

112TH CONGRESS
1ST SESSION

S. 413

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

FEBRUARY 17, 2011

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 “Cybersecurity and
5 Internet Freedom Act of 2011”.

6 **SEC. 2. INTERNET FREEDOM ACT.**

7 (a) SHORT TITLE.—This section may be cited as the
8 “Internet Freedom Act”.

9 (b) FINDINGS.—Congress finds that—

1 (1) the Internet is vital to almost every facet of
2 the daily lives of the people of the United States,
3 from the water we drink to the power we use to the
4 ways we communicate;

5 (2) in the modern world, the Internet is essen-
6 tial to the free flow of ideas and information;

7 (3) it is vital that the Internet, and the access
8 of the people of the United States to the Internet,
9 be protected to ensure the reliability of the critical
10 services that rely upon this network and the avail-
11 ability of the information and communications that
12 travel over this network;

13 (4) the Internet has developed into a robust
14 network within the United States, with thousands of
15 providers, making it technically impossible to shut
16 down the Internet;

17 (5) although the United States must ensure the
18 security of the Nation and its critical infrastructure,
19 the actions of the Government must not encroach on
20 rights guaranteed by the First Amendment to the
21 Constitution of the United States;

22 (6) cyber attacks are a real and evolving threat
23 to the information infrastructure and economy of the
24 Nation;

1 (7) the Sergeant at Arms of the Senate re-
2 ported in March 2010 that the computer systems of
3 executive branch agencies of the Federal Govern-
4 ment and Congress are probed or attacked an aver-
5 age of 1,800,000,000 times per month;

6 (8) experts estimate that cyber attacks can
7 produce \$8,000,000,000 in annual losses to the na-
8 tional economy;

9 (9) in the event of a cyber attack, it is essential
10 that the law clearly and unambiguously delineate
11 limits on what the Federal Government can and can-
12 not do to protect the information infrastructure that
13 is essential to the reliable operation of the Internet
14 and the critical infrastructure of the Nation; and

15 (10) neither the President, the Director of the
16 National Center for Cybersecurity and Communica-
17 tions, nor any other officer or employee of the Fed-
18 eral Government should have the authority to shut
19 down the Internet.

20 (c) LIMITATION.—Notwithstanding any provision of
21 this Act, an amendment made by this Act, or section 706
22 of the Communications Act of 1934 (47 U.S.C. 606), nei-
23 ther the President, the Director of the National Center
24 for Cybersecurity and Communications, or any officer or

- 1 employee of the United States Government shall have the
- 2 authority to shut down the Internet.

3 **SEC. 3. TABLE OF CONTENTS.**

- 4 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Internet Freedom Act.
- Sec. 3. Table of contents.
- Sec. 4. Definitions.

TITLE I—OFFICE OF CYBERSPACE POLICY

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

TITLE II—NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS

- Sec. 201. Cybersecurity.

TITLE III—FEDERAL INFORMATION SECURITY MANAGEMENT

- Sec. 301. Coordination of Federal information policy.

TITLE IV—RECRUITMENT AND PROFESSIONAL DEVELOPMENT

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

TITLE V—OTHER PROVISIONS

- Sec. 501. Cybersecurity research and development.
- Sec. 502. Prioritized critical information infrastructure.
- Sec. 503. National Center for Cybersecurity and Communications acquisition authorities.
- Sec. 504. Evaluation of the effective implementation of Office of Management and Budget information security related policies and directives.
- Sec. 505. Technical and conforming amendments.

1 **SEC. 4. 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;

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

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

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

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

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

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

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

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

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

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

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

25 (B) does not include—

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

7 (7) INCIDENT.—The term “incident” has the
8 meaning given that term in section 3551 of title 44,
9 United States Code, as added by this Act.

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

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

22 (A) integrity, by guarding against im-
23 proper information modification or destruction,
24 including by ensuring information nonrepudi-
25 ation and authenticity;

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

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

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

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

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

19 (13) NATIONAL CENTER FOR CYBERSECURITY
20 AND COMMUNICATIONS.—The term “National Cen-
21 ter for Cybersecurity and Communications” means
22 the National Center for Cybersecurity and Commu-
23 nications established under section 242(a) of the
24 Homeland Security Act of 2002, as added by this
25 Act.

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

4 (A) that is owned, operated, or controlled
5 within or from the United States; and

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

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

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

16 (17) OFFICE.—The term “Office” means the
17 Office of Cyberspace Policy established under section
18 101.

19 (18) RESILIENCY.—The term “resiliency”
20 means the ability to eliminate or reduce the mag-
21 nitude or duration of a disruptive event, including
22 the ability to prevent, prepare for, respond to, and
23 recover from the event.

24 (19) RISK.—The term “risk” means the poten-
25 tial for an unwanted outcome resulting from an inci-

1 dent, as determined by the likelihood of the occur-
 2 rence of the incident and the associated con-
 3 sequences, including potential for an adverse out-
 4 come assessed as a function of threats,
 5 vulnerabilities, and consequences associated with an
 6 incident.

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

11 **TITLE I—OFFICE OF** 12 **CYBERSPACE POLICY**

13 **SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBER-** 14 **SPACE POLICY.**

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

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

11 (H) protection of privacy and civil liberties;

12 (I) military and intelligence activities; and

13 (J) identity management and authentica-
14 tion;

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

20 (A) diplomatic, economic, military, intel-
21 ligence, homeland security, and law enforcement
22 policies and activities within and among Federal
23 agencies; and

24 (B) offensive activities, defensive activities,
25 and other policies and activities necessary to en-

1 sure effective capabilities to operate in cyber-
2 space;

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

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

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

20 (B) the security of—

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

1 (ii) a national security system.

2 (b) DIRECTOR OF CYBERSPACE POLICY.—

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

6 (2) EXECUTIVE SCHEDULE POSITION.—Section
7 5312 of title 5, United States Code, is amended by
8 adding at the end the following:

9 “Director of Cyberspace Policy.”.

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

12 (a) APPOINTMENT.—

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

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

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

24 (b) RESPONSIBILITIES.—The Director shall—

1 (1) advise the President regarding the estab-
2 lishment of policies, goals, objectives, and priorities
3 for securing the information infrastructure of the
4 Nation;

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

12 (3) work with Federal agencies to—

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

16 (i) the Department of Homeland Se-
17 curity;

18 (ii) the Department of Defense;

19 (iii) the Department of Commerce;

20 (iv) the Department of State;

21 (v) the Department of Justice;

22 (vi) the Department of Energy;

23 (vii) through the Director of National
24 Intelligence, the intelligence community;
25 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;

19 (12) carry out the responsibilities for national
20 security and emergency preparedness communica-
21 tions described in section 706 of the Communica-
22 tions Act of 1934 (47 U.S.C. 606) to ensure integra-
23 tion and coordination; and

24 (13) as assigned by the President, other duties
25 relating to the security and resiliency of cyberspace.

1 (c) CONFORMING REGULATIONS AND ORDERS.—The
 2 President shall amend the regulations and orders issued
 3 under section 706 of the Communications Act of 1934 (47
 4 U.S.C. 606) in accordance with subsection (b)(12).

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

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

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

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

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

12 “(iii) notwithstanding the exception
 13 under subparagraph (A) (relating to an ap-
 14 pointment made by the President, by and
 15 with the advice and consent of the Senate),
 16 the Director of Cyberspace Policy.”.

17 **SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET RE-**
 18 **QUESTS RELATING TO THE NATIONAL STRAT-**
 19 **EGY.**

20 (a) IN GENERAL.—For each fiscal year, the head of
 21 each Federal agency shall transmit to the Director a copy
 22 of any portion of the budget of the Federal agency in-
 23 tended to implement the National Strategy at the same
 24 time as that budget request is submitted to the Office of
 25 Management and Budget in the preparation of the budget

1 of the President submitted to Congress under section
2 1105(a) of title 31, United States Code.

3 (b) **TIMELY SUBMISSIONS.**—The head of each Fed-
4 eral agency shall ensure the timely development and sub-
5 mission to the Director of each proposed budget under this
6 section, in such format as may be designated by the Direc-
7 tor with the concurrence of the Director of the Office of
8 Management and Budget.

9 (c) **ADEQUACY OF THE PROPOSED BUDGET RE-**
10 **QUESTS.**—With the assistance of, and in coordination
11 with, the Office of E-Government and Information Tech-
12 nology and the National Center for Cybersecurity and
13 Communications, the Director shall review each budget
14 submission to assess the adequacy of the proposed request
15 with regard to implementation of the National Strategy,
16 including the overall sufficiency of the requests to imple-
17 ment effectively the National Strategy across all Federal
18 agencies.

19 (d) **INADEQUATE BUDGET REQUESTS.**—If the Direc-
20 tor concludes that a budget request submitted under sub-
21 section (a) is inadequate, in whole or in part, to implement
22 the objectives of the National Strategy, the Director shall
23 submit to the Director of the Office of Management and
24 Budget and the head of the Federal agency submitting
25 the budget request a written description of funding levels

1 and specific initiatives that would, in the determination
2 of the Director, make the request adequate.

3 **SEC. 105. ACCESS TO INTELLIGENCE.**

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

12 (1) the Federal information infrastructure;

13 (2) information infrastructure that is owned,
14 operated, controlled, or licensed for use by, or on be-
15 half of, the Department of Defense, a military de-
16 partment, or another element of the intelligence
17 community;

18 (3) a national security system; or

19 (4) national information infrastructure.

20 **SEC. 106. CONSULTATION.**

21 (a) IN GENERAL.—The Director may consult and ob-
22 tain recommendations from, as needed, such Presidential
23 and other advisory entities as the Director determines will
24 assist in carrying out the mission of the Office, includ-
25 ing—

1 (1) the National Security Telecommunications
2 Advisory Committee;

3 (2) the National Infrastructure Advisory Coun-
4 cil;

5 (3) the Privacy and Civil Liberties Oversight
6 Board;

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

8 (5) the Critical Infrastructure Partnership Ad-
9 visory Council;

10 (6) the Committee on Foreign Investment in
11 the United States;

12 (7) the Information Security and Privacy Advi-
13 sory Board;

14 (8) the National Cybersecurity Advisory Council
15 established under section 239 of the Homeland Se-
16 curity Act of 2002, as added by this Act; and

17 (9) any other entity that may provide assistance
18 to the Director.

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

1 **SEC. 107. REPORTS TO CONGRESS.**

2 (a) IN GENERAL.—The Director shall submit an an-
 3 nual report to the appropriate congressional committees
 4 describing the activities, ongoing projects, and plans of the
 5 Federal Government designed to meet the goals and objec-
 6 tives of the National Strategy.

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

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

13 **TITLE II—NATIONAL CENTER**
 14 **FOR CYBERSECURITY AND**
 15 **COMMUNICATIONS**

16 **SEC. 201. CYBERSECURITY.**

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

20 **“Subtitle E—Cybersecurity**

21 **“SEC. 241. DEFINITIONS.**

22 “In this subtitle—

23 “(1) the term ‘agency information infrastruc-
 24 ture’ means the Federal information infrastructure
 25 of a particular Federal agency;

1 “(2) the term ‘appropriate committees of Con-
2 gress’ means the Committee on Homeland Security
3 and Governmental Affairs of the Senate and the
4 Committee on Homeland Security of the House of
5 Representatives;

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

9 “(4) the term ‘covered critical infrastructure’
10 means a system or asset identified by the Secretary
11 as covered critical infrastructure under section 254;

12 “(5) the term ‘cyber risk’ means any risk to in-
13 formation infrastructure, including physical or per-
14 sonnel risks and security vulnerabilities, that, if ex-
15 ploited or not mitigated, could pose a significant risk
16 of disruption to the operation of information infra-
17 structure essential to the reliable operation of cov-
18 ered critical infrastructure;

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

21 “(7) the term ‘Federal agency’—

22 “(A) means any executive department,
23 military department, Government corporation,
24 Government controlled corporation, or other es-
25 tablishment in the executive branch of the Gov-

1 ernment (including the Executive Office of the
2 President), or any independent regulatory agen-
3 cy; 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 “(8) the term ‘Federal 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, any Federal agency,
13 including information systems used or operated
14 by another entity on behalf of a Federal agency;
15 and

16 “(B) does not include—

17 “(i) a national security system; or

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

23 “(9) the term ‘incident’ has the meaning given
24 that term in section 3551 of title 44, United States
25 Code;

1 “(10) the term ‘information infrastructure’
2 means the underlying framework that information
3 systems and assets rely on to process, transmit, re-
4 ceive, or store information electronically, including—

5 “(A) programmable electronic devices and
6 communications networks; and

7 “(B) any associated hardware, software, or
8 data;

9 “(11) the term ‘information security’ means
10 protecting information and information systems
11 from disruption or unauthorized access, use, disclo-
12 sure, modification, or destruction in order to pro-
13 vide—

14 “(A) integrity, by guarding against im-
15 proper information modification or destruction,
16 including by ensuring information nonrepudi-
17 ation and authenticity;

18 “(B) confidentiality, by preserving author-
19 ized restrictions on access and disclosure, in-
20 cluding means for protecting personal privacy
21 and proprietary information; and

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

24 “(12) the term ‘information sharing and anal-
25 ysis center’ means a self-governed forum whose

1 members work together within a specific sector of
2 critical infrastructure to identify, analyze, and share
3 with other members and the Federal Government
4 critical information relating to threats,
5 vulnerabilities, or incidents to the security and resil-
6 iency of the critical infrastructure that comprises the
7 specific sector;

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

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

14 “(15) the term ‘management controls’ means
15 safeguards or countermeasures for an information
16 system that focus on the management of risk and
17 the management of information system security;

18 “(16) the term ‘National Cybersecurity Advi-
19 sory Council’ means the National Cybersecurity Ad-
20 visory Council established under section 239;

21 “(17) the term ‘national cyber emergency’
22 means an actual or imminent action by any indi-
23 vidual or entity to exploit a cyber risk in a manner
24 that disrupts, attempts to disrupt, or poses a signifi-
25 cant risk of disruption to the operation of the infor-

1 mation infrastructure essential to the reliable oper-
2 ation of covered critical infrastructure;

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

5 “(A) that is owned, operated, or controlled
6 within or from the United States; and

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

9 “(19) the term ‘national security system’ has
10 the meaning given that term in section 3551 of title
11 44, United States Code;

12 “(20) the term ‘operational controls’ means the
13 safeguards and countermeasures for an information
14 system that are primarily implemented and executed
15 by individuals not systems;

16 “(21) the term ‘sector-specific agency’ means
17 the relevant Federal agency responsible for infra-
18 structure protection activities in a designated critical
19 infrastructure sector or key resources category under
20 the National Infrastructure Protection Plan, or any
21 other appropriate Federal agency identified by the
22 President after the date of enactment of this sub-
23 title;

24 “(22) the term ‘sector coordinating councils’
25 means self-governed councils that are composed of

1 representatives of key stakeholders within a specific
2 sector of critical infrastructure that serve as the
3 principal private sector policy coordination and plan-
4 ning entities with the Federal Government relating
5 to the security and resiliency of the critical infra-
6 structure that comprise that sector;

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

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

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

20 “(26) the term ‘terrorism information’ has the
21 meaning given that term in section 1016 of the In-
22 telligence Reform and Terrorism Prevention Act of
23 2004 (6 U.S.C. 485);

24 “(27) the term ‘United States person’ has the
25 meaning given that term in section 101 of the For-

1 eign Intelligence Surveillance Act of 1978 (50
2 U.S.C. 1801); and

3 “(28) the term ‘US–CERT’ means the United
4 States Computer Emergency Readiness Team estab-
5 lished under section 244.

6 **“SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND**
7 **COMMUNICATIONS.**

8 “(a) ESTABLISHMENT.—

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

12 “(2) OPERATIONAL ENTITY.—The Center
13 may—

14 “(A) enter into contracts for the procure-
15 ment of property and services for the Center;
16 and

17 “(B) appoint employees of the Center in
18 accordance with the civil service laws of the
19 United States.

20 “(b) DIRECTOR.—

21 “(1) IN GENERAL.—The Center shall be headed
22 by a Director, who shall be appointed by the Presi-
23 dent, by and with the advice and consent of the Sen-
24 ate.

1 “(2) REPORTING TO SECRETARY.—The Direc-
 2 tor shall report directly to the Secretary and serve
 3 as the principal advisor to the Secretary on cyberse-
 4 curity and the operations, security, and resiliency of
 5 the information infrastructure and communications
 6 infrastructure of the United States.

7 “(3) PRESIDENTIAL ADVICE.—The Director
 8 shall regularly advise the President on the exercise
 9 of the authorities provided under this subtitle or any
 10 other provision of law relating to the security of the
 11 Federal information infrastructure or an agency in-
 12 formation infrastructure.

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

15 “(A) a demonstrated ability in and knowl-
 16 edge of information technology, cybersecurity,
 17 and the operations, security and resiliency of
 18 communications networks; and

19 “(B) significant executive leadership and
 20 management experience in the public or private
 21 sector.

22 “(5) LIMITATION ON SERVICE.—

23 “(A) IN GENERAL.—Subject to subpara-
 24 graph (B), the individual serving as the Direc-
 25 tor may not, while so serving, serve in any

1 other capacity in the Federal Government, ex-
2 cept to the extent that the individual serving as
3 Director is doing so in an acting capacity.

4 “(B) EXCEPTION.—The Director may
5 serve on any commission, board, council, or
6 similar entity with responsibilities or duties re-
7 lating to cybersecurity or the operations, secu-
8 rity, and resiliency of the information infra-
9 structure and communications infrastructure of
10 the United States at the direction of the Presi-
11 dent or as otherwise provided by law.

12 “(c) DEPUTY DIRECTORS.—

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

16 “(2) INFRASTRUCTURE PROTECTION.—

17 “(A) APPOINTMENT.—There shall be a
18 Deputy Director appointed by the Secretary,
19 who shall have expertise in infrastructure pro-
20 tection.

21 “(B) RESPONSIBILITIES.—The Deputy Di-
22 rector appointed under subparagraph (A)
23 shall—

24 “(i) assist the Director and the As-
25 sistant Secretary for Infrastructure Protec-

tion in coordinating, managing, and directing the information, communications, and physical infrastructure protection responsibilities and activities of the Department, including activities under Homeland Security Presidential Directive–7, or any successor thereto, and the National Infrastructure Protection Plan, or any successor thereto;

“(ii) review the budget for the Center and the Office of Infrastructure Protection before submission of the budget to the Secretary to ensure that activities are appropriately coordinated;

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

“(iv) subject to the direction of the Director resolve conflicts between the Center and the Office of Infrastructure Protection relating to the information, commu-

1 communications, and physical infrastructure pro-
 2 tection responsibilities of the Center and
 3 the Office of Infrastructure Protection;
 4 and

5 “(v) perform such other duties as the
 6 Director may assign.

