(c)(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 sserting “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 (c) 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(c) 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 (c) 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 (c) 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 (c)(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 (c)(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 “(c) 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 imbursable 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 ERTIES 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 “(c) 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. 124l(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 (c)(1) and (d)(1)(B) of section
13 2304 of title 10, United States Code, instead of the au-
14 thorities under subsections (c)(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. 321c)—

19 (A) by striking subsection (b); and

20 (B) by redesignating subsection (c) 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.”.

○