

112TH CONGRESS
2D SESSION

S. 2151

To improve information security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 1, 2012

Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To improve information security, and for other purposes.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Strengthening and Enhancing Cybersecurity by Using
6 Research, Education, Information, and Technology Act of
7 2012” or “SECURE IT”.

8 (b) TABLE OF CONTENTS.—The table of contents of
9 this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—FACILITATING SHARING OF CYBER THREAT
INFORMATION

- Sec. 101. Definitions.
- Sec. 102. Authorization to share cyber threat information.
- Sec. 103. Information Sharing by the Federal government.
- Sec. 104. Report on implementation.
- Sec. 105. Technical amendments.
- Sec. 106. Access to classified information.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY
POLICY

- Sec. 201. Coordination of Federal information security policy.
- Sec. 202. Management of information technology.
- Sec. 203. No new funding.
- Sec. 204. Technical and conforming amendments.

TITLE III—CRIMINAL PENALTIES

- Sec. 301. Penalties for fraud and related activity in connection with computers.
- Sec. 302. Trafficking in passwords.
- Sec. 303. Conspiracy and attempted computer fraud offenses.
- Sec. 304. Criminal and civil forfeiture for fraud and related activity in connection with computers.
- Sec. 305. Damage to critical infrastructure computers.
- Sec. 306. Limitation on actions involving unauthorized use.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

- Sec. 401. National High-Performance Computing Program planning and coordination.
- Sec. 402. Research in areas of national importance.
- Sec. 403. Program improvements.
- Sec. 404. Improving education of networking and information technology, including high performance computing.
- Sec. 405. Conforming and technical amendments to the High-Performance Computing Act of 1991.
- Sec. 406. Federal cyber scholarship-for-service program.
- Sec. 407. Study and analysis of certification and training of information infrastructure professionals.
- Sec. 408. Cybersecurity strategic research and development plan.
- Sec. 409. International cybersecurity technical standards.
- Sec. 410. Identity management research and development.
- Sec. 411. Federal cybersecurity research and development.

1 **TITLE I—FACILITATING SHAR-**
2 **ING OF CYBER THREAT IN-**
3 **FORMATION**

4 **SEC. 101. DEFINITIONS.**

5 In this title:

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

4 (2) ANTITRUST LAWS.—The term “antitrust
5 laws”—

6 (A) has the meaning given the term in sec-
7 tion 1(a) of the Clayton Act (15 U.S.C. 12(a));

8 (B) includes section 5 of the Federal
9 Trade Commission Act (15 U.S.C. 45) to the
10 extent that section 5 of that Act applies to un-
11 fair methods of competition; and

12 (C) includes any State law that has the
13 same intent and effect as the laws under sub-
14 paragraphs (A) and (B).

15 (3) COUNTERMEASURE.—The term “counter-
16 measure” means an automated or a manual action
17 with defensive intent to mitigate cyber threats.

18 (4) CYBER THREAT INFORMATION.—The term
19 “cyber threat information” means information that
20 may be indicative of or describes—

21 (A) a technical or operation vulnerability
22 or a cyber threat mitigation measure;

23 (B) an action or operation to mitigate a
24 cyber threat;

1 (C) malicious reconnaissance, including
2 anomalous patterns of network activity that ap-
3 pear to be transmitted for the purpose of gath-
4 ering technical information related to a cyberse-
5 curity threat;

6 (D) a method of defeating a technical con-
7 trol;

8 (E) a method of defeating an operational
9 control;

10 (F) network activity or protocols known to
11 be associated with a malicious cyber actor or
12 that may signify malicious intent;

13 (G) a method of causing a user with legiti-
14 mate access to an information system or infor-
15 mation that is stored on, processed by, or
16 transiting an information system to inadvert-
17 ently enable the defeat of a technical or oper-
18 ational control;

19 (H) any other attribute of a cybersecurity
20 threat or information that would foster situa-
21 tional awareness of the United States security
22 posture, if disclosure of such attribute or infor-
23 mation is not otherwise prohibited by law;

24 (I) the actual or potential harm caused by
25 a cyber incident, including information

1 exfiltrated when it is necessary in order to iden-
2 tify or describe a cybersecurity threat; or

3 (J) any combination thereof.