7 “(C) ANNUAL EVALUATION.—The Assist-
 8 ant Secretary for Infrastructure Protection
 9 shall submit annually to the Director an evalua-
 10 tion of the performance of the Deputy Director
 11 appointed under subparagraph (A).

12 “(3) INTELLIGENCE COMMUNITY.—The Direc-
 13 tor of National Intelligence shall identify an em-
 14 ployee of an element of the intelligence community
 15 to serve as a Deputy Director of the Center. The
 16 employee shall be detailed to the Center on a reim-
 17 bursable basis for such period as is agreed to by the
 18 Director and the Director of National Intelligence,
 19 and, while serving as Deputy Director, shall report
 20 directly to the Director of the Center.

21 “(d) LIAISON OFFICERS.—

22 “(1) IN GENERAL.—The Secretary of Defense,
 23 the Attorney General, the Secretary of Commerce,
 24 and the Director of National Intelligence shall detail
 25 personnel to the Center to act as full-time liaisons

1 with the Department of Defense, the Department of
2 Justice, the National Institute of Standards and
3 Technology, and elements of the intelligence commu-
4 nity to assist in coordination between and among the
5 Center, the Department of Defense, the Department
6 of Justice, the National Institute of Standards and
7 Technology, and elements of the intelligence commu-
8 nity.

9 “(2) PRIVATE SECTOR.—

10 “(A) IN GENERAL.—Consistent with appli-
11 cable law and ethics requirements, and except
12 as provided in subparagraph (B), the Director
13 may authorize representatives from private sec-
14 tor entities to participate in the activities of the
15 Center to improve the information sharing,
16 analysis, and coordination of activities of the
17 US-CERT.

18 “(B) LIMITATION.—A representative from
19 a private sector entity authorized to participate
20 in the activities of the Center under subpara-
21 graph (A) may not participate in any activities
22 of the Center under section 248, 249, or 250.

23 “(e) PRIVACY OFFICER.—

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

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

9 “(f) DUTIES OF DIRECTOR.—

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

11 “(A) working cooperatively with the private
 12 sector, lead the Federal effort to secure, pro-
 13 tect, and ensure the resiliency of the Federal in-
 14 formation infrastructure, national information
 15 infrastructure, and communications infrastruc-
 16 ture of the United States, including commu-
 17 nications networks;

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

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

1 mation infrastructure that is owned, operated,
2 controlled, or licensed for use by, or on behalf
3 of, the Department of Defense, a military de-
4 partment, or another element of the intelligence
5 community, and information infrastructure lo-
6 cated outside the United States the disruption
7 of which could result in national or regional
8 catastrophic damage in the United States by
9 sharing and integrating classified and unclassi-
10 fied information, including information relating
11 to threats, vulnerabilities, traffic, trends, inci-
12 dents, and other anomalous activities affecting
13 the infrastructure or systems, on a routine and
14 continuous basis with—

15 “(i) the National Threat Operations
16 Center of the National Security Agency;

17 “(ii) the United States Cyber Com-
18 mand, including the Joint Task Force-
19 Global Network Operations;

20 “(iii) the Cyber Crime Center of the
21 Department of Defense;

22 “(iv) the National Cyber Investigative
23 Joint Task Force;

24 “(v) the Intelligence Community Inci-
25 dent Response Center;

1 “(vi) any other Federal agency, or
2 component thereof, identified by the Direc-
3 tor; and

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

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

14 “(E)(i) develop, in coordination with the
15 Assistant Secretary for Infrastructure Protec-
16 tion, other Federal agencies, the private sector,
17 and State and local governments, a national in-
18 cident response plan that details the roles of
19 Federal agencies, State and local governments,
20 and the private sector, including plans to be ex-
21 ecuted in response to a declaration of a national
22 cyber emergency by the President under section
23 249; and

24 “(ii) establish mechanisms for assisting
25 owners or operators of critical infrastructure,

1 including covered critical infrastructure, in the
2 deployment of emergency measures or other ac-
3 tions, including measures to restore the critical
4 infrastructure in the event of the destruction or
5 a serious disruption of the critical infrastruc-
6 ture;

7 “(F) conduct risk-based assessments of the
8 Federal information infrastructure with respect
9 to acts of terrorism, natural disasters, and
10 other large-scale disruptions and provide the re-
11 sults of the assessments to the Director of
12 Cyberspace Policy and to affected Federal agen-
13 cies;

14 “(G) develop, oversee the implementation
15 of, and enforce policies, principles, and guide-
16 lines on information security for the Federal in-
17 formation infrastructure, including timely adop-
18 tion of and compliance with standards devel-
19 oped by the National Institute of Standards
20 and Technology under section 20 of the Na-
21 tional Institute of Standards and Technology
22 Act (15 U.S.C. 278g-3);

23 “(H) provide assistance to the National In-
24 stitute of Standards and Technology in devel-
25 oping standards under section 20 of the Na-

1 tional Institute of Standards and Technology
2 Act (15 U.S.C. 278g-3);

3 “(I) provide to Federal agencies manda-
4 tory security controls to mitigate and remediate
5 vulnerabilities of and incidents affecting the
6 Federal information infrastructure;

7 “(J) subject to paragraph (2), and as
8 needed, assist the Director of the Office of
9 Management and Budget and the Director of
10 Cyberspace Policy in conducting analysis and
11 prioritization of budgets, resources, and policies
12 relating to the security of the Federal informa-
13 tion infrastructure;

14 “(K) in accordance with section 253, de-
15 velop, periodically update, and implement a
16 supply chain risk management strategy to en-
17 hance, in a risk-based and cost-effective man-
18 ner, the security of the communications and in-
19 formation technology products and services pur-
20 chased by the Federal Government;

21 “(L) notify the Director of Cyberspace
22 Policy of any incident involving the Federal in-
23 formation infrastructure, information infra-
24 structure that is owned, operated, controlled, or
25 licensed for use by, or on behalf of, the Depart-

1 ment of Defense, a military department, or an-
2 other element of the intelligence community, or
3 the national information infrastructure that
4 could compromise or significantly affect eco-
5 nomic or national security;

6 “(M) consult, in coordination with the Di-
7 rector of Cyberspace Policy, with appropriate
8 international partners to enhance the security
9 of the Federal information infrastructure, na-
10 tional information infrastructure, and informa-
11 tion infrastructure located outside the United
12 States the disruption of which could result in
13 national or regional catastrophic damage in the
14 United States;

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

23 “(ii) ensure the information required under
24 clause (i) and section 3553(c)(1)(A) of title 44,
25 United States Code, including the views of the

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

11 “(iii) in conjunction with the quadrennial
12 homeland security review required under section
13 707, and at such other times determined appro-
14 priate by the Director, analyze the composite
15 security state of the national information infra-
16 structure and submit to the President, Con-
17 gress, and the Secretary a report regarding ac-
18 tions necessary to enhance the composite secu-
19 rity state of the national information infrastruc-
20 ture based on the analysis; and

21 “(iv) foster collaboration and serve as the
22 primary contact between the Federal Govern-
23 ment, State and local governments, and private
24 entities on matters relating to the security of

1 the Federal information infrastructure and the
2 national information infrastructure;

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

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

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

24 “(R) ensure, in coordination with the pri-
25 vacy officer designated under subsection (e), the

1 Privacy Officer appointed under section 222,
2 and the Director of the Office of Civil Rights
3 and Civil Liberties appointed under section 705,
4 that the activities of the Center comply with all
5 policies, regulations, and laws protecting the
6 privacy and civil liberties of United States per-
7 sons;

8 “(S) subject to the availability of re-
9 sources, in accordance with applicable law relat-
10 ing to the protection of trade secrets, and at
11 the discretion of the Director, provide voluntary
12 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 and in-
13 formation infrastructure located outside the
14 United States the disruption of which could re-
15 sult in national or regional catastrophic damage
16 in the United States, on a sector-by-sector
17 basis, with respect to acts of terrorism, natural
18 disasters, and other large-scale disruptions or
19 financial harm, which shall identify and
20 prioritize risks to the national information in-
21 frastructure and information infrastructure lo-
22 cated outside the United States the disruption
23 of which could result in national or regional
24 catastrophic damage in the United States, in-

cluding vulnerabilities and associated consequences; and

“(ii) coordinate and evaluate the mitigation or remediation of vulnerabilities and consequences identified under clause (i);

“(U) regularly evaluate and assess technologies designed to enhance the protection of the Federal information infrastructure and national information infrastructure, including an assessment of the cost-effectiveness of the technologies;

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

“(W) develop and implement outreach and awareness programs on cybersecurity, including—

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

“(ii) an education campaign to increase the understanding of State and local

1 governments and private sector entities of
2 the costs of failing to ensure effective secu-
3 rity of information infrastructure and cost-
4 effective methods to mitigate and reme-
5 diate vulnerabilities; and

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

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

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

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

19 “(iii) oversight, in coordination with
20 the Director of the Office of Cyberspace
21 Policy, of the efforts by Federal agencies
22 to address deficiencies identified in the
23 after action reports required under clause
24 (ii);

1 “(Y) coordinate with the Assistant Sec-
2 retary for Infrastructure Protection to ensure
3 that—

4 “(i) cybersecurity is appropriately ad-
5 dressed in carrying out the infrastructure
6 protection responsibilities described in sec-
7 tion 201(d); and

8 “(ii) the operations of the Center and
9 the Office of Infrastructure Protection
10 avoid duplication and use, to the maximum
11 extent practicable, joint mechanisms for in-
12 formation sharing and coordination with
13 the private sector;

14 “(Z) oversee the activities of the Office of
15 Emergency Communications established under
16 section 1801;

17 “(AA) in coordination with the Director of
18 the Office of Cyberspace Policy and the heads
19 of relevant Federal agencies, develop and imple-
20 ment an identity management strategy for
21 cyberspace, which shall include, at a minimum,
22 research and development goals, an analysis of
23 appropriate protections for privacy and civil lib-
24 erties, and mechanisms to develop and dissemi-
25 nate best practices and standards relating to

1 identity management, including usability and
2 transparency; and

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

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

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

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

22 “(j) ASSISTANT TO THE DIRECTOR FOR STATE,
 23 LOCAL, AND PRIVATE SECTOR OUTREACH.—The Director
 24 shall identify a senior official in the Center who—

25 “(1) shall report directly to the Director; and

1 “(2) in coordination with the Special Assistant
2 to the Secretary appointed under section 102(f),
3 shall—

4 “(A) advise the Director on policies and
5 regulations, rules, requirements or other actions
6 affecting the private sector, including the eco-
7 nomic impact;

8 “(B) work with individual businesses and
9 other nongovernmental organizations to foster
10 dialogue with the Center;

11 “(C) foster partnerships and facilitate
12 communication between the Center and State
13 and local governments and private sector enti-
14 ties;

15 “(D) coordinate and maintain communica-
16 tion and interaction with State and local gov-
17 ernments and private sector entities on matters
18 relating to the security of the Federal informa-
19 tion infrastructure and the national information
20 infrastructure;

21 “(E) assist the Director in sharing best
22 practices, guidelines, and other important infor-
23 mation relating to the policies, goals, and activi-
24 ties of the Center;

1 “(F) assist the Director in developing and
 2 implementing the national cybersecurity exer-
 3 cise program under subsection (f)(1)(X) as it
 4 relates to State and local governments and pri-
 5 vate sector entities;

6 “(G) assist the Director in developing the
 7 national incident response plan under sub-
 8 section (f)(1)(E) as it relates to State and local
 9 governments and private sector entities;

10 “(H) assist the Director in information
 11 sharing activities of the Center as it relates to
 12 State and local governments and private sector
 13 entities; and

14 “(I) perform any other duties, as directed
 15 by the Director.

16 **“SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COL-**
 17 **LABORATION.**

18 “(a) IN GENERAL.—The Director and the Assistant
 19 Secretary for Infrastructure Protection shall coordinate
 20 the information, communications, and physical infrastruc-
 21 ture protection responsibilities and activities of the Center
 22 and the Office of Infrastructure Protection.

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

1 **“SEC. 244. UNITED STATES COMPUTER EMERGENCY READI-**
2 **NESS TEAM.**

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

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

9 “(1) collect, coordinate, and disseminate infor-
10 mation on—

11 “(A) risks to the Federal information in-
12 frastructure, information infrastructure that is
13 owned, operated, controlled, or licensed for use
14 by, or on behalf of, the Department of Defense,
15 a military department, or another element of
16 the intelligence community, or the national in-
17 formation infrastructure; and

18 “(B) security controls to enhance the secu-
19 rity of the Federal information infrastructure
20 or the national information infrastructure
21 against the risks identified in subparagraph
22 (A); and

23 “(2) establish a mechanism for engagement
24 with the private sector.

25 “(c) MONITORING, ANALYSIS, WARNING, AND RE-
26 SPONSE.—

1 “(1) DUTIES.—Subject to paragraph (2), the
2 US–CERT shall—

3 “(A) provide analysis and reports to Fed-
4 eral agencies on the security of the Federal in-
5 formation infrastructure;

6 “(B) provide continuous, automated moni-
7 toring of the Federal information infrastructure
8 at external Internet access points, which shall
9 include detection and warning of threats,
10 vulnerabilities, traffic, trends, incidents, and
11 other anomalous activities affecting the infor-
12 mation security of the Federal information in-
13 frastructure;

14 “(C) warn Federal agencies of threats,
15 vulnerabilities, incidents, and anomalous activi-
16 ties that could affect the Federal information
17 infrastructure;

18 “(D) develop, recommend, and deploy secu-
19 rity controls to mitigate or remediate
20 vulnerabilities;

21 “(E) support Federal agencies in con-
22 ducting risk assessments of the agency informa-
23 tion infrastructure;

24 “(F) disseminate to Federal agencies risk
25 analyses of incidents that could impair the risk-

1 based security of the Federal information infra-
2 structure;

3 “(G) develop and acquire predictive ana-
4 lytic tools to evaluate threats, vulnerabilities,
5 traffic, trends, incidents, and anomalous activi-
6 ties;

7 “(H) aid in the detection of, and warn
8 owners or operators of national information in-
9 frastructure regarding, threats, vulnerabilities,
10 and incidents, affecting the national informa-
11 tion infrastructure, including providing—

12 “(i) timely, targeted, and actionable
13 notifications of threats, vulnerabilities, and
14 incidents;

15 “(ii) notifications under this subpara-
16 graph; and

17 “(iii) recommended security controls
18 to mitigate or remediate vulnerabilities;
19 and

20 “(I) respond to assistance requests from
21 Federal agencies and, subject to the availability
22 of resources, owners or operators of the na-
23 tional information infrastructure to—

24 “(i) isolate, mitigate, or remediate in-
25 cidents;

1 “(ii) recover from damages and miti-
2 gate or remediate vulnerabilities; and

3 “(iii) evaluate security controls and
4 other actions taken to secure information
5 infrastructure and incorporate lessons
6 learned into best practices, policies, prin-
7 ciples, and guidelines.

8 “(2) REQUIREMENT.—With respect to the Fed-
9 eral information infrastructure, the US–CERT shall
10 conduct the activities described in paragraph (1) in
11 a manner consistent with the responsibilities of the
12 head of a Federal agency described in section 3553
13 of title 44, United States Code.

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

17 “(A) in conjunction with the Inspector
18 General of the Department, conduct an inde-
19 pendent audit or review of the activities of the
20 US–CERT under paragraph (1)(B), which shall
21 include, at a minimum, an assessment of
22 whether and to what extent the activities au-
23 thorized under paragraph (1)(B) have mon-
24 itored communications other than communica-
25 tions to or from a Federal agency; and

1 “(B) submit to the appropriate committees
2 of Congress and the President a report regard-
3 ing the audit or review under subparagraph
4 (A).

5 “(4) CLASSIFIED ANNEX.—A report submitted
6 under paragraph (3) shall be submitted in an un-
7 classified form, but may include a classified annex,
8 if necessary.

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

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

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

23 “(1) maintain communication;

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

1 “(3) respond to inquiries or requests.

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

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

16 “(2) PHYSICAL ACCESS.—Upon request of the
17 Director, and in consultation with the head of a
18 Federal agency, the Federal agency shall provide
19 physical access to any facility of the Federal agency
20 necessary to determine whether the Federal agency
21 is in compliance with any policies, principles, and
22 guidelines established by the Director under this
23 subtitle, or otherwise necessary to carry out the du-
24 ties, responsibilities, and authorities of the Director
25 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

under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or national information infrastructure shall provide that information to the Director in a timely manner; and

“(3) the Director, in coordination with the Director of the Office of Management and Budget, the Attorney General, the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee), the Director of National Intelligence, and the Archivist of the United States, shall establish guidelines to ensure that information is transferred, stored, and preserved—

“(A) in accordance with applicable laws relating to the protection of trade secrets and other applicable laws; and

“(B) in a manner that protects the privacy and civil liberties of United States persons and intelligence sources and methods.

“(b) OPERATIONAL EVALUATIONS.—

1 “(1) IN GENERAL.—The Director—

2 “(A) subject to paragraph (2), shall de-
3 velop, maintain, and enhance capabilities to
4 evaluate the security of the Federal information
5 infrastructure as described in section
6 3554(a)(3) of title 44, United States Code, in-
7 cluding the ability to conduct risk-based pene-
8 tration testing and vulnerability assessments;

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

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

1 “(2) OPERATIONAL EVALUATIONS.—

2 “(A) IN GENERAL.—The Director may
3 conduct risk-based operational evaluations of
4 the agency information infrastructure of any
5 Federal agency, at a time determined by the
6 Director, in consultation with the head of the
7 Federal agency, using the capabilities developed
8 under paragraph (1)(A).

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

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

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

4 “(A) take corrective measures to meet the
5 policies, principles, standards, and guidelines;
6 and

7 “(B) develop a plan to remediate or miti-
8 gate any vulnerabilities addressed by the poli-
9 cies, principles, standards, and guidelines;

10 “(2) within such time period as the Director
11 shall prescribe, the head of the Federal agency
12 shall—

13 “(A) implement a corrective measure or
14 develop a mitigation plan in accordance with
15 paragraph (1); or

16 “(B) submit to the Director, the Director
17 of the Office of Management and Budget, the
18 Inspector General for the Federal agency, and
19 the appropriate committees of Congress a re-
20 port indicating why the Federal agency has not
21 implemented the corrective measure or devel-
22 oped a mitigation plan; and

23 “(3) after providing notice to the head of the
24 affected Federal agency, the Director may direct the
25 isolation of any component of the agency informa-

tion infrastructure, consistent with the contingency or continuity of operation plans applicable to the agency information infrastructure, until corrective measures are taken or mitigation plans approved by the Director are put in place, if—

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

“(B) the failure to comply presents a significant danger to the Federal information infrastructure.

“SEC. 246. INFORMATION SHARING.

“(a) FEDERAL AGENCIES.—

“(1) INFORMATION SHARING PROGRAM.—Consistent with the responsibilities described in sections 242 and 244, the Director, in consultation with the other members of the Chief Information Officers Council established under section 3603 of title 44, United States Code, and the Federal Information Security Taskforce, shall establish a program for sharing information with and between the Center and other Federal agencies that includes processes and procedures, including standard operating procedures—

1 “(A) under which the Director regularly
2 shares with each Federal agency—

3 “(i) analysis and reports on the com-
4 posite security state of the Federal infor-
5 mation infrastructure and information in-
6 frastructure that is owned, operated, con-
7 trolled, or licensed for use by, or on behalf
8 of, the Department of Defense, a military
9 department, or another element of the in-
10 telligence community, which shall include
11 information relating to threats,
12 vulnerabilities, incidents, or anomalous ac-
13 tivities;

14 “(ii) any available analysis and re-
15 ports regarding the security of the agency
16 information infrastructure; and

17 “(iii) means and methods of pre-
18 venting, responding to, mitigating, and re-
19 mediating vulnerabilities; and

20 “(B) under which the Director may re-
21 quest information from Federal agencies con-
22 cerning the security of the Federal information
23 infrastructure, information infrastructure that
24 is owned, operated, controlled, or licensed for
25 use by, or on behalf of, the Department of De-

1 fense, a military department, or another ele-
2 ment of the intelligence community, or the na-
3 tional information infrastructure necessary to
4 carry out the duties of the Director under this
5 subtitle or any other provision of law.

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

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

10 “(B) guidance on what information shall
11 be shared, including information regarding inci-
12 dents;

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

15 “(D) processes and procedures under
16 which the Director or the head of a Federal
17 agency may report noncompliance with the pro-
18 gram to the Director of Cyberspace Policy.

19 “(3) US–CERT.—The Director of the US–
20 CERT shall ensure that the head of each Federal
21 agency has continual access to data collected by the
22 US–CERT regarding the agency information infra-
23 structure of the Federal agency.

24 “(4) FEDERAL AGENCIES.—

1 “(A) IN GENERAL.—The head of a Federal
2 agency shall comply with all processes and pro-
3 cedures established under this subsection re-
4 garding notification to the Director relating to
5 incidents.

6 “(B) IMMEDIATE NOTIFICATION RE-
7 QUIRED.—Unless otherwise directed by the
8 President, any Federal agency with a national
9 security system shall immediately notify the Di-
10 rector regarding any incident affecting the risk-
11 based security of the national security system.

12 “(b) STATE AND LOCAL GOVERNMENTS, PRIVATE
13 SECTOR, AND INTERNATIONAL PARTNERS.—

14 “(1) IN GENERAL.—The Director shall establish
15 processes and procedures, including standard oper-
16 ating procedures, to ensure bidirectional information
17 sharing with State and local governments, private
18 entities, and international partners of the United
19 States on—

20 “(A) threats, vulnerabilities, incidents, and
21 anomalous activities affecting the national in-
22 formation infrastructure; and

23 “(B) means and methods of preventing, re-
24 sponding to, and mitigating and remediating
25 vulnerabilities.

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

4 “(A) means or methods of accessing classi-
5 fied or unclassified information, as appropriate
6 and in accordance with applicable laws regard-
7 ing trade secrets, that will provide situational
8 awareness of the security of the Federal infor-
9 mation infrastructure and the national informa-
10 tion infrastructure relating to threats,
11 vulnerabilities, traffic, trends, incidents, and
12 other anomalous activities affecting the Federal
13 information infrastructure or the national infor-
14 mation infrastructure;

15 “(B) a mechanism, established in consulta-
16 tion with the heads of the relevant sector-spe-
17 cific agencies, sector coordinating councils, and
18 information sharing and analysis centers, by
19 which owners and operators of covered critical
20 infrastructure shall report incidents in the in-
21 formation infrastructure for covered critical in-
22 frastructure under subsection (c)(1)(A);

23 “(C) guidance on the form, content, and
24 priority of incident reports that shall be sub-

1 mitted under subsection (c)(1)(A), which
2 shall—

3 “(i) include appropriate mechanisms
4 to protect—

5 “(I) information in accordance
6 with section 251;

7 “(II) personally identifiable infor-
8 mation; and

9 “(III) trade secrets; and

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

14 “(D) a procedure for notifying an informa-
15 tion technology provider if a vulnerability is de-
16 tected in the product or service produced by the
17 information technology provider and, where pos-
18 sible, working with the information technology
19 provider to remediate the vulnerability before
20 any public disclosure of the vulnerability so as
21 to minimize the opportunity for the vulner-
22 ability to be exploited; and

23 “(E) an evaluation of the need to provide
24 security clearances to employees of State and

1 local governments, private entities, and inter-
 2 national partners to carry out this subsection.

3 “(3) GUIDELINES.—The Director, in consulta-
 4 tion with the Attorney General, the Director of Na-
 5 tional Intelligence, and the Privacy Officer estab-
 6 lished under section 242(e), shall develop guidelines
 7 to protect the privacy and civil liberties of United
 8 States persons and intelligence sources and methods,
 9 while carrying out this subsection.

10 “(c) INCIDENTS.—

11 “(1) NON-FEDERAL ENTITIES.—

12 “(A) IN GENERAL.—

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

1 “(ii) LIMITATION.—Clause (i) shall
2 not authorize the Director, the Center, the
3 Department, or any other Federal entity
4 to—

5 “(I) compel the disclosure of in-
6 formation relating to an incident un-
7 less otherwise authorized by law; or

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

24 “(B) REPORTING PROCEDURES.—The Di-
25 rector shall establish procedures that enable

1 and encourage the owner or operator of na-
2 tional information infrastructure to report to
3 the Director regarding incidents affecting such
4 information infrastructure.

5 “(2) INFORMATION PROTECTION.—Notwith-
6 standing any other provision of law, information re-
7 ported under paragraph (1) shall be protected from
8 unauthorized disclosure, in accordance with section
9 251.

10 “(d) ADDITIONAL RESPONSIBILITIES.—The Director
11 shall—

12 “(1) share data collected on the Federal infor-
13 mation infrastructure with the National Science
14 Foundation and other accredited research institu-
15 tions for the sole purpose of cybersecurity research
16 in a manner that protects privacy and civil liberties
17 of United States persons and intelligence sources
18 and methods;

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

21 “(A) input about the operations of the
22 Center; and

23 “(B) recommendations for improvements
24 of the Center; and

1 “(3) in coordination with the Secretary of De-
2 fense, the Director of National Intelligence, the Sec-
3 retary of State, and the Attorney General, develop
4 information sharing pilot programs with inter-
5 national partners of the United States.

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

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

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

23 “(1) regularly assess and evaluate cybersecurity
24 standards and guidelines issued by private sector or-
25 ganizations, recognized international and domestic

1 standards setting organizations, and Federal agen-
 2 cies; and

3 “(2) in coordination with the National Institute
 4 of Standards and Technology, encourage the devel-
 5 opment of, and recommend changes to, the stand-
 6 ards and guidelines described in paragraph (1) for
 7 securing the national information infrastructure.

8 “(c) GUIDANCE AND TECHNICAL ASSISTANCE.—

9 “(1) IN GENERAL.—The Director shall promote
 10 best practices and related standards and guidelines
 11 to assist owners and operators of national informa-
 12 tion infrastructure in increasing the security of the
 13 national information infrastructure and protecting
 14 against and mitigating or remediating known
 15 vulnerabilities.

16 “(2) REQUIREMENT.—Technical assistance pro-
 17 vided under section 242(f)(1)(S) and best practices
 18 promoted under this section shall be prioritized
 19 based on risk.

20 “(d) CRITERIA.—In promoting best practices or rec-
 21 ommending changes to standards and guidelines under
 22 this section, the Director shall ensure that best practices,
 23 and related standards and guidelines—

24 “(1) address cybersecurity in a comprehensive,
 25 risk-based manner;

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

4 “(3) increase the ability of the owners or opera-
5 tors of national information infrastructure to protect
6 against and mitigate or remediate known
7 vulnerabilities;

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

10 “(5) as necessary and appropriate, are sector
11 specific;

12 “(6) to the maximum extent possible, incor-
13 porate standards and guidelines established by pri-
14 vate sector organizations, recognized international
15 and domestic standards setting organizations, and
16 Federal agencies;

17 “(7) consider voluntary programs by internet
18 service providers to assist individuals using the
19 internet service providers in the identification and
20 mitigation of cyber threats and vulnerabilities, with
21 the consent of the individual users; and

22 “(8) provide sufficient flexibility to permit a
23 range of security solutions.

1 **“SEC. 248. CYBER RISKS TO COVERED CRITICAL INFRA-**
 2 **STRUCTURE.**

3 “(a) IDENTIFICATION OF CYBER RISKS.—

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

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

20 “(A) the actual or assessed threat, includ-
 21 ing a consideration of adversary capabilities and
 22 intent, preparedness, target attractiveness, and
 23 deterrence capabilities;

24 “(B) the extent and likelihood of death, in-
 25 jury, or serious adverse effects to human health

1 and safety caused by a disruption of the reliable
 2 operation of covered critical infrastructure;

3 “(C) the threat to or impact on national
 4 security caused by a disruption of the reliable
 5 operation of covered critical infrastructure;

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

10 “(E) the harm to the economy that would
 11 result from a disruption of the reliable oper-
 12 ation of covered critical infrastructure; and

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

23 “(3) REPORT.—

24 “(A) IN GENERAL.—Not later than 180
 25 days after the date of enactment of this sub-

1 title, and annually thereafter, the Director, in
 2 coordination with the head of the sector-specific
 3 agency with responsibility for the covered crit-
 4 ical infrastructure and the head of any Federal
 5 agency that is not a sector-specific agency with
 6 responsibilities for regulating the covered crit-
 7 ical infrastructure, shall submit to the appro-
 8 priate committees of Congress a report on the
 9 findings of the identification and evaluation of
 10 cyber risks under this subsection. Each report
 11 submitted under this paragraph shall be sub-
 12 mitted in an unclassified form, but may include
 13 a classified annex.

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

19 “(b) RISK-BASED SECURITY PERFORMANCE RE-
 20 QUIREMENTS.—

21 “(1) IN GENERAL.—Not later than 270 days
 22 after the date of the enactment of this subtitle, in
 23 coordination with the heads of the sector-specific
 24 agencies with responsibility for covered critical infra-
 25 structure and the head of any Federal agency that

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

12 “(2) PROCEDURES.—The regulations issued
13 under this subsection shall—

14 “(A) include a process under which owners
15 and operators of covered critical infrastructure
16 are informed of identified cyber risks and secu-
17 rity performance requirements designed to re-
18 mediate or mitigate the cyber risks, in combina-
19 tion with best practices recommended under
20 section 247;

21 “(B) establish a process for owners and
22 operators of covered critical infrastructure to
23 select security measures, including any best
24 practices recommended under section 247, that,
25 in combination, satisfy the security performance

1 requirements established by the Director under
2 this subsection;

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

7 “(D) establish a process under which the
8 Director—

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

13 “(ii) may determine whether the pro-
14 posed security measures satisfy the secu-
15 rity performance requirements established
16 by the Director under this subsection; and

17 “(E) establish a process under which the
18 Director—

19 “(i) identifies to owners and operators
20 of covered critical infrastructure cyber
21 risks that are not capable of effective re-
22 mediation or mitigation using available
23 best practices or security measures;

24 “(ii) provides owners and operators of
25 covered critical infrastructure the oppor-

tunity to develop best practices or security measures to remediate or mitigate the cyber risks identified in clause (i) without the prior approval of the Director and without affecting the compliance of the covered critical infrastructure with the requirements under this section;

“(iii) in accordance with applicable law relating to the protection of trade secrets, permits owners and operators of covered critical infrastructure to report to the Center the development of effective best practices or security measures to remediate or mitigate the cyber risks identified under clause (i); and

“(iv) incorporates the best practices and security measures developed into the risk-based security performance requirements under this section.

“(3) INTERNATIONAL COOPERATION ON SECURING COVERED CRITICAL INFRASTRUCTURE.—

“(A) IN GENERAL.—The Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal

1 agency that is not a sector-specific agency with
2 responsibilities for regulating the covered crit-
3 ical infrastructure, shall—

4 “(i) consistent with the protection of
5 intelligence sources and methods and other
6 sensitive matters, inform the owner or op-
7 erator of information infrastructure located
8 outside the United States the disruption of
9 which could result in national or regional
10 catastrophic damage in the United States
11 and the government of the country in
12 which the information infrastructure is lo-
13 cated of any cyber risks to the information
14 infrastructure; and

15 “(ii) coordinate with the government
16 of the country in which the information in-
17 frastructure is located and, as appropriate,
18 the owner or operator of the information
19 infrastructure, regarding the implementa-
20 tion of security measures or other meas-
21 ures to the information infrastructure to
22 mitigate or remediate cyber risks.

23 “(B) INTERNATIONAL AGREEMENTS.—The
24 Director shall carry out this paragraph in a

1 manner consistent with applicable international
2 agreements.

3 “(4) RISK-BASED SECURITY PERFORMANCE RE-
4 QUIREMENTS.—

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

8 “(i) based on the factors listed in sub-
9 section (a)(2); and

10 “(ii) designed to remediate or mitigate
11 identified cyber risks and any associated
12 consequences of an exploitation based on
13 such risks.

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

18 “(i) the Director of the National Se-
19 curity Agency;

20 “(ii) the Director of the National In-
21 stitute of Standards and Technology;

22 “(iii) the National Cybersecurity Advi-
23 sory Council;

24 “(iv) the heads of sector-specific agen-
25 cies; and

1 “(v) the heads of Federal agencies
2 that are not sector-specific agencies with
3 responsibilities for regulating the covered
4 critical infrastructure.

5 “(C) ALTERNATIVE MEASURES.—

6 “(i) IN GENERAL.—The owners and
7 operators of covered critical infrastructure
8 shall have flexibility to implement any se-
9 curity measure, or combination thereof, to
10 satisfy the security performance require-
11 ments described in subparagraph (A) and
12 the Director may not disapprove under this
13 section any proposed security measures, or
14 combination thereof, based on the presence
15 or absence of any particular security meas-
16 ure if the proposed security measures, or
17 combination thereof, satisfy the security
18 performance requirements established by
19 the Director under this section or are con-
20 sistent with the process for addressing new
21 or evolving cyber risks established under
22 paragraph (2)(E).

23 “(ii) RECOMMENDED SECURITY MEAS-
24 URES.—The Director may recommend to
25 an owner and operator of covered critical

1 infrastructure a specific security measure,
2 or combination thereof, that will satisfy the
3 security performance requirements estab-
4 lished by the Director. The absence of the
5 recommended security measures, or com-
6 bination thereof, may not serve as the
7 basis for a disapproval of the security
8 measure, or combination thereof, proposed
9 by the owner or operator of covered critical
10 infrastructure if the proposed security
11 measure, or combination thereof, otherwise
12 satisfies the security performance require-
13 ments established by the Director under
14 this section.

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

16 “(a) DECLARATION.—

17 “(1) IN GENERAL.—The President may issue a
18 declaration of a national cyber emergency to covered
19 critical infrastructure if there is an ongoing or immi-
20 nent action by any individual or entity to exploit a
21 cyber risk in a manner that disrupts, attempts to
22 disrupt, or poses a significant risk of disruption to
23 the operation of the information infrastructure es-
24 sential to the reliable operation of covered critical in-
25 frastructure. Any declaration under this section shall

1 specify the covered critical infrastructure subject to
2 the national cyber emergency.

3 “(2) NOTIFICATION.—Upon issuing a declara-
4 tion under paragraph (1), the President shall, con-
5 sistent with the protection of intelligence sources
6 and methods, notify the owners and operators of the
7 specified covered critical infrastructure and any
8 other relevant private sector entity of the nature of
9 the national cyber emergency.

10 “(3) AUTHORITIES.—If the President issues a
11 declaration under paragraph (1), the Director
12 shall—

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

18 “(B) develop and coordinate emergency
19 measures or actions necessary to preserve the
20 reliable operation, and mitigate or remediate
21 the consequences of the potential disruption, of
22 covered critical infrastructure;

23 “(C) ensure that emergency measures or
24 actions directed under this section represent the
25 least disruptive means feasible to the operations

1 of the covered critical infrastructure and to the
2 national information infrastructure;

3 “(D) subject to subsection (g), direct ac-
4 tions by other Federal agencies to respond to
5 the national cyber emergency;

6 “(E) coordinate with officials of State and
7 local governments, international partners of the
8 United States, owners and operators of covered
9 critical infrastructure specified in the declara-
10 tion, and other relevant private sector entities
11 to respond to the national cyber emergency;

12 “(F) initiate a process under section 248
13 to address the cyber risk that may be exploited
14 by the national cyber emergency; and

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

17 “(4) REIMBURSEMENT.—A Federal agency
18 shall be reimbursed for expenditures under this sec-
19 tion from funds appropriated for the purposes of
20 this section. Any funds received by a Federal agency
21 as reimbursement for services or supplies furnished
22 under the authority of this section shall be deposited
23 to the credit of the appropriation or appropriations
24 available on the date of the deposit for the services
25 or supplies.

1 “(5) CONSULTATION.—In carrying out this sec-
2 tion, the Director shall consult with the Secretary,
3 the Secretary of Defense, the Director of the Na-
4 tional Security Agency, the Director of the National
5 Institute of Standards and Technology, and any
6 other official, as directed by the President.

7 “(6) PROHIBITED ACTIONS.—The authority to
8 direct compliance with an emergency measure or ac-
9 tion under this section shall not authorize the Direc-
10 tor, the Center, the Department, or any other Fed-
11 eral entity to—

12 “(A) restrict or prohibit communications
13 carried by, or over, covered critical infrastruc-
14 ture and not specifically directed to or from the
15 covered critical infrastructure unless the Direc-
16 tor determines that no other emergency meas-
17 ure or action will preserve the reliable oper-
18 ation, and mitigate or remediate the con-
19 sequences of the potential disruption, of the
20 covered critical infrastructure or the national
21 information infrastructure;

22 “(B) control covered critical infrastructure;

23 “(C) compel the disclosure of information
24 unless specifically authorized by law; or

1 “(D) intercept a wire, oral, or electronic
 2 communication (as those terms are defined in
 3 section 2510 of title 18, United States Code),
 4 access a stored electronic or wire communica-
 5 tion, install or use a pen register or trap and
 6 trace device, or conduct electronic surveillance
 7 (as defined in section 101 of the Foreign Intel-
 8 ligence Surveillance Act of 1978 (50 U.S.C.
 9 1801)) relating to an incident, unless otherwise
 10 authorized under chapter 119, chapter 121, or
 11 chapter 206 of title 18, United States Code, or
 12 the Foreign Intelligence Surveillance Act of
 13 1978 (50 U.S.C. 1801 et seq.).

14 “(7) PRIVACY.—In carrying out this section,
 15 the Director shall ensure that the privacy and civil
 16 liberties of United States persons are protected.

17 “(b) DISCONTINUANCE OF EMERGENCY MEAS-
 18 URES.—

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

24 “(A) the Director details in writing why
 25 the emergency measure or action remains nec-

1 essary to address the identified national cyber
2 emergency; and

3 “(B) the President issues a written order
4 or directive reaffirming the national cyber
5 emergency, the continuing nature of the na-
6 tional cyber emergency, or the need to continue
7 the adoption of the emergency measure or ac-
8 tion.

9 “(2) EXTENSIONS.—An emergency measure or
10 action extended in accordance with paragraph (1)
11 may—

12 “(A) remain in effect for not more than 30
13 days after the date on which the emergency
14 measure or action was to cease to have effect;
15 and

16 “(B) unless a joint resolution described in
17 subsection (f)(1) is enacted, be extended for not
18 more than 3 additional 30-day periods, if the
19 requirements of paragraph (1) and subsection
20 (d) are met.

21 “(c) COMPLIANCE WITH EMERGENCY MEASURES.—

22 “(1) IN GENERAL.—Subject to paragraph (2),
23 the owner or operator of covered critical infrastruc-
24 ture shall immediately comply with any emergency
25 measure or action developed by the Director under

1 this section during the pendency of any declaration
 2 by the President under subsection (a)(1) or an ex-
 3 tension under subsection (b)(2).

4 “(2) ALTERNATIVE MEASURES.—

5 “(A) IN GENERAL.—If the Director deter-
 6 mines that a proposed security measure, or any
 7 combination thereof, submitted by the owner or
 8 operator of covered critical infrastructure in ac-
 9 cordance with the process established under sec-
 10 tion 248(b)(2) will effectively mitigate or reme-
 11 diate the cyber risk associated with the national
 12 cyber emergency that is the subject of the dec-
 13 laration under this section, or effectively miti-
 14 gate or remediate the consequences of the po-
 15 tential disruption of the covered critical infra-
 16 structure based on the cyber risk at least as ef-
 17 fectively as the emergency measures or actions
 18 directed by the Director under this section, the
 19 owner or operator may comply with paragraph
 20 (1) of this subsection by implementing the pro-
 21 posed security measure, or combination thereof,
 22 approved by the Director under the process es-
 23 tablished under section 248.

24 “(B) COMPLIANCE PENDING SUBMISSION
 25 OR APPROVAL.—Before submission of a pro-

posed security measure, or combination thereof,
 and during the pendency of any review by the
 Director under the process established under
 section 248, the owner or operator of covered
 critical infrastructure shall remain in compli-
 ance with any emergency measure or action de-
 veloped by the Director under this section dur-
 ing the pendency of any declaration by the
 President under subsection (a)(1) or an exten-
 sion under subsection (b)(2), until such time as
 the Director has approved an alternative pro-
 posed security measure, or combination thereof,
 under this paragraph.

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

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

“(i) consistent with the protection of
 intelligence sources and methods and other
 sensitive matters, inform the owner or op-

erator of information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States and the government of the country in which the information infrastructure is located of any cyber risks to the information infrastructure that led to the declaration of a national cyber emergency; and

“(ii) coordinate with the government of the country in which the information infrastructure is located and, as appropriate, the owner or operator of the information infrastructure, regarding the implementation of emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure that is the subject of the national cyber emergency.

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

“(d) REPORTING.—

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

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

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

17 “(A) the nature of the national cyber
18 emergency;

19 “(B) the reasons that risk-based security
20 requirements under section 248 are not suffi-
21 cient to address the national cyber emergency;

22 “(C) the actions necessary to preserve the
23 reliable operation and mitigate the con-
24 sequences of the potential disruption of covered
25 critical infrastructure; and

1 “(D) in the case of an extension of a na-
 2 tional cyber emergency under subsection
 3 (b)(2)—

4 “(i) why the emergency measures or
 5 actions continue to be necessary to address
 6 the national cyber emergency; and

7 “(ii) when the President expects the
 8 national cyber emergency to abate.

9 “(e) STATUTORY DEFENSES AND CIVIL LIABILITY
 10 LIMITATIONS FOR COMPLIANCE WITH EMERGENCY
 11 MEASURES.—

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

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

14 “(i) means a civil action filed in a
 15 Federal or State court against a covered
 16 entity; and

17 “(ii) does not include an action
 18 brought under section 2520 or 2707 of
 19 title 18, United States Code, or section
 20 110 or 308 of the Foreign Intelligence
 21 Surveillance Act of 1978 (50 U.S.C. 1810
 22 and 1828);

23 “(B) the term ‘covered entity’ means any
 24 entity that owns or operates covered critical in-
 25 frastructure, including any owner, operator, of-

1 ficer, employee, agent, landlord, custodian, pro-
 2 vider of information technology, or other person
 3 acting for or on behalf of that entity with re-
 4 spect to the covered critical infrastructure; and

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

13 “(2) APPLICATION OF LIMITATIONS ON CIVIL
 14 LIABILITY.—The limitations on civil liability under
 15 paragraph (3) apply if—

16 “(A) the President has issued a declaration
 17 of national cyber emergency under subsection
 18 (a)(1);

19 “(B) the Director has—

20 “(i) issued emergency measures or ac-
 21 tions for which compliance is required
 22 under subsection (c)(1); or

23 “(ii) approved security measures
 24 under subsection (c)(2);

1 “(C) the covered entity is in compliance
2 with—

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

5 “(ii) security measures which the Di-
6 rector has approved under subsection
7 (c)(2); and

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

13 “(I) emergency measures or actions
14 for which compliance is required under
15 subsection (c)(1); or

16 “(II) security measures which the Di-
17 rector has approved under subsection
18 (c)(2); or

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

1 “(I) emergency measures or actions
2 for which compliance is required under
3 subsection (c)(1); or

4 “(II) security measures which the Di-
5 rector has approved under subsection
6 (c)(2).

7 “(3) LIMITATIONS ON CIVIL LIABILITY.—In any
8 covered civil action that is related to any incident as-
9 sociated with a cyber risk covered by a declaration
10 of a national cyber emergency and for which Direc-
11 tor has issued emergency measures or actions for
12 which compliance is required under subsection (c)(1)
13 or for which the Director has approved security
14 measures under subsection (c)(2), or that is the di-
15 rect consequence of actions taken in good faith for
16 the purpose of implementing security measures or
17 actions which the Director has approved under sub-
18 section (c)(2)—

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

24 “(B) noneconomic damages may be award-
25 ed against a defendant only in an amount di-

rectly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover non-economic damages unless the plaintiff suffered physical harm.

“(4) CIVIL ACTIONS ARISING OUT OF IMPLEMENTATION OF EMERGENCY MEASURES OR ACTIONS.—A covered civil action may not be maintained against a covered entity that is the direct consequence of actions taken in good faith for the purpose of implementing specific emergency measures or actions for which compliance is required under subsection (c)(1), if—

“(A) the President has issued a declaration of national cyber emergency under subsection (a)(1) and the action was taken during the period covered by that declaration;

“(B) the Director has issued emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2);

“(C) the covered entity is in compliance with the emergency measures required under subsection (c)(1) or that the Director has approved under subsection (c)(2); and

“(D)(i) the Director certifies to the court in which the covered civil action is pending that the actions taken by the entity during the period covered by the declaration under subsection (a)(1) were consistent with the implementation of emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2); or

“(ii) notwithstanding the lack of a certification, the entity demonstrates by a preponderance of the evidence that the actions taken during the period covered by the declaration under subsection (a)(1) are consistent with the implementation of emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2).

“(5) CERTAIN ACTIONS NOT SUBJECT TO LIMITATIONS ON LIABILITY.—

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

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

4 “(i) whose recovery is otherwise pre-
5 cluded by application of paragraph (4);
6 and

7 “(ii) who has suffered—

8 “(I) serious physical injury or
9 death; or

10 “(II) substantial damage or de-
11 struction to his primary residence.

12 “(C) RULE OF CONSTRUCTION.—Recovery
13 available under subparagraph (B) shall be lim-
14 ited to those damages available under subpara-
15 graphs (A) and (B) of paragraph (3), except
16 that neither reasonable and necessary medical
17 benefits nor lifetime total benefits for lost em-
18 ployment income due to permanent and total
19 disability shall be limited herein.

20 “(D) INDEMNIFICATION.—In any civil ac-
21 tion brought under subparagraph (B), the
22 United States shall defend and indemnify any
23 covered entity. Any covered entity defended and
24 indemnified under this subparagraph shall fully
25 cooperate with the United States in the defense

1 by the United States in any proceeding and
 2 shall be reimbursed the reasonable costs associ-
 3 ated with such cooperation.

4 “(f) JOINT RESOLUTION TO EXTEND CYBER EMER-
 5 GENCY.—

6 “(1) IN GENERAL.—For purposes of subsection
 7 (b)(2)(B), a joint resolution described in this para-
 8 graph means only a joint resolution—

9 “(A) the title of which is as follows: ‘Joint
 10 resolution approving the extension of a cyber
 11 emergency’; and

12 “(B) the matter after the resolving clause
 13 of which is as follows: ‘That Congress approves
 14 the continuation of the emergency measure or
 15 action issued by the Director of the National
 16 Center for Cybersecurity and Communications
 17 on _____ for not longer
 18 than an additional 120-day period.’, the blank
 19 space being filled in with the date on which the
 20 emergency measure or action to which the joint
 21 resolution applies was issued.

22 “(2) PROCEDURE.—

23 “(A) NO REFERRAL.—A joint resolution
 24 described in paragraph (1) shall not be referred

1 to a committee in either House of Congress and
2 shall immediately be placed on the calendar.

3 “(B) CONSIDERATION.—

4 “(i) DEBATE LIMITATION.—A motion
5 to proceed to a joint resolution described in
6 paragraph (1) is highly privileged in the
7 House of Representatives and is privileged
8 in the Senate and is not debatable. The
9 motion is not subject to a motion to post-
10 pone. In the Senate, consideration of the
11 joint resolution, and on all debatable mo-
12 tions and appeals in connection therewith,
13 shall be limited to not more than 10 hours,
14 which shall be divided equally between the
15 majority leader and the minority leader, or
16 their designees. A motion further to limit
17 debate is in order and not debatable. All
18 points of order against the joint resolution
19 (and against consideration of the joint res-
20 olution) are waived. An amendment to, or
21 a motion to postpone, or a motion to pro-
22 ceed to the consideration of other business,
23 or a motion to recommit the joint resolu-
24 tion is not in order.

1 “(ii) **PASSAGE.**—In the Senate, imme-
 2 diately following the conclusion of the de-
 3 bate on a joint resolution described in
 4 paragraph (1), and a single quorum call at
 5 the conclusion of the debate if requested in
 6 accordance with the rules of the Senate,
 7 the vote on passage of the joint resolution
 8 shall occur.

9 “(iii) **APPEALS.**—Appeals from the
 10 decisions of the Chair relating to the appli-
 11 cation of the rules of the Senate to the
 12 procedure relating to a joint resolution de-
 13 scribed in paragraph (1) shall be decided
 14 without debate.

15 “(C) **OTHER HOUSE ACTS FIRST.**—If, be-
 16 fore the passage by 1 House of a joint resolu-
 17 tion of that House described in paragraph (1),
 18 that House receives from the other House a
 19 joint resolution described in paragraph (1)—

20 “(i) the procedure in that House shall
 21 be the same as if no joint resolution had
 22 been received from the other House; and

23 “(ii) the vote on final passage shall be
 24 on the joint resolution of the other House.

1 “(D) MAJORITY REQUIRED FOR ADOPTION.—A joint resolution considered under this
 2 subsection shall require an affirmative vote of a
 3 majority of the Members, duly chosen and
 4 sworn, for adoption.
 5

6 “(3) RULEMAKING.—This subsection is enacted
 7 by Congress—

8 “(A) as an exercise of the rulemaking
 9 power of the Senate and the House of Rep-
 10 resentatives, respectively, and is deemed to be
 11 part of the rules of each House, respectively but
 12 applicable only with respect to the procedure to
 13 be followed in that House in the case of a joint
 14 resolution described in paragraph (1), and it
 15 supersedes other rules only to the extent that it
 16 is inconsistent with such rules; and

17 “(B) with full recognition of the constitu-
 18 tional right of either House to change the rules
 19 (so far as they relate to the procedure of that
 20 House) at any time, in the same manner, and
 21 to the same extent as in the case of any other
 22 rule of that House.

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

1 “(1) alter or supersede the authority of the Sec-
 2 retary of Defense, the Attorney General, or the Di-
 3 rector of National Intelligence in responding to a na-
 4 tional cyber emergency; or

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

8 **“SEC. 250. ENFORCEMENT.**

9 “(a) ANNUAL CERTIFICATION OF COMPLIANCE.—

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

21 “(2) FAILURE TO COMPLY.—If an owner or op-
 22 erator of covered critical infrastructure fails to sub-
 23 mit a certification in accordance with paragraph (1),
 24 or if the certification indicates the owner or operator
 25 is not in compliance, the Director may issue an

1 order requiring the owner or operator to submit pro-
2 posed security measures under section 248 or com-
3 ply with specific emergency measures or actions
4 under section 249.

5 “(b) RISK-BASED EVALUATIONS.—

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

13 “(2) DOCUMENT REVIEW AND INSPECTION.—

14 An evaluation performed under paragraph (1) may
15 include—

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

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

24 “(3) EVALUATION SELECTION FACTORS.—In
25 determining whether sufficient risk exists to justify

1 an evaluation under this subsection, the Director
2 shall consider—

3 “(A) the specific cyber risks affecting or
4 potentially affecting the information infrastruc-
5 ture of the specific system or asset constituting
6 covered critical infrastructure;

7 “(B) any reliable intelligence or other in-
8 formation indicating a cyber risk or credible na-
9 tional cyber emergency to the information infra-
10 structure of the specific system or asset consti-
11 tuting covered critical infrastructure;

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

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

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

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

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

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

9 “(c) CIVIL PENALTIES.—

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

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

17 “(d) LIMITATION ON CIVIL LIABILITY.—

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

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

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

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

110 or 308 of the Foreign Intelligence
Surveillance Act of 1978 (50 U.S.C. 1810
and 1828);

“(B) the term ‘covered entity’ means any
entity that owns or operates covered critical in-
frastructure, including any owner, operator, of-
ficer, employee, agent, landlord, custodian, pro-
vider of information technology, or other person
acting for or on behalf of that entity with re-
spect to the covered critical infrastructure; and

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

“(2) LIMITATIONS ON CIVIL LIABILITY.—If a
covered entity experiences an incident related to a
cyber risk identified under section 248(a), in any
covered civil action for damages directly caused by
the incident related to that cyber risk—

“(A) the covered entity shall not be liable
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 risk.

4 “(4) LIMITATION.—This subsection shall only
5 apply to harm directly caused by the incident related
6 to the cyber risk and shall not apply to damages
7 caused by any additional or intervening acts or omis-
8 sions 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 security performance requirements of covered
21 critical infrastructure under subsection 248(b) and this
22 section including—

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, the Attorney Gen-

1 eral, and the National Cybersecurity Advisory Coun-
2 cil, as necessary to implement this section.

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

5 “(A) consistent with subsections (e)(2)(D)
6 and (g) of section 214 and the processes, proce-
7 dures, and guidelines developed under section
8 246(b), include provisions for information shar-
9 ing among Federal, State, and local and offi-
10 cials, private entities, or international partners
11 of the United States necessary to carry out the
12 authorities and responsibilities of 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 or
5 affect measures and controls relating to the protec-
6 tion of classified information as prescribed by Fed-
7 eral statute or under Executive Order 12958, or any
8 successor of that order;

9 “(3) limit the right of an individual to make
10 any disclosure—

11 “(A) protected or authorized under section
12 2302(b)(8) or 7211 of title 5, United States
13 Code;

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

1 tive order to be kept secret in the interest of
2 national defense or the conduct of foreign af-
3 fairs; or

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

8 “(4) prevent the Director from using informa-
9 tion required to be submitted under sections 246,
10 248, or 249 for enforcement of this subtitle, includ-
11 ing enforcement proceedings subject to appropriate
12 safeguards;

13 “(5) authorize information to be withheld from
14 Congress, the Government Accountability Office, or
15 Inspector General of the Department;

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

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

20 “(f) AUDIT.—

21 “(1) IN GENERAL.—Not later than 1 year after
22 the date of enactment of the Cybersecurity and
23 Internet Freedom Act of 2011, the Inspector Gen-
24 eral of the Department shall conduct an audit of the
25 management of information submitted under sub-

1 section (b) and report the findings to appropriate
2 committees of Congress.

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

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

7 “(B) the processes for marking and dis-
8 seminating the information and resolving any
9 disputes;

10 “(C) how the information is used for the
11 purposes of this section, and whether that use
12 is effective;

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

15 “(E) whether the kinds of information sub-
16 mitted have been appropriate and useful, or
17 overbroad or overnarrow;

18 “(F) whether the information protections
19 allow for adequate accountability and trans-
20 parency of the regulatory, enforcement, and
21 other aspects of implementing this subtitle; and

22 “(G) any other factors at the discretion of
23 the Inspector General.

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

2 “(a) IN GENERAL.—The head of each sector-specific
3 agency and the head of any Federal agency that is not
4 a sector-specific agency with responsibilities for regulating
5 covered critical infrastructure shall coordinate with the
6 Director on any activities of the sector-specific agency or
7 Federal agency that relate to the efforts of the agency re-
8 garding security or resiliency of the national information
9 infrastructure, including critical infrastructure and cov-
10 ered critical infrastructure, within or under the super-
11 vision of the agency.

12 “(b) DUPLICATIVE REPORTING REQUIREMENTS.—
13 The head of each sector-specific agency and the head of
14 any Federal agency that is not a sector-specific agency
15 with responsibilities for regulating covered critical infra-
16 structure shall coordinate with the Director to eliminate
17 and avoid the creation of duplicate reporting or compli-
18 ance requirements relating to the security or resiliency of
19 the national information infrastructure, including critical
20 infrastructure and covered critical infrastructure, within
21 or under the supervision of the agency.

22 “(c) REQUIREMENTS.—

23 “(1) IN GENERAL.—To the extent that the head
24 of each sector-specific agency and the head of any
25 Federal agency that is not a sector-specific agency
26 with responsibilities for regulating covered critical

1 infrastructure has the authority to establish regula-
2 tions, rules, or requirements or other required ac-
3 tions that are applicable to the security of national
4 information infrastructure, including critical infra-
5 structure and covered critical infrastructure, the
6 head of that agency shall—

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

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

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

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

1 “(3) RULE OF CONSTRUCTION.—Nothing in
 2 this section shall be construed to provide additional
 3 authority for any sector-specific agency or any Fed-
 4 eral agency that is not a sector-specific agency with
 5 responsibilities for regulating national information
 6 infrastructure, including critical infrastructure or
 7 covered critical infrastructure, to establish standards
 8 or other measures that are applicable to the security
 9 of national information infrastructure not otherwise
 10 authorized by law.

11 **“SEC. 253. STRATEGY FOR FEDERAL CYBERSECURITY SUP-**
 12 **PLY CHAIN MANAGEMENT.**

13 “(a) IN GENERAL.—The Secretary, in consultation
 14 with the Director of Cyberspace Policy, the Director, the
 15 Secretary of Defense, the Secretary of Commerce, the Sec-
 16 retary of State, the Director of National Intelligence, the
 17 Administrator of General Services, the Administrator for
 18 Federal Procurement Policy, the other members of the
 19 Chief Information Officers Council established under sec-
 20 tion 3603 of title 44, United States Code, the Chief Acqui-
 21 sition Officers Council established under section 1311 of
 22 title 41, United States Code, the Chief Financial Officers
 23 Council established under section 302 of the Chief Finan-
 24 cial Officers Act of 1990 (31 U.S.C. 901 note), and the
 25 private sector, shall develop, periodically update, and im-

1 plement a supply chain risk management strategy de-
 2 signed to ensure, based on mission criticality and cost ef-
 3 fectiveness, the security of the Federal information infra-
 4 structure, including protection against unauthorized ac-
 5 cess to, alteration of information in, disruption of oper-
 6 ations of, interruption of communications or services of,
 7 and insertion of malicious software, engineering
 8 vulnerabilities, or otherwise corrupting software, hard-
 9 ware, services, or products intended for use in Federal in-
 10 formation infrastructure.

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

13 “(1) address risks in the supply chain during
 14 the entire life cycle of any part of the Federal infor-
 15 mation infrastructure;

16 “(2) place particular emphasis on—

17 “(A) securing critical information systems
 18 and the Federal information infrastructure;

19 “(B) developing processes that—

20 “(i) incorporate all-source intelligence
 21 analysis into assessments of the supply
 22 chain for the Federal information infra-
 23 structure;

24 “(ii) assess risks from potential sup-
 25 pliers providing critical components or

1 services of the Federal information infra-
2 structure;

3 “(iii) assess risks from individual
4 components, including all subcomponents,
5 or software used in or affecting the Fed-
6 eral information infrastructure;

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

14 “(v) detect the occurrence, reduce the
15 likelihood of occurrence, and mitigate or
16 remediate the risks associated with prod-
17 ucts containing counterfeit components or
18 malicious functions;

19 “(vi) enhance developmental and oper-
20 ational test and evaluation capabilities, in-
21 cluding software vulnerability detection
22 methods and automated methods and tools
23 that shall be integrated into acquisition
24 policy practices by Federal agencies and,

1 where appropriate, make the capabilities
2 available for use by the private sector; and

3 “(vii) protect the intellectual property
4 and trade secrets of suppliers of informa-
5 tion and communications technology prod-
6 ucts and services;

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

13 “(D) identifying acquisition practices of
14 Federal agencies that increase risks in the sup-
15 ply chain and developing a process to provide
16 recommendations for revisions to those proc-
17 esses; and

18 “(E) sharing with the private sector, to the
19 fullest extent possible, the threats identified in
20 the supply chain and working with the private
21 sector to develop responses to those threats as
22 identified; and

23 “(3) to the maximum extent practicable, pro-
24 mote the ability of Federal agencies to procure au-
25 thentic commercial off the shelf information and

1 communications technology products and services
2 from a diverse pool of suppliers.

3 “(c) IMPLEMENTATION.—The Federal Acquisition
4 Regulatory Council established under section 1302(a) of
5 title 41, United States Code, shall—

6 “(1) amend the Federal Acquisition Regulation
7 maintained under section 1303(a)(1) of title 41,
8 United States Code, to—

9 “(A) incorporate, where relevant, the sup-
10 ply chain risk management strategy developed
11 under subsection (a) to improve security
12 throughout the acquisition process; and

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

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

24 “(d) PREFERENCES FOR ACQUISITION OF COMMER-
25 CIAL ITEMS.—The strategy developed under this section,

1 and any actions taken under subsection (c), shall be con-
 2 sistent with the preferences for the acquisition of commer-
 3 cial items under section 2377 of title 10, United States
 4 Code, and section 3307 of title 41, United States Code.”.

5 **TITLE III—FEDERAL INFORMA-**
 6 **TION SECURITY MANAGE-**
 7 **MENT**

8 **SEC. 301. COORDINATION OF FEDERAL INFORMATION POL-**
 9 **ICY.**

10 (a) FINDINGS.—Congress finds that—

11 (1) since 2002 the Federal Government has ex-
 12 perienceed multiple high-profile incidents that re-
 13 sulted in the theft of sensitive information amount-
 14 ing to more than the entire print collection con-
 15 tained in the Library of Congress, including person-
 16 ally identifiable information, advanced scientific re-
 17 search, and prenegotiated United States diplomatic
 18 positions; and

19 (2) chapter 35 of title 44, United States Code,
 20 must be amended to increase the coordination of
 21 Federal agency activities and to enhance situational
 22 awareness throughout the Federal Government using
 23 more effective enterprise-wide automated moni-
 24 toring, detection, and response capabilities.

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

4 “SUBCHAPTER II—INFORMATION SECURITY
5 “§ 3550. **Purposes**

6 “The purposes of this subchapter are to—

7 “(1) provide a comprehensive framework for en-
8 suring the effectiveness of information security con-
9 trols over information resources that support the
10 Federal information infrastructure and the oper-
11 ations and assets of agencies;

12 “(2) recognize the highly networked nature of
13 the current Federal information infrastructure and
14 provide effective Government-wide management and
15 oversight of the related information security risks,
16 including coordination of information security efforts
17 throughout the civilian, national security, and law
18 enforcement communities;

19 “(3) provide for development and maintenance
20 of prioritized and risk-based security controls re-
21 quired to protect Federal information infrastructure
22 and information systems; and

23 “(4) provide a mechanism for improved over-
24 sight of Federal agency information security pro-
25 grams.

1 “(5) acknowledge that commercially developed
 2 information security products offer advanced, dy-
 3 namic, robust, and effective information security so-
 4 lutions, reflecting market solutions for the protection
 5 of critical information infrastructures important to
 6 the national defense and economic security of the
 7 Nation that are designed, built, and operated by the
 8 private sector; and

9 “(6) recognize that the selection of specific
 10 technical hardware and software information secu-
 11 rity solutions should be left to individual agencies
 12 from among commercially developed products.

13 **“§ 3551. Definitions**

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

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

18 “(1) The term ‘agency information infrastruc-
 19 ture’—

20 “(A) means information infrastructure
 21 that is owned, operated, controlled, or licensed
 22 for use by, or on behalf of, an agency, including
 23 information systems used or operated by an-
 24 other entity on behalf of the agency; and

1 “(B) does not include national security
2 systems.

3 “(2) The term ‘automated and continuous mon-
4 itoring’ means monitoring at a frequency and suffi-
5 ciency such that the data exchange requires little to
6 no human involvement and is not interrupted.

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

9 “(A) actually or imminently jeopardizes—

10 “(i) the information security of infor-
11 mation infrastructure; or

12 “(ii) the information that information
13 infrastructure processes, stores, receives,
14 or transmits; or

15 “(B) constitutes a violation of security
16 policies, security procedures, or acceptable use
17 policies applicable to information infrastructure.

18 “(4) The term ‘information infrastructure’
19 means the underlying framework that information
20 systems and assets rely on to process, transmit, re-
21 ceive, or store information electronically, including
22 programmable electronic devices and communica-
23 tions networks and any associated hardware, soft-
24 ware, or data.

1 “(5) The term ‘information security’ means
2 protecting information and information systems
3 from disruption or unauthorized access, use, disclo-
4 sure, modification, or destruction in order to pro-
5 vide—

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

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

14 “(C) availability, by ensuring timely and
15 reliable access to and use of information.

16 “(6) The term ‘information technology’ has the
17 meaning given that term in section 11101 of title
18 40.

19 “(7) The term ‘management controls’ means
20 safeguards or countermeasures for an information
21 system that focus on the management of risk and
22 the management of information system security.

23 “(8)(A) The term ‘national security system’
24 means any information system (including any tele-
25 communications system) used or operated by an

1 agency or by a contractor of an agency, or other or-
2 ganization on behalf of an agency—

3 “(i) the function, operation, or use of
4 which—

5 “(I) involves intelligence activities;

6 “(II) involves cryptologic activities re-
7 lated to national security;

8 “(III) involves command and control
9 of military forces;

10 “(IV) involves equipment that is an
11 integral part of a weapon or weapons sys-
12 tem; or

13 “(V) subject to subparagraph (B), is
14 critical to the direct fulfillment of military
15 or intelligence missions; or

16 “(ii) that is protected at all times by proce-
17 dures established for information that have
18 been specifically authorized under criteria es-
19 tablished by an Executive order or an Act of
20 Congress to be kept classified in the interest of
21 national defense or foreign policy.

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

1 “(9) The term ‘operational controls’ means the
2 safeguards and countermeasures for an information
3 system that are primarily implemented and executed
4 by individuals, not systems.

5 “(10) The term ‘risk’ means the potential for
6 an unwanted outcome resulting from an incident, as
7 determined by the likelihood of the occurrence of the
8 incident and the associated consequences, including
9 potential for an adverse outcome assessed as a func-
10 tion of threats, vulnerabilities, and consequences as-
11 sociated with an incident.

12 “(11) The term ‘risk-based security’ means se-
13 curity commensurate with the risk and magnitude of
14 harm resulting from the loss, misuse, or unauthor-
15 ized access to, or modification, of information, in-
16 cluding assuring that systems and applications used
17 by the agency operate effectively and provide appro-
18 priate confidentiality, integrity, and availability.

19 “(12) The term ‘security controls’ means the
20 management, operational, and technical controls pre-
21 scribed for an information system to protect the in-
22 formation security of the system.

23 “(13) The term ‘technical controls’ means the
24 safeguards or countermeasures for an information
25 system that are primarily implemented and executed

1 by the information system through mechanism con-
 2 tained in the hardware, software, or firmware com-
 3 ponents of the system.

4 **“§ 3552. Authority and functions of the National Cen-**
 5 **ter for Cybersecurity and Communica-**
 6 **tions**

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

9 “(1) develop, oversee the implementation of,
 10 and enforce policies, principles, and guidelines on in-
 11 formation security, including through ensuring time-
 12 ly agency adoption of and compliance with standards
 13 developed under section 20 of the National Institute
 14 of Standards and Technology Act (15 U.S.C. 278g–
 15 3) and subtitle E of title II of the Homeland Secu-
 16 rity Act of 2002;

17 “(2) provide to agencies security controls that
 18 agencies shall be required to be implemented to miti-
 19 gate and remediate vulnerabilities, attacks, and ex-
 20 ploitations discovered as a result of activities re-
 21 quired under this subchapter or subtitle E of title II
 22 of the Homeland Security Act of 2002;

23 “(3) to the extent practicable—

24 “(A) prioritize the policies, principles,
 25 standards, and guidelines promulgated under

1 section 20 of the National Institute of Stand-
2 ards and Technology Act (15 U.S.C. 278g-3),
3 paragraph (1), and subtitle E of title II of the
4 Homeland Security Act of 2002, based upon
5 the risk of an incident; and

6 “(B) develop guidance that requires agen-
7 cies to monitor, including automated and con-
8 tinuous monitoring of, the effective implementa-
9 tion of policies, principles, standards, and
10 guidelines developed under section 20 of the
11 National Institute of Standards and Technology
12 Act (15 U.S.C. 278g-3), paragraph (1), and
13 subtitle E of title II of the Homeland Security
14 Act of 2002;

15 “(C) ensure the effective operation of tech-
16 nical capabilities within the National Center for
17 Cybersecurity and Communications to enable
18 automated and continuous monitoring of any
19 information collected as a result of the guidance
20 developed under subparagraph (B) and use the
21 information to enhance the risk-based security
22 of the Federal information infrastructure; and

23 “(D) ensure the effective operation of a se-
24 cure system that satisfies information reporting

1 requirements under sections 3553(c) and
2 3556(c);

3 “(4) require agencies, consistent with the stand-
4 ards developed under section 20 of the National In-
5 stitute of Standards and Technology Act (15 U.S.C.
6 278g–3) or paragraph (1) and the requirements of
7 this subchapter, to identify and provide information
8 security protections commensurate with the risk re-
9 sulting from the disruption or unauthorized access,
10 use, disclosure, modification, or destruction of—

11 “(A) information collected or maintained
12 by or on behalf of an agency; or

13 “(B) information systems used or operated
14 by an agency or by a contractor of an agency
15 or other organization on behalf of an agency;

16 “(5) oversee agency compliance with the re-
17 quirements of this subchapter, including coordi-
18 nating with the Office of Management and Budget
19 to use any authorized action under section 11303 of
20 title 40 to enforce accountability for compliance with
21 such requirements;

22 “(6) review, at least annually, and approve or
23 disapprove, agency information security programs
24 required under section 3553(b); and

1 “(7) coordinate information security policies
 2 and procedures with the Administrator for Elec-
 3 tronic Government and the Administrator for the
 4 Office of Information and Regulatory Affairs with
 5 related information resources management policies
 6 and procedures.

7 “(b) NATIONAL SECURITY SYSTEMS.—The authori-
 8 ties of the Director of the National Center for Cybersecu-
 9 rity and Communications under this section shall not
 10 apply to national security systems.

11 **“§ 3553. Agency responsibilities**

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

13 “(1) be responsible for—

14 “(A) providing information security protec-
 15 tions commensurate with the risk and mag-
 16 nitude of the harm resulting from unauthorized
 17 access, use, disclosure, disruption, modification,
 18 or destruction of—

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

21 “(ii) agency information infrastruc-
 22 ture;

23 “(B) complying with the requirements of
 24 this subchapter and related policies, procedures,
 25 standards, and guidelines, including—

1 “(i) information security require-
2 ments, including security controls, devel-
3 oped by the Director of the National Cen-
4 ter for Cybersecurity and Communications
5 under section 3552, subtitle E of title II of
6 the Homeland Security Act of 2002, or
7 any other provision of law;

8 “(ii) information security policies,
9 principles, standards, and guidelines pro-
10 mulgated under section 20 of the National
11 Institute of Standards and Technology Act
12 (15 U.S.C. 278g–3) and section
13 3552(a)(1);

14 “(iii) information security standards
15 and guidelines for national security sys-
16 tems issued in accordance with law and as
17 directed by the President; and

18 “(iv) ensuring the standards imple-
19 mented for information systems and na-
20 tional security systems of the agency are
21 complementary and uniform, to the extent
22 practicable;

23 “(C) ensuring that information security
24 management processes are integrated with
25 agency strategic and operational planning and

1 budget processes, including policies, procedures,
2 and practices described in subsection (c)(1)(C);

3 “(D) as appropriate, maintaining secure
4 facilities that have the capability of accessing,
5 sending, receiving, and storing classified infor-
6 mation;

7 “(E) maintaining a sufficient number of
8 personnel with security clearances, at the ap-
9 propriate levels, to access, send, receive and
10 analyze classified information to carry out the
11 responsibilities of this subchapter; and

12 “(F) ensuring that information security
13 performance indicators and measures are in-
14 cluded in the annual performance evaluations of
15 all managers, senior managers, senior executive
16 service personnel, and political appointees;

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

22 “(A) assessing the risk and magnitude of
23 the harm that could result from the disruption
24 or unauthorized access, use, disclosure, modi-

1 fication, or destruction of such information or
2 information systems;

3 “(B) determining the levels of information
4 security appropriate to protect such information
5 and information systems in accordance with
6 policies, principles, standards, and guidelines
7 promulgated under section 20 of the National
8 Institute of Standards and Technology Act (15
9 U.S.C. 278g–3), section 3552(a)(1), and sub-
10 title E of title II of the Homeland Security Act
11 of 2002, for information security categoriza-
12 tions and related requirements;

13 “(C) implementing policies and procedures
14 to cost effectively reduce risks to an acceptable
15 level;

16 “(D) periodically testing and evaluating in-
17 formation security controls and techniques to
18 ensure that such controls and techniques are
19 operating effectively; and

20 “(E) withholding all bonus and cash
21 awards to senior agency officials accountable
22 for the operation of such agency information in-
23 frastructure that are recognized by the Chief
24 Information Security Officer as impairing the

1 risk-based security information, information
2 system, or agency information infrastructure;

3 “(3) delegate to a senior agency officer des-
4 ignated as the Chief Information Security Officer
5 the authority and budget necessary to ensure and
6 enforce compliance with the requirements imposed
7 on the agency under this subchapter, subtitle E of
8 title II of the Homeland Security Act of 2002, or
9 any other provision of law, including—

10 “(A) overseeing the establishment, mainte-
11 nance, and management of a security oper-
12 ations center that has technical capabilities that
13 can, through automated and continuous moni-
14 toring—

15 “(i) detect, report, respond to, con-
16 tain, remediate, and mitigate incidents
17 that impair risk-based security of the in-
18 formation, information systems, and agen-
19 cy information infrastructure, in accord-
20 ance with policy provided by the Director
21 of the National Center for Cybersecurity
22 and Communications;

23 “(ii) monitor and, on a risk-based
24 basis, mitigate and remediate the
25 vulnerabilities of every information system

1 within the agency information infrastruc-
2 ture;

3 “(iii) continually evaluate risks posed
4 to information collected or maintained by
5 or on behalf of the agency and information
6 systems and hold senior agency officials
7 accountable for ensuring the risk-based se-
8 curity of such information and information
9 systems;

10 “(iv) collaborate with the Director of
11 the National Center for Cybersecurity and
12 Communications and appropriate public
13 and private sector security operations cen-
14 ters to address incidents that impact the
15 security of information and information
16 systems that extend beyond the control of
17 the agency; and

18 “(v) report any incident described
19 under clauses (i) and (ii), as directed by
20 the policy of the Director of the National
21 Center for Cybersecurity and Communica-
22 tions and the Inspector General of the
23 agency;

24 “(B) collaborating with the Administrator
25 for E–Government and the Chief Information

1 Officer to establish, maintain, and update an
2 enterprise network, system, storage, and secu-
3 rity architecture, that can be accessed by the
4 National Cybersecurity Communications Center
5 and includes—

6 “(i) information on how security con-
7 trols are implemented throughout the
8 agency information infrastructure; and

9 “(ii) information on how the controls
10 described under subparagraph (A) main-
11 tain the appropriate level of confidentiality,
12 integrity, and availability of information
13 and information systems based on—

14 “(I) the policy of the Director of
15 the National Center for Cybersecurity
16 and Communications; and

17 “(II) the standards or guidance
18 developed by the National Institute of
19 Standards and Technology;

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

23 “(D) developing, maintaining, and over-
24 seeing information security policies, procedures,
25 and control techniques to address all applicable

1 requirements, including those issued under sec-
2 tion 3552;

3 “(E) training, consistent with the require-
4 ments of section 406 of the Cybersecurity and
5 Internet Freedom Act of 2011, and overseeing
6 personnel with significant responsibilities for in-
7 formation security with respect to such respon-
8 sibilities; and

9 “(F) assisting senior agency officers con-
10 cerning their responsibilities under paragraph
11 (2);

12 “(4) ensure that the Chief Information Security
13 Officer has a sufficient number of cleared and
14 trained personnel with technical skills identified by
15 the Director of the National Center for Cybersecu-
16 rity and Communications as critical to maintaining
17 the risk-based security of agency information infra-
18 structure as required by the subchapter and other
19 applicable laws;

20 “(5) ensure that the agency Chief Information
21 Security Officer, in coordination with appropriate
22 senior agency officials, reports not less than annu-
23 ally to the head of the agency on the effectiveness
24 of the agency information security program, includ-
25 ing progress of remedial actions;

1 “(6) ensure that the Chief Information Security
2 Officer—

3 “(A) possesses necessary qualifications, in-
4 cluding education, professional certifications,
5 training, experience, and the security clearance
6 required to administer the functions described
7 under this subchapter; and

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

10 “(7) ensure that components of that agency es-
11 tablish and maintain an automated reporting mecha-
12 nism that allows the Chief Information Security Of-
13 ficer with responsibility for the entire agency, and all
14 components thereof, to implement, monitor, and hold
15 senior agency officers accountable for the implemen-
16 tation of appropriate security policies, procedures,
17 and controls of agency components.

18 “(b) AGENCY-WIDE INFORMATION SECURITY PRO-
19 GRAM.—Each agency shall develop, document, and imple-
20 ment an agency-wide information security program, ap-
21 proved by the Director of the National Center for Cyberse-
22 curity and Communications under section 3552(a)(6) and
23 consistent with components across and within agencies, to
24 provide information security for the information and infor-
25 mation systems that support the operations and assets of

1 the agency, including those provided or managed by an-
2 other agency, contractor, or other source, that includes—

3 “(1) frequent assessments, at least twice each
4 month—

5 “(A) of the risk and magnitude of the
6 harm that could result from the disruption or
7 unauthorized access, use, disclosure, modifica-
8 tion, or destruction of information and informa-
9 tion systems that support the operations and
10 assets of the agency; and

11 “(B) that assess whether information or
12 information systems should be removed or mi-
13 grated to more secure networks or standards
14 and make recommendations to the head of the
15 agency and the Director of the National Center
16 for Cybersecurity and Communications based
17 on that assessment;

18 “(2) consistent with guidance developed under
19 section 3554, vulnerability assessments and penetra-
20 tion tests commensurate with the risk posed to an
21 agency information infrastructure;

22 “(3) ensure that information security
23 vulnerabilities are remediated or mitigated based on
24 the risk posed to the agency;

25 “(4) policies and procedures that—

1 “(A) are informed and revised by the as-
2 sessments required under paragraphs (1) and
3 (2);

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

6 “(C) ensure that information security is
7 addressed throughout the life cycle of each
8 agency information system; and

9 “(D) ensure compliance with—

10 “(i) the requirements of this sub-
11 chapter;

12 “(ii) policies and procedures pre-
13 scribed by the Director of the National
14 Center for Cybersecurity and Communica-
15 tions;

16 “(iii) minimally acceptable system
17 configuration requirements, as determined
18 by the Director of the National Center for
19 Cybersecurity and Communications; and

20 “(iv) any other applicable require-
21 ments, including standards and guidelines
22 for national security systems issued in ac-
23 cordance with law and as directed by the
24 President;

1 “(5) subordinate plans for providing risk-based
2 information security for networks, facilities, and sys-
3 tems or groups of information systems, as appro-
4 priate;

5 “(6) role-based security awareness training,
6 consistent with the requirements of section 406 of
7 the Cybersecurity and Internet Freedom Act of
8 2011, to inform personnel with access to the agency
9 network, including contractors and other users of in-
10 formation systems that support the operations and
11 assets of the agency, of—

12 “(A) information security risks associated
13 with agency activities; and

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

17 “(7) periodic testing and evaluation of the ef-
18 fectiveness of information security policies, proce-
19 dures, and practices, to be performed with a rigor
20 and frequency depending on risk, which shall in-
21 clude—

22 “(A) testing and evaluation not less than
23 twice each year of security controls of informa-
24 tion collected or maintained by or on behalf of
25 the agency and every information system identi-

1 fied in the inventory required under section
2 3505(c);

3 “(B) the effectiveness of ongoing moni-
4 toring, including automated and continuous
5 monitoring, vulnerability scanning, and intru-
6 sion detection and prevention of incidents posed
7 to the risk-based security of information and in-
8 formation systems as required under subsection
9 (a)(3); and

10 “(C) testing relied on in—

11 “(i) an operational evaluation under
12 section 3554;

13 “(ii) an independent assessment under
14 section 3556; or

15 “(iii) another evaluation, to the extent
16 specified by the Director of the National
17 Center for Cybersecurity and Communica-
18 tions;

19 “(8) a process for planning, implementing, eval-
20 uating, and documenting remedial action to address
21 any deficiencies in the information security policies,
22 procedures, and practices of the agency;

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

1 “(A) to the extent practicable, automated
2 and continuous monitoring of the use of infor-
3 mation and information systems;

4 “(B) requirements for mitigating risks and
5 remediating vulnerabilities associated with such
6 incidents systemically within the agency infor-
7 mation infrastructure before substantial dam-
8 age is done; and

9 “(C) notifying and coordinating with the
10 Director of the National Center for Cybersecu-
11 rity and Communications, as required by this
12 subchapter, subtitle E of title II of the Home-
13 land Security Act of 2002, and any other provi-
14 sion of law; and

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

18 “(c) AGENCY REPORTING.—

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

20 “(A) ensure that information relating to
21 the adequacy and effectiveness of information
22 security policies, procedures, and practices, is
23 available to the entities identified under para-
24 graph (2) through the system developed under

1 section 3552(a)(3), including information relat-
2 ing to—

3 “(i) compliance with the requirements
4 of this subchapter;

5 “(ii) the effectiveness of the informa-
6 tion security policies, procedures, and prac-
7 tices of the agency based on a determina-
8 tion of the aggregate effect of identified
9 deficiencies and vulnerabilities;

10 “(iii) an identification and analysis of
11 any significant deficiencies identified in
12 such policies, procedures, and practices;

13 “(iv) an identification of any vulner-
14 ability that could impair the risk-based se-
15 curity of the agency information infra-
16 structure; and

17 “(v) results of any operational evalua-
18 tion conducted under section 3554 and
19 plans of action to address the deficiencies
20 and vulnerabilities identified as a result of
21 such operational evaluation;

22 “(B) follow the policy, guidance, and
23 standards of the Director of the National Cen-
24 ter for Cybersecurity and Communications, in
25 consultation with the Federal Information Secu-

1 rity Taskforce, to continually update, and en-
2 sure the electronic availability of both a classi-
3 fied and unclassified version of the information
4 required under subparagraph (A);

5 “(C) ensure the information under sub-
6 paragraph (A) addresses the adequacy and ef-
7 fectiveness of information security policies, pro-
8 cedures, and practices in plans and reports re-
9 lating to—

10 “(i) annual agency budgets;

11 “(ii) information resources manage-
12 ment of this subchapter;

13 “(iii) information technology manage-
14 ment and procurement under this chapter
15 or any other applicable provision of law;

16 “(iv) subtitle E of title II of the
17 Homeland Security Act of 2002;

18 “(v) program performance under sec-
19 tions 1105 and 1115 through 1119 of title
20 31, and sections 2801 and 2805 of title
21 39;

22 “(vi) financial management under
23 chapter 9 of title 31, and the Chief Finan-
24 cial Officers Act of 1990 (31 U.S.C. 501

1 note; Public Law 101–576) (and the
2 amendments made by that Act);

3 “(vii) financial management systems
4 under the Federal Financial Management
5 Improvement Act (31 U.S.C. 3512 note);

6 “(viii) internal accounting and admin-
7 istrative controls under section 3512 of
8 title 31; and

9 “(ix) performance ratings, salaries,
10 and bonuses provided to the senior man-
11 agers and supporting personnel taking into
12 account program performance as it relates
13 to complying with this subchapter; and

14 “(D) report any significant deficiency in a
15 policy, procedure, or practice identified under
16 subparagraph (A) or (B)—

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

19 “(ii) if relating to financial manage-
20 ment systems, as an instance of a lack of
21 substantial compliance under the Federal
22 Financial Management Improvement Act
23 (31 U.S.C. 3512 note).

24 “(2) ADEQUACY AND EFFECTIVENESS INFOR-
25 MATION.—Information required under paragraph

(1)(A) shall, to the extent possible and in accordance with applicable law, policy, guidance, and standards, be available on an automated and continuous basis to—

“(A) the Director of the National Center for Cybersecurity and Communications;

“(B) the Office of Management and Budget;

“(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

“(D) the Committee on Government Oversight and Reform of the House of Representatives;

“(E) the Committee on Homeland Security of the House of Representatives;

“(F) other appropriate authorization and appropriations committees of Congress;

“(G) the Inspector General of the Federal agency; and

“(H) the Comptroller General.

“(d) INCLUSIONS IN PERFORMANCE PLANS.—

“(1) IN GENERAL.—In addition to the requirements of subsection (c), each agency, in consultation with the Director of the National Center for Cybersecurity and Communications, shall include as part

1 of the performance plan required under section 1115
2 of title 31 a description of the time periods the re-
3 sources, including budget, staffing, and training,
4 that are necessary to implement the program re-
5 quired under subsection (b).

6 “(2) RISK ASSESSMENTS.—The description
7 under paragraph (1) shall be based on the risk and
8 vulnerability assessments required under subsection
9 (b) and evaluations required under section 3554.

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

15 “(f) MORE STRINGENT STANDARDS.—The head of
16 an agency may employ standards for the cost effective in-
17 formation security for information systems within or
18 under the supervision of that agency that are more strin-
19 gent than the standards the Director of the National Cen-
20 ter for Cybersecurity and Communications prescribes
21 under this subchapter, subtitle E of title II of the Home-
22 land Security Act of 2002, or any other provision of law,
23 if the more stringent standards—

24 “(1) contain at least the applicable standards
25 made compulsory and binding by the Director of the

1 National Center for Cybersecurity and Communica-
2 tions; and

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

5 **“§ 3554. Annual operational evaluation**

6 “(a) GUIDANCE.—

7 “(1) IN GENERAL.—Not later than 1 year after
8 the date of enactment of the Cybersecurity and
9 Internet Freedom Act of 2011 and each year there-
10 after, the Director of the National Center for Cyber-
11 security and Communications shall oversee, coordi-
12 nate, and develop guidance for the effective imple-
13 mentation of operational evaluations of the Federal
14 information infrastructure and agency information
15 security programs and practices to determine the ef-
16 fectiveness of such program and practices.

17 “(2) COLLABORATION IN DEVELOPMENT.—In
18 developing guidance for the operational evaluations
19 described under this section, the Director of the Na-
20 tional Center for Cybersecurity and Communications
21 shall collaborate with the Federal Information Secu-
22 rity Taskforce and the Council of Inspectors General
23 on Integrity and Efficiency, and other agencies as
24 necessary, to develop and update risk-based perform-
25 ance indicators and measures that assess the ade-

quacy and effectiveness of information security of an agency and the Federal information infrastructure.

“(3) CONTENTS OF OPERATIONAL EVALUATION.—Each operational evaluation under this section—

“(A) shall be prioritized based on risk; and

“(B) shall—

“(i) test the effectiveness of agency information security policies, procedures, and practices of the information systems of the agency, or a representative subset of those information systems;

“(ii) assess (based on the results of the testing) compliance with—

“(I) the requirements of this subchapter; and

“(II) related information security policies, procedures, standards, and guidelines;

“(iii) evaluate whether agencies—

“(I) effectively monitor, detect, analyze, protect, report, and respond to vulnerabilities and incidents;

“(II) report to and collaborate with the appropriate public and pri-

1 vate security operation centers, the
2 Director of the National Center for
3 Cybersecurity and Communications,
4 and law enforcement agencies; and

5 “(III) remediate or mitigate the
6 risk posed by attacks and exploi-
7 tations in a timely fashion in order to
8 prevent future vulnerabilities and inci-
9 dents; and

10 “(iv) identify deficiencies of agency in-
11 formation security policies, procedures, and
12 controls on the agency information infra-
13 structure.

14 “(b) CONDUCT AN OPERATIONAL EVALUATION.—

15 “(1) IN GENERAL.—Except as provided under
16 paragraph (2), and in consultation with the Chief
17 Information Officer and senior officials responsible
18 for the affected systems, the Chief Information Se-
19 curity Officer of each agency shall not less than an-
20 nually—

21 “(A) conduct an operational evaluation of
22 the agency information infrastructure for
23 vulnerabilities, attacks, and exploitations of the
24 agency information infrastructure;

1 “(B) evaluate the ability of the agency to
2 monitor, detect, correlate, analyze, report, and
3 respond to incidents; and

4 “(C) report to the head of the agency, the
5 Director of the National Center for Cybersecu-
6 rity and Communications, the Chief Informa-
7 tion Officer, and the Inspector General for the
8 agency the findings of the operational evalua-
9 tion.

10 “(2) SATISFACTION OF REQUIREMENTS BY
11 OTHER EVALUATION.—Unless otherwise specified by
12 the Director of the National Center for Cybersecu-
13 rity and Communications, if the Director of the Na-
14 tional Center for Cybersecurity and Communications
15 conducts an operational evaluation of the agency in-
16 formation infrastructure under section 245(b)(2)(A)
17 of the Homeland Security Act of 2002, the Chief In-
18 formation Security Officer may deem the require-
19 ments of paragraph (1) satisfied for the year in
20 which the operational evaluation described under
21 this paragraph is conducted.

22 “(c) CORRECTIVE MEASURES MITIGATION AND RE-
23 MEDIATION PLANS.—

24 “(1) IN GENERAL.—In consultation with the
25 Director of the National Center for Cybersecurity

1 and Communications and the Chief Information Of-
2 ficer, Chief Information Security Officers shall reme-
3 diate or mitigate vulnerabilities in accordance with
4 this subsection.

5 “(2) RISK-BASED PLAN.—After an operational
6 evaluation is conducted under this section or under
7 section 245(b) of the Homeland Security Act of
8 2002, the agency shall submit to the Director of the
9 National Center for Cybersecurity and Communica-
10 tions in a timely fashion a risk-based plan for ad-
11 dressing recommendations and mitigating and reme-
12 diating vulnerabilities identified as a result of such
13 operational evaluation, including a timeline and
14 budget for implementing such plan.

15 “(3) APPROVAL OR DISAPPROVAL.—Not later
16 than 15 days after receiving a plan submitted under
17 paragraph (2), the Director of the National Center
18 for Cybersecurity and Communications shall—

19 “(A) approve or disprove the agency plan;

20 and

21 “(B) comment on the adequacy and effec-
22 tiveness of the plan.

23 “(4) ISOLATION FROM INFRASTRUCTURE.—

24 “(A) IN GENERAL.—The Director of the
25 National Center for Cybersecurity and Commu-

1 nications may, consistent with the contingency
2 or continuity of operation plans applicable to
3 such agency information infrastructure, order
4 the isolation of any component of the Federal
5 information infrastructure from any other Fed-
6 eral information infrastructure, if—

7 “(i) an agency does not implement
8 measures in a risk-based plan approved
9 under this subsection; and

10 “(ii) the failure to comply presents a
11 significant danger to the Federal informa-
12 tion infrastructure.

13 “(B) DURATION.—An isolation under sub-
14 paragraph (A) shall remain in effect until—

15 “(i) the Director of the National Cen-
16 ter for Cybersecurity and Communications
17 determines that corrective measures have
18 been implemented; or

19 “(ii) an updated risk-based plan is ap-
20 proved by the Director of the National
21 Center for Cybersecurity and Communica-
22 tions and implemented by the agency.

23 “(d) OPERATIONAL GUIDANCE.—The Director of the
24 National Center for Cybersecurity and Communications
25 shall—

1 “(1) not later than 180 days after the date of
 2 enactment of the Cybersecurity and Internet Free-
 3 dom Act of 2011, develop operational guidance for
 4 operational evaluations as required under this sec-
 5 tion that are risk-based and cost effective; and

6 “(2) periodically evaluate and ensure informa-
 7 tion is available on an automated and continuous
 8 basis through the system required under section
 9 3552(a)(3)(D) to Congress on—

10 “(A) the adequacy and effectiveness of the
 11 operational evaluations conducted under this
 12 section or section 245(b) of the Homeland Se-
 13 curity Act of 2002; and

14 “(B) possible executive and legislative ac-
 15 tions for cost-effectively managing the risks to
 16 the Federal information infrastructure.

17 **“§ 3555. Federal Information Security Taskforce**

18 “(a) ESTABLISHMENT.—There is established in the
 19 executive branch a Federal Information Security
 20 Taskforce.

21 “(b) MEMBERSHIP.—The members of the Federal In-
 22 formation Security Taskforce shall be full-time senior Gov-
 23 ernment employees and shall be as follows:

24 “(1) The Director of the National Center for
 25 Cybersecurity and Communications.

1 “(2) The Administrator of the Office of Elec-
2 tronic Government of the Office of Management and
3 Budget.

4 “(3) The Chief Information Security Officer of
5 each agency described under section 901(b) of title
6 31.

7 “(4) The Chief Information Security Officer of
8 the Department of the Army, the Department of the
9 Navy, and the Department of the Air Force.

10 “(5) A representative from the Office of Cyber-
11 space Policy.

12 “(6) A representative from the Office of the Di-
13 rector of National Intelligence.

14 “(7) A representative from the United States
15 Cyber Command.

16 “(8) A representative from the National Secu-
17 rity Agency.

18 “(9) A representative from the United States
19 Computer Emergency Readiness Team.

20 “(10) A representative from the Intelligence
21 Community Incident Response Center.

22 “(11) A representative from the Committee on
23 National Security Systems.

24 “(12) A representative from the National Insti-
25 tute for Standards and Technology.

1 “(13) A representative from the Council of In-
2 spectors General on Integrity and Efficiency.

3 “(14) A representative from State and local
4 government.

5 “(15) Any other officer or employee of the
6 United States designated by the chairperson.

7 “(c) CHAIRPERSON AND VICE-CHAIRPERSON.—

8 “(1) CHAIRPERSON.—The Director of the Na-
9 tional Center for Cybersecurity and Communications
10 shall act as chairperson of the Federal Information
11 Security Taskforce.

12 “(2) VICE-CHAIRPERSON.—The vice-chairperson
13 of the Federal Information Security Taskforce
14 shall—

15 “(A) be selected by the Federal Informa-
16 tion Security Taskforce from among its mem-
17 bers;

18 “(B) serve a 1-year term and may serve
19 multiple terms; and

20 “(C) serve as a liaison to the Chief Infor-
21 mation Officer, Council of the Inspectors Gen-
22 eral on Integrity and Efficiency, Committee on
23 National Security Systems, and other councils
24 or committees as appointed by the chairperson.

1 “(d) FUNCTIONS.—The Federal Information Security
2 Taskforce shall—

3 “(1) be the principal interagency forum for col-
4 laboration regarding best practices and recommenda-
5 tions for agency information security and the secu-
6 rity of the Federal information infrastructure;

7 “(2) assist in the development of and annually
8 evaluate guidance to fulfill the requirements under
9 sections 3554 and 3556;

10 “(3) share experiences and innovative ap-
11 proaches relating to threats against the Federal in-
12 formation infrastructure, information sharing and
13 information security best practices, penetration test-
14 ing regimes, and incident response, mitigation, and
15 remediation;

16 “(4) promote the development and use of stand-
17 ard performance indicators and measures for agency
18 information security that—

19 “(A) are outcome-based;

20 “(B) focus on risk management;

21 “(C) align with the business and program
22 goals of the agency;

23 “(D) measure improvements in the agency
24 security posture over time; and

1 “(E) reduce burdensome and inefficient
2 performance indicators and measures;

3 “(5) recommend to the Office of Personnel
4 Management the necessary qualifications to be es-
5 tablished for Chief Information Security Officers to
6 be capable of administering the functions described
7 under this subchapter including education, training,
8 and experience;

9 “(6) enhance information system processes by
10 establishing a prioritized baseline of information se-
11 curity measures and controls that can be continu-
12 ously monitored through automated mechanisms;
13 and

14 “(7) evaluate the effectiveness and efficiency of
15 any reporting and compliance requirements that are
16 required by law related to the information security
17 of Federal information infrastructure; and

18 “(8) submit proposed enhancements developed
19 under paragraphs (1) through (7) to the Director of
20 the National Center for Cybersecurity and Commu-
21 nications.

22 “(e) TERMINATION.—

23 “(1) IN GENERAL.—Except as provided under
24 paragraph (2), the Federal Information Security
25 Taskforce shall terminate 4 years after the date of

1 enactment of the Cybersecurity and Internet Free-
2 dom Act of 2011.

3 “(2) EXTENSION.—The President may—

4 “(A) extend the Federal Information Secu-
5 rity Taskforce by executive order; and

6 “(B) make more than 1 extension under
7 this paragraph for any period as the President
8 may determine.

9 **“§ 3556. Independent Assessments**

10 “(a) IN GENERAL.—

11 “(1) INSPECTORS GENERAL ASSESSMENTS.—
12 Not less than every 2 years, each agency with an In-
13 spector General appointed under the Inspector Gen-
14 eral Act of 1978 (5 U.S.C. App.) or any other law
15 shall assess the adequacy and effectiveness of the in-
16 formation security program developed under section
17 3553 (b) and (c), and evaluations conducted under
18 section 3554.

19 “(2) INDEPENDENT ASSESSMENTS.—For each
20 agency to which paragraph (1) does not apply, the
21 head of the agency shall engage an independent ex-
22 ternal auditor to perform the assessment.

23 “(b) STANDARDS.—The assessments required under
24 subsection (a) shall be performed in accordance with
25 standards developed by the Government Accountability

1 Office, in collaboration with the Council of Inspectors
2 General on Integrity and Efficiency and with assistance
3 from the Federal Information Security Taskforce.

4 “(c) EXISTING ASSESSMENTS.—The assessments re-
5 quired under this section may be based in whole or in part
6 on an audit, evaluation, or report relating to programs or
7 practices of the applicable agency.

8 “(d) REPORTING OF INFORMATION.—

9 “(1) INSPECTORS GENERAL REPORTING.—Each
10 Inspector General shall ensure information obtained
11 as a result of the assessment required under this
12 section, or any other relevant information, is—

13 “(A) provided to the head of the agency,
14 the agency Chief Information Security Officer,
15 and the agency Chief Information Officer; and

16 “(B) available through the system required
17 under section 3552(a)(3)(D) to Congress and
18 the Director of the National Center for Cyber-
19 security and Communications.

20 “(2) HEADS OF AGENCIES REPORTING.—If an
21 assessment described under subsection (a)(2) is per-
22 formed, the head of the agency shall comply with the
23 requirements of paragraph (1) (A) and (B).

1 **“§ 3557. Protection of Information**

2 “In complying with this subchapter, agencies, eval-
3 uators, and Inspectors General shall take appropriate ac-
4 tions to ensure the protection of information which, if dis-
5 closed, may adversely affect information security. Protec-
6 tions under this chapter shall be commensurate with the
7 risk and comply with all applicable laws and regulations.

8 **“§ 3558. Department of Defense and Central Intel-
9 ligence Agency systems**

10 “(a) IN GENERAL.—The authorities of the Director
11 of the National Center for Cybersecurity and Communica-
12 tions under this subchapter shall be delegated to—

13 “(1) the Secretary of Defense in the case of
14 systems described under subsection (b); and

15 “(2) the Director of the Central Intelligence
16 Agency in the case of systems described under sub-
17 section (c).

18 “(b) DEPARTMENT OF DEFENSE SYSTEMS.—The
19 systems described under this subsection are systems that
20 are operated by the Department of Defense, a contractor
21 of the Department of Defense, or another entity on behalf
22 of the Department of Defense that processes any informa-
23 tion the unauthorized access, use, disclosure, disruption,
24 modification, or destruction of which would have a debili-
25 tating impact on the mission of the Department of De-
26 fense.

1 “(c) CENTRAL INTELLIGENCE AGENCY SYSTEMS.—
 2 The systems described under this subsection are systems
 3 that are operated by the Central Intelligence Agency, a
 4 contractor of the Central Intelligence Agency, or another
 5 entity on behalf of the Central Intelligence Agency that
 6 processes any information the unauthorized access, use,
 7 disclosure, disruption, modification, or destruction of
 8 which would have a debilitating impact on the mission of
 9 the Central Intelligence Agency.”.

10 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

11 (1) TABLE OF SECTIONS.—The table of sections
 12 for chapter 35 of title 44, United States Code, is
 13 amended by striking the matter relating to sub-
 14 chapters II and III and inserting the following:

“SUBCHAPTER II—INFORMATION SECURITY

“3550. Purposes.

“3551. Definitions.

“3552. Authority and functions of the National Center for Cybersecurity and
 Communications.

“3553. Agency responsibilities.

“3554. Annual operational evaluation.

“3555. Federal Information Security Taskforce.

“3556. Independent assessments.

“3557. Protection of information.

“3558. Department of Defense and Central Intelligence Agency systems.”.

15 (2) OTHER REFERENCES.—

16 (A) Section 1001(c)(1)(A) of the Home-
 17 land Security Act of 2002 (6 U.S.C.
 18 511(c)(1)(A)) is amended by striking “section
 19 3532(3)” and inserting “section 3551(b)”.

1 (B) Section 2222(j)(6) of title 10, United
2 States Code, is amended by striking “section
3 3542(b)(2))” and inserting “section 3551(b)”.

4 (C) Section 2223(c)(3) of title 10, United
5 States Code, is amended, by striking “section
6 3542(b)(2))” and inserting “section 3551(b)”.

7 (D) Section 2315 of title 10, United States
8 Code, is amended by striking “section
9 3542(b)(2))” and inserting “section 3551(b)”.

10 (E) Section 20(a)(2) of the National Insti-
11 tute of Standards and Technology Act (15
12 U.S.C. 278g–3) is amended by striking “section
13 3532(b)(2)” and inserting “section 3551(b)”.

14 (F) Section 21(b)(2) of the National Insti-
15 tute of Standards and Technology Act (15
16 U.S.C. 278g–4(b)(2)) is amended by striking
17 “Institute and” and inserting “Institute, the
18 Director of the National Center on Cybersecu-
19 rity and Communications, and”.

20 (G) Section 21(b)(3) of the National Insti-
21 tute of Standards and Technology Act (15
22 U.S.C. 278g–4(b)(3)) is amended by inserting
23 “the Director of the National Center on Cyber-
24 security and Communications,” after “the Di-
25 rector of the National Security Agency,”.

1 (H) Section 8(d)(1) of the Cyber Security
 2 Research and Development Act (15 U.S.C.
 3 7406(d)(1)) is amended by striking “section
 4 3534(b)” and inserting “section 3553(b)”.

5 (3) HOMELAND SECURITY ACT OF 2002.—

6 (A) TITLE X.—The Homeland Security
 7 Act of 2002 (6 U.S.C. 101 et seq.) is amended
 8 by striking title X.

9 (B) TABLE OF CONTENTS.—The table of
 10 contents in section 1(b) of the Homeland Secu-
 11 rity Act of 2002 (6 U.S.C. 101 et seq.) is
 12 amended by striking the matter relating to title
 13 X.

14 (d) REPEAL OF OTHER STANDARDS.—

15 (1) IN GENERAL.—Section 11331 of title 40,
 16 United States Code, is repealed.

17 (2) TECHNICAL AND CONFORMING AMEND-
 18 MENTS.—

19 (A) Section 20(c)(3) of the National Insti-
 20 tute of Standards and Technology Act (15
 21 U.S.C. 278g–3(c)(3)) is amended by striking
 22 “under section 11331 of title 40, United States
 23 Code”.

24 (B) Section 20(d)(1) of the National Insti-
 25 tute of Standards and Technology Act (15

1 U.S.C. 278g–3(d)(1)) is amended by striking
2 “the Director of the Office of Management and
3 Budget for promulgation under section 11331
4 of title 40, United States Code” and inserting
5 “the Secretary of Commerce for promulgation”.

6 (C) Section 11302(d) of title 40, United
7 States Code, is amended by striking “under sec-
8 tion 11331 of this title and”.

9 (D) Section 1874A (e)(2)(A)(ii) of the So-
10 cial Security Act (42 U.S.C.1395kk-1
11 (e)(2)(A)(ii)) is amended by striking “section
12 11331 of title 40, United States Code” and in-
13 serting “section 3552 of title 44, United States
14 Code”.

15 (E) Section 3504(g)(2) of title 44, United
16 States Code, is amended by striking “section
17 11331 of title 40” and inserting “section 3552
18 of title 44”.

19 (F) Section 3504(h)(1) of title 44, United
20 States Code, is amended by inserting “, the Di-
21 rector of the National Center for Cybersecurity
22 and Communications,” after “the National In-
23 stitute of Standards and Technology”.

24 (G) Section 3504(h)(1)(B) of title 44,
25 United States Code, is amended by striking

1 “under section 11331 of title 40” and inserting
 2 “section 3552 of title 44”.

3 (H) Section 3518(d) of title 44, United
 4 States Code, is amended by striking “sections
 5 11331 and 11332” and inserting “section
 6 11332”.

7 (I) Section 3602(f)(8) of title 44, United
 8 States Code, is amended by striking “under sec-
 9 tion 11331 of title 40.

10 (J) Section 3603(f)(5) of title 44, United
 11 States Code, is amended by striking “and pro-
 12 mulgated under section 11331 of title 40,”.

13 **TITLE IV—RECRUITMENT AND** 14 **PROFESSIONAL DEVELOPMENT**

15 **SEC. 401. DEFINITIONS.**

16 In this title:

17 (1) CYBERSECURITY MISSION.—The term “cy-
 18 bersecurity mission” means the activities of the Fed-
 19 eral Government that encompass the full range of
 20 threat reduction, vulnerability reduction, deterrence,
 21 international engagement, incident response, resil-
 22 iency, and recovery policies and activities, including
 23 computer network operations, information assur-
 24 ance, law enforcement, diplomacy, military, and in-

1 telligence missions as such activities relate to the se-
2 curity and stability of cyberspace.

3 (2) FEDERAL AGENCY’S CYBERSECURITY MIS-
4 SION.—The term “Federal agency’s cybersecurity
5 mission” means, with respect to any Federal agency,
6 the portion of the cybersecurity mission that is the
7 responsibility of the Federal agency.

8 **SEC. 402. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

9 (a) IN GENERAL.—The Director of the Office of Per-
10 sonnel Management and the Director shall assess the
11 readiness and capacity of the Federal workforce to meet
12 the needs of the cybersecurity mission of the Federal Gov-
13 ernment.

14 (b) STRATEGY.—

15 (1) IN GENERAL.—The Director of the Office of
16 Personnel Management, in consultation with the Di-
17 rector and the Director of the Office of Management
18 and Budget, shall develop a comprehensive work-
19 force strategy that enhances the readiness, capacity,
20 training, and recruitment and retention of Federal
21 cybersecurity personnel.

22 (2) CONTENTS.—The strategy developed under
23 paragraph (1) shall include—

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

1 (B) 10-year and 20-year projections of
2 workforce needs.

3 (3) DATES FOR COMPLETION.—The strategy
4 under this subsection shall be—

5 (A) completed not later than 180 days
6 after the date of enactment of this Act; and

7 (B) updated as needed.

8 **SEC. 403. STRATEGIC CYBERSECURITY WORKFORCE PLAN-**
9 **NING.**

10 (a) FEDERAL AGENCY DEVELOPMENT OF STRA-
11 TEGIC CYBERSECURITY WORKFORCE PLANS.—Not later
12 than 180 days after the date of enactment of this Act and
13 in every subsequent year, and subject to subsection (c)(2),
14 the head of each Federal agency shall develop a strategic
15 cybersecurity workforce plan as part of the Federal agency
16 performance plan required under section 1115 of title 31,
17 United States Code.

18 (b) BASIS AND GUIDANCE FOR PLANS.—Each Fed-
19 eral agency shall develop a plan prepared under subsection
20 (a) on the basis of the assessment developed under section
21 402 and any subsequent guidance issued by the Director
22 of the Office of Personnel Management, in consultation
23 with the Director and the Director of the Office of Man-
24 agement and Budget.

25 (c) CONTENTS OF THE PLAN.—

1 (1) IN GENERAL.—Subject to paragraph (2),
2 each plan prepared under subsection (a) shall in-
3 clude—

4 (A) a description of the Federal agency’s
5 cybersecurity mission;

6 (B) a description and analysis, relating to
7 the specialized workforce needed by the Federal
8 agency to fulfill the Federal agency’s cybersecu-
9 rity mission, including—

10 (i) the workforce needs of the Federal
11 agency on the date of the report, and 10-
12 year and 20-year projections of workforce
13 needs;

14 (ii) hiring projections to meet work-
15 force needs, including, for at least a 2-year
16 period, specific occupation and grade lev-
17 els;

18 (iii) long-term and short-term stra-
19 tegic goals to address critical skills defi-
20 ciencies, including analysis of the numbers
21 of and reasons for attrition of employees;

22 (iv) recruitment strategies, including
23 the use of student internships, part-time
24 employment, student loan reimbursement,
25 and telework, to attract highly qualified

1 candidates from diverse backgrounds and
2 geographic locations;

3 (v) an assessment of the sources and
4 availability of individuals with needed ex-
5 pertise;

6 (vi) ways to streamline the hiring
7 process;

8 (vii) the barriers to recruiting and hir-
9 ing individuals qualified in cybersecurity
10 and recommendations to overcome the bar-
11 riers; and

12 (viii) a training and development plan,
13 consistent with the curriculum developed
14 under section 406, to enhance and improve
15 the knowledge of employees.

16 (2) FEDERAL AGENCIES WITH SMALL SPECIAL-
17 IZED WORKFORCE.—In accordance with guidance
18 issued under subsection (b), a Federal agency that
19 needs only a small specialized workforce to fulfill the
20 Federal agency's cybersecurity mission may, in lieu
21 of developing a separate strategic cybersecurity
22 workforce plan, present the workforce plan compo-
23 nent referred to in paragraph (1)(A) and those com-
24 ponents referred to in paragraph (1)(B) that are rel-
25 evant and appropriate to the circumstances of the

1 agency as part of the Federal agency performance
2 plan required under section 1115 of title 31, United
3 States Code.

4 **SEC. 404. CYBERSECURITY OCCUPATION CLASSIFICATIONS.**

5 (a) IN GENERAL.—Not later than 1 year after the
6 date of enactment of this Act, the Director of the Office
7 of Personnel Management, in coordination with the Direc-
8 tor, shall develop and issue comprehensive occupation clas-
9 sifications for Federal employees engaged in cybersecurity
10 missions.

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

16 **SEC. 405. MEASURES OF CYBERSECURITY HIRING EFFEC-**
17 **TIVENESS.**

18 (a) IN GENERAL.—The head of each Federal agency
19 shall measure, and collect information on, indicators of the
20 effectiveness of the recruitment and hiring by the Federal
21 agency of a workforce needed to fulfill the Federal agen-
22 cy's cybersecurity mission.

23 (b) TYPES OF INFORMATION.—The indicators of ef-
24 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

(B) exercise the authorities of the Office of Personnel Management and the head of an agency under that section with respect to retention bonuses paid under this subsection.

(2) LIMITATIONS ON AMOUNT OF ANNUAL BONUSES.—

(A) DEFINITIONS.—In this paragraph:

(i) MAXIMUM TOTAL PAY.—The term “maximum total pay” means—

(I) in the case of an employee described under subsection (c)(2)(B)(i), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code;

(II) in the case of an employee described under subsection (c)(2)(B)(ii)(I)(aa), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of 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 after the date of enactment
3 of this Act, the Director shall submit a report to the
4 appropriate committees of Congress with a plan for
5 the execution of the authorities provided under this
6 section.

7 (2) ANNUAL REPORT.—Not later than 6
8 months after the date of enactment of this Act, and
9 every year thereafter, the Director shall submit to
10 the appropriate committees of Congress a detailed
11 report that—

12 (A) discusses how the actions taken during
13 the period of the report are fulfilling the critical
14 hiring needs of the Center;

15 (B) assesses metrics relating to individuals
16 hired under the authority of this section, includ-
17 ing—

18 (i) the numbers of individuals hired;
19 (ii) the turnover in relevant positions;
20 (iii) with respect to each individual
21 hired—

22 (I) the position for which hired;
23 (II) the salary paid;
24 (III) any retention bonus paid
25 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 tion to the extent such statistics are
2 available; and
3 (C) includes rates of pay set in accordance
4 with subsection (c).

5 **TITLE V—OTHER PROVISIONS**

6 **SEC. 501. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

7 Subtitle D of title II of the Homeland Security Act
8 of 2002 (6 U.S.C. 161 et seq.) is amended by adding at
9 the end the following:

10 **“SEC. 238. CYBERSECURITY RESEARCH AND DEVELOP-** 11 **MENT.**

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

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

22 “(1) advance the development and accelerate
23 the deployment of more secure versions of funda-
24 mental Internet protocols and architectures, includ-

1 ing for the secure domain name addressing system
2 and routing security;

3 “(2) improve and create technologies for detect-
4 ing and analyzing attacks or intrusions, including
5 analysis of malicious software;

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

10 “(4) develop and support infrastructure and
11 tools to support cybersecurity research and develop-
12 ment efforts, including modeling, testbeds, and data
13 sets for assessment of new cybersecurity tech-
14 nologies;

15 “(5) assist the development and support of
16 technologies to reduce vulnerabilities in process con-
17 trol systems;

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

20 “(7) test, evaluate, and facilitate, with appro-
21 priate protections for any proprietary information
22 concerning the technologies, the transfer of tech-
23 nologies associated with the engineering of less vul-
24 nerable software and securing the information tech-
25 nology software development lifecycle;

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

3 “(9) assist the development of technologies de-
4 signed to increase the security and resiliency of tele-
5 communications networks;

6 “(10) advance the protection of privacy and
7 civil liberties in cybersecurity technology and prac-
8 tices; and

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

12 “(c) COORDINATION WITH OTHER RESEARCH INI-
13 TIATIVES.—The Under Secretary—

14 “(1) shall ensure that the research and develop-
15 ment program carried out under subsection (a) is
16 consistent with the national strategy to increase the
17 security and resilience of cyberspace developed by
18 the Director of Cyberspace Policy under section 101
19 of the Cybersecurity and Internet Freedom Act of
20 2011, or any succeeding strategy;

21 “(2) shall, to the extent practicable, coordinate
22 the research and development activities of the De-
23 partment with other ongoing research and develop-
24 ment security-related initiatives, including research
25 being conducted by—

1 “(A) the National Institute of Standards
2 and Technology;

3 “(B) the National Science Foundation;

4 “(C) the National Academy of Sciences;

5 “(D) other Federal agencies, as defined
6 under section 241;

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

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

13 “(3) shall carry out any research and develop-
14 ment project under subsection (a) through a reim-
15 bursable agreement with an appropriate Federal
16 agency, as defined under section 241, if the Federal
17 agency—

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

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

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

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

8 “(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIB-
9 ERTIES ISSUES.—

10 “(1) CONSULTATION.—In carrying out research
11 and development projects under subsection (a), the
12 Under Secretary shall consult with the Privacy Offi-
13 cer appointed under section 222 and the Officer for
14 Civil Rights and Civil Liberties of the Department
15 appointed under section 705.

16 “(2) PRIVACY IMPACT ASSESSMENTS.—In ac-
17 cordance with sections 222 and 705, the Privacy Of-
18 ficer shall conduct privacy impact assessments and
19 the Officer for Civil Rights and Civil Liberties shall
20 conduct reviews, as appropriate, for research and de-
21 velopment projects carried out under subsection (a)
22 that the Under Secretary determines could have an
23 impact on privacy, civil rights, or civil liberties.

1 **“SEC. 239. NATIONAL CYBERSECURITY ADVISORY COUNCIL.**

2 “(a) ESTABLISHMENT.—Not later than 90 days after
3 the date of enactment of this section, the Secretary shall
4 establish an advisory committee under section 871 on pri-
5 vate sector cybersecurity, to be known as the National Cy-
6 bersecurity Advisory Council (in this section referred to
7 as the ‘Council’).

8 “(b) RESPONSIBILITIES.—

9 “(1) IN GENERAL.—The Council shall advise
10 the Director of the National Center for Cybersecu-
11 rity and Communications on the implementation of
12 the cybersecurity provisions affecting the private sec-
13 tor under this subtitle and subtitle E.

14 “(2) INCENTIVES AND REGULATIONS.—The
15 Council shall advise the Director of the National
16 Center for Cybersecurity and Communications and
17 appropriate committees of Congress (as defined in
18 section 241) and any other congressional committee
19 with jurisdiction over the particular matter regard-
20 ing how market incentives and regulations may be
21 implemented to enhance the cybersecurity and eco-
22 nomic security of the Nation.

23 “(c) MEMBERSHIP.—

24 “(1) IN GENERAL.—The members of the Coun-
25 cil shall be appointed the Director of the National
26 Center for Cybersecurity and Communications and

1 shall, to the extent practicable, represent a geo-
2 graphic and substantive cross-section of owners and
3 operators of critical infrastructure and others with
4 expertise in cybersecurity, including, as appro-
5 priate—

6 “(A) representatives of covered critical in-
7 frastructure (as defined under section 241);

8 “(B) academic institutions with expertise
9 in cybersecurity;

10 “(C) Federal, State, and local government
11 agencies with expertise in cybersecurity;

12 “(D) a representative of the National Se-
13 curity Telecommunications Advisory Council, as
14 established by Executive Order 12382 (47 Fed.
15 Reg. 40531; relating to the establishment of the
16 advisory council), as amended by Executive
17 Order 13286 (68 Fed. Reg. 10619), as in effect
18 on August 3, 2009, or any successor entity;

19 “(E) a representative of the Communica-
20 tions Sector Coordinating Council, or any suc-
21 cessor entity;

22 “(F) a representative of the Information
23 Technology Sector Coordinating Council, or any
24 successor entity;

1 “(G) individuals, acting in their personal
2 capacity, with demonstrated technical expertise
3 in cybersecurity; and

4 “(H) such other individuals as the Director
5 determines to be appropriate, including owners
6 of small business concerns (as defined under
7 section 3 of the Small Business Act (15 U.S.C.
8 632)).

9 “(2) TERM.—The members of the Council shall
10 be appointed for 2 year terms and may be appointed
11 to consecutive terms.

12 “(3) LEADERSHIP.—The Chairperson and Vice-
13 Chairperson of the Council shall be selected by mem-
14 bers of the Council from among the members of the
15 Council and shall serve 2-year terms.

16 “(d) APPLICABILITY OF FEDERAL ADVISORY COM-
17 MITTEE ACT.—The Federal Advisory Committee Act (5
18 U.S.C. App.) shall not apply to the Council.”.

19 **SEC. 502. PRIORITIZED CRITICAL INFORMATION INFRA-**
20 **STRUCTURE.**

21 (a) IN GENERAL.—Section 210E(a)(2) of the Home-
22 land Security Act of 2002 (6 U.S.C. 124l(a)(2)) is amend-
23 ed—

24 (1) by striking “In accordance” and inserting
25 the following:

1 “(A) IN GENERAL.—In accordance”; and
2 (2) by adding at the end the following:

3 “(B) CONSIDERATIONS.—In establishing
4 and maintaining a list under subparagraph (A),
5 the Secretary, in coordination with the Director
6 of the National Center for Cybersecurity and
7 Communications, shall consider cyber risks and
8 consequences by sector, including—

9 “(i) the factors listed in section
10 248(a)(2);

11 “(ii) interdependencies between com-
12 ponents of covered critical infrastructure
13 (as defined under section 241); and

14 “(iii) the potential for the destruction
15 or disruption of the system or asset to
16 cause—

17 “(I) a mass casualty event which
18 includes an extraordinary number of
19 fatalities;

20 “(II) severe economic con-
21 sequences;

22 “(III) mass evacuations with a
23 prolonged absence; or

1 “(IV) severe degradation of na-
2 tional security capabilities, including
3 intelligence and defense functions.”.

4 (b) COVERED CRITICAL INFRASTRUCTURE.—Title II
5 of the Homeland Security Act of 2002 (6 U.S.C. 121 et
6 seq.) (as amended by section 201 of this Act) is further
7 amended by adding at the end the following:

8 **“SEC. 254. COVERED CRITICAL INFRASTRUCTURE.**

9 “(a) IDENTIFICATION OF COVERED CRITICAL INFRA-
10 STRUCTURE.—

11 “(1) IN GENERAL.—Subject to paragraphs (2)
12 and (3), the Secretary, in coordination with sector-
13 specific agencies and in consultation with the Na-
14 tional Cybersecurity Advisory Council and other ap-
15 propriate representatives of State and local govern-
16 ments and the private sector, shall establish and
17 maintain a list of systems or assets that constitute
18 covered critical infrastructure for purposes of this
19 subtitle.

20 “(2) REQUIREMENTS.—

21 “(A) IN GENERAL.—A system or asset
22 may not be identified as covered critical infra-
23 structure under this section unless such system
24 or asset meets each of the requirements under
25 subparagraph (B) (i), (ii), and (iii).

1 “(B) REQUIREMENTS.—The requirements
2 referred to under subparagraph (A) are that—

3 “(i) the destruction or the disruption
4 of the reliable operation of the system or
5 asset would cause national or regional cat-
6 astrophic effects identified under section
7 210E(a)(2)(B)(iii);

8 “(ii) the system or asset is on the
9 prioritized critical infrastructure list estab-
10 lished by the Secretary under section
11 210E(a)(2); and

12 “(iii)(I) the system or asset is a com-
13 ponent of the national information infra-
14 structure; or

15 “(II) the national information infra-
16 structure is essential to the reliable oper-
17 ation of the system or asset.

18 “(3) LIMITATION.—A system or asset may not
19 be identified as covered critical infrastructure under
20 this section based solely on activities protected by
21 the first amendment to the United States Constitu-
22 tion.

23 “(b) NOTIFICATION.—

24 “(1) IDENTIFICATION OF SYSTEM OR ASSET.—

25 If the Secretary identifies any system or asset as

1 covered critical infrastructure under subsection (a),
2 the Secretary shall promptly notify the owner or op-
3 erator of that system or asset of that identification.

4 “(2) SYSTEM OR ASSET NO LONGER COVERED
5 CRITICAL INFRASTRUCTURE.—If the Secretary de-
6 termines that any system or asset that was identi-
7 fied as covered critical infrastructure under sub-
8 section (a) no longer constitutes covered critical in-
9 frastructure, the Secretary shall promptly notify the
10 owner or operator of that system or asset of that de-
11 termination.

12 “(c) REDRESS.—

13 “(1) IN GENERAL.—Subject to paragraphs (2)
14 and (3), the Secretary shall develop a mechanism,
15 consistent with subchapter II of chapter 5 of title 5,
16 United States Code, for an owner or operator noti-
17 fied under subsection (b)(1) to appeal the identifica-
18 tion of a system or asset as covered critical infra-
19 structure under this section.

20 “(2) APPEAL TO FEDERAL COURT.—A civil ac-
21 tion seeking judicial review of a final agency action
22 taken under the mechanism developed under para-
23 graph (1) shall be filed in the United States District
24 Court for the District of Columbia.

1 “(3) COMPLIANCE.—The owner or operator of a
2 system or asset identified as covered critical infra-
3 structure shall comply with any requirement of this
4 subtitle relating to covered critical infrastructure
5 until such time as the system or asset is no longer
6 identified as covered critical infrastructure, based
7 on—

8 “(A) an appeal under paragraph (1);

9 “(B) a determination of the Secretary un-
10 related to an appeal; or

11 “(C) a final judgment entered in a civil ac-
12 tion seeking judicial review brought in accord-
13 ance with paragraph (2).

14 “(d) ADDITION OF SYSTEMS OR ASSETS.—

15 “(1) IN GENERAL.—The Secretary shall develop
16 a process under which any owner or operator of a
17 system or asset that may constitute covered critical
18 infrastructure may—

19 “(A) request that such system or asset be
20 identified by the Secretary as covered critical
21 infrastructure under this section; and

22 “(B) submit material supporting such a re-
23 quest to the Director of the Center for consider-
24 ation by the Secretary in carrying out this sec-
25 tion.

1 “(2) FINAL DECISION.—A decision to identify
 2 any system or asset as covered critical infrastructure
 3 based on a request submitted under this sub-
 4 section—

5 “(A) is committed to the sole, unreviewable
 6 discretion of the Secretary; and

7 “(B) shall not be subject to—

8 “(i) an appeal under subsection (c); or

9 “(ii) judicial review.”.

10 **SEC. 503. NATIONAL CENTER FOR CYBERSECURITY AND**
 11 **COMMUNICATIONS ACQUISITION AUTHORI-**
 12 **TIES.**

13 (a) IN GENERAL.—The National Center for Cyberse-
 14 curity and Communications is authorized to use the au-
 15 thorities under subsections (c)(1) and (d)(1)(B) of section
 16 2304 of title 10, United States Code, instead of the au-
 17 thorities under subsections (a)(1) and (b)(2) of section
 18 3304 of title 41, United States Code, subject to all other
 19 requirements of sections 3301 and 3304 of title 41, United
 20 States Code.

21 (b) GUIDELINES.—Not later than 90 days after the
 22 date of enactment of this Act, the chief procurement offi-
 23 cer of the Department of Homeland Security shall issue
 24 guidelines for use of the authority under subsection (a).

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

5 (d) REPORTING.—

6 (1) IN GENERAL.—On a semiannual basis, the
7 Director of the National Center for Cybersecurity
8 and Communications shall submit a report on use of
9 the authority granted by subsection (a) to—

10 (A) the Committee on Homeland Security
11 and Governmental Affairs of the Senate; and

12 (B) the Committee on Homeland Security
13 of the House of Representatives.

14 (2) CONTENTS.—Each report submitted under
15 paragraph (1) shall include, at a minimum—

16 (A) the number of contract actions taken
17 under the authority under subsection (a) during
18 the period covered by the report; and

19 (B) for each contract action described in
20 subparagraph (A)—

21 (i) the total dollar value of the con-
22 tract action;

23 (ii) a summary of the market research
24 conducted by the National Center for Cy-
25 bersecurity and Communications, including

1 a list of all offerors who were considered
2 and those who actually submitted bids, in
3 order to determine that use of the author-
4 ity was appropriate; and

5 (iii) a copy of the justification and ap-
6 proval documents required by section
7 3304(e) of title 41, United States Code.

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. 504. EVALUATION OF THE EFFECTIVE IMPLEMENTA-**
13 **TION OF OFFICE OF MANAGEMENT AND**
14 **BUDGET INFORMATION SECURITY RELATED**
15 **POLICIES AND DIRECTIVES.**

16 (a) IN GENERAL.—The Administrator for Electronic
17 Government and Information Technology, in coordination
18 with the Chief Information Officers Council, the Federal
19 Information Security Taskforce, and Council on Inspec-
20 tors General on Integrity and Efficiency, shall evaluate
21 agency adoption and effective implementation of appro-
22 priate information security related policies, memoranda,
23 and directives issued by the Office of Management and
24 Budget including—

1 (1) OMB Memorandum M-10-15, FY 2010
2 Reporting Instructions for the Federal Information
3 Security Management Act and Agency Privacy Man-
4 agement, issued April 21, 2010;

5 (2) OMB Memorandum M-09-32, Update on
6 the Trusted Internet Connections Initiative, issued
7 September 17, 2009;

8 (3) OMB Memorandum M-09-02, Information
9 Technology Management Structure and Governance
10 Framework, issued October 21, 2008;

11 (4) OMB Memorandum M-08-23, Securing the
12 Federal Government's Domain Name System Infra-
13 structure, issued April 22, 2008;

14 (5) OMB Memorandum M-08-22, Guidance on
15 the Federal Desktop Core Configuration (FDCC),
16 issued August 11, 2008;

17 (6) OMB Memorandum M-07-16, Safe-
18 guarding Against and Responding to the Breach of
19 Personally Identifiable Information, issued May 22,
20 2007;

21 (7) OMB Memorandum M-07-06, Validating
22 and Monitoring Agency Issuance of Personal Iden-
23 tity Verification Credentials, issued January 11,
24 2007;

1 (8) OMB Memorandum M-04-26, Personal
2 Use Policies and “File Sharing” Technology, issued
3 September 8, 2004; and

4 (9) OMB Memorandum M-03-22, OMB Guid-
5 ance for Implementing the Privacy Provisions of the
6 E-Government Act of 2002, issued September 26,
7 2003.

8 (b) REPORT.—Not later than 1 year after the date
9 of enactment of this Act, the Office of Management and
10 Budget shall submit a report on the evaluation required
11 under subsection (a) to the appropriate congressional com-
12 mittees which shall include—

13 (1) an examination of whether Federal agencies
14 have effectively implemented information security
15 policies;

16 (2) identification of and reasons why Federal
17 agencies are not in compliance with information se-
18 curity policies;

19 (3) the extent to which contractors working on
20 behalf of Federal agencies are in compliance and ef-
21 fectively implementing information security policies;
22 and

23 (4) recommended legislative and executive
24 branch actions.

1 **SEC. 505. TECHNICAL AND CONFORMING AMENDMENTS.**

2 (a) **ELIMINATION OF ASSISTANT SECRETARY FOR**
 3 **CYBERSECURITY AND COMMUNICATIONS.**—The Homeland
 4 Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

5 (1) in section 103(a)(8) (6 U.S.C. 113(a)(8)),
 6 by striking “, cybersecurity,”;

7 (2) in section 514 (6 U.S.C. 321c)—

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

9 (B) by redesignating subsection (c) as sub-
 10 section (b); and

11 (3) in section 1801(b) (6 U.S.C. 571(b)), by
 12 striking “shall report to the Assistant Secretary for
 13 Cybersecurity and Communications” and inserting
 14 “shall report to the Director of the National Center
 15 for Cybersecurity and Communications”.

16 (b) **CIO COUNCIL.**—Section 3603(b) of title 44,
 17 United States Code, is amended—

18 (1) by redesignating paragraph (7) as para-
 19 graph (8); and

20 (2) by inserting after paragraph (6) the fol-
 21 lowing:

22 “(7) The Director of the National Center for
 23 Cybersecurity and Communications.”.

24 (c) **REPEAL.**—The Homeland Security Act of 2002
 25 (6 U.S.C. 101 et seq.) is amended—

26 (1) by striking section 223 (6 U.S.C. 143); and

1 (2) by redesignating sections 224 and 225 (6
2 U.S.C. 144 and 145) as sections 223 and 224, re-
3 spectively.

4 (d) TECHNICAL CORRECTION.—Section 1802(a) of
5 the Homeland Security Act of 2002 (6 U.S.C. 572(a)) is
6 amended in the matter preceding paragraph (1) by strik-
7 ing “Department of”.

8 (e) EXECUTIVE SCHEDULE POSITION.—Section 5313
9 of title 5, United States Code, is amended by adding at
10 the end the following:

11 “Director of the National Center for Cybersecurity
12 and Communications.”.

13 (f) TABLE OF CONTENTS.—The table of contents in
14 section 1(b) of the Homeland Security Act of 2002 (6
15 U.S.C. 101 et seq.) is amended—

16 (1) by striking the items relating to sections
17 223, 224, and 225 and inserting the following:

“Sec. 223. NET guard.

“Sec. 224. Cyber Security Enhancements Act of 2002.”;

18 and

19 (2) by inserting after the item relating to sec-
20 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 Cybersecurity and Communications.
- “Sec. 246. Information sharing.
- “Sec. 247. Private sector assistance.
- “Sec. 248. Cyber risks to covered critical infrastructure.
- “Sec. 249. National cyber emergencies.
- “Sec. 250. Enforcement.
- “Sec. 251. Protection of information.
- “Sec. 252. Sector-specific agencies.
- “Sec. 253. Strategy for Federal cybersecurity supply chain management.
- “Sec. 254. Covered critical infrastructure.”.