4 (5) CYBERSECURITY CENTER.—The term “cy-
5 bersecurity center” means the Department of De-
6 fense Cyber Crime Center, the Intelligence Commu-
7 nity Incident Response Center, the United States
8 Cyber Command Joint Operations Center, the Na-
9 tional Cyber Investigative Joint Task Force, the Na-
10 tional Security Agency/Central Security Service
11 Threat Operations Center, the National Cybersecu-
12 rity and Communications Integration Center, and
13 any successor center.

14 (6) CYBERSECURITY SYSTEM.—The term “cy-
15 bersecurity system” means a system designed or em-
16 ployed to ensure the integrity, confidentiality, or
17 availability of, or to safeguard, a system or network,
18 including measures intended to protect a system or
19 network from—

20 (A) efforts to degrade, disrupt, or destroy
21 such system or network; or

22 (B) theft or misappropriations of private
23 or government information, intellectual prop-
24 erty, or personally identifiable information.

1 (7) ENTITY.—The term “entity” means any
2 private entity, non-Federal government agency or
3 department, or State, tribal, or local government
4 agency or department (including an officer, em-
5 ployee, or agent thereof).

6 (8) INFORMATION SECURITY.—The term “infor-
7 mation security” means protecting information and
8 information systems from disruption or unauthorized
9 access, use, disclosure, modification, or destruction
10 in order to provide—

11 (A) integrity, by guarding against im-
12 proper information modification or destruction,
13 including by ensuring information nonrepudi-
14 ation and authenticity;

15 (B) confidentiality, by preserving author-
16 ized restrictions on access and disclosure, in-
17 cluding means for protecting personal privacy
18 and proprietary information; or

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

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

24 (10) MALICIOUS RECONNAISSANCE.—The term
25 “malicious reconnaissance” means a method for ac-

1 tively probing or passively monitoring an information
2 system for the purpose of discerning technical
3 vulnerabilities of the information system, if such
4 method is associated with a known or suspected cy-
5 bersecurity threat.

6 (11) OPERATIONAL CONTROL.—The term
7 “operational control” means a security control for
8 an information system that primarily is implemented
9 and executed by people.

10 (12) OPERATIONAL VULNERABILITY.—The
11 term “operational vulnerability” means any attribute
12 of policy, process, or procedure that could enable or
13 facilitate the defeat of an operational control.

14 (13) PRIVATE ENTITY.—The term “private en-
15 tity” means any individual or any private group, or-
16 ganization, or corporation, including an officer, em-
17 ployee, or agent thereof.

18 (14) TECHNICAL CONTROL.—The term “tech-
19 nical control” means a hardware or software restric-
20 tion on, or audit of, access or use of an information
21 system or information that is stored on, processed
22 by, or transiting an information system that is in-
23 tended to ensure the confidentiality, integrity, or
24 availability of that system.

1 (15) **TECHNICAL VULNERABILITY.**—The term
2 “technical vulnerability” means any attribute of
3 hardware or software that could enable or facilitate
4 the defeat of a technical control.

5 **SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT IN-**
6 **FORMATION.**

7 (a) **VOLUNTARY DISCLOSURE.**—

8 (1) **PRIVATE ENTITIES.**—Notwithstanding any
9 other provision of law, a private entity may, for the
10 purpose of preventing, investigating, or otherwise
11 mitigating threats to information security, on its
12 own networks, or as authorized by another entity, on
13 such entity’s networks, employ countermeasures and
14 use cybersecurity systems in order to obtain, iden-
15 tify, or otherwise possess cyber threat information.

16 (2) **ENTITIES.**—Notwithstanding any other pro-
17 vision of law, an entity may disclose cyber threat in-
18 formation to—

19 (A) a cybersecurity center; or

20 (B) any other entity in order to assist with
21 preventing, investigating, or otherwise miti-
22 gating threats to information security.

23 (3) **INFORMATION SECURITY PROVIDERS.**—If
24 the cyber threat information described in paragraph
25 (1) is obtained, identified, or otherwise possessed in

1 the course of providing information security prod-
2 ucts or services under contract to another entity,
3 that entity shall, at any time prior to disclosure of
4 such information, be given a reasonable opportunity
5 to authorize or prevent such disclosure or to request
6 anonymization of such information.

7 (b) REQUIRED DISCLOSURE.—

8 (1) IN GENERAL.—An entity providing elec-
9 tronic communication services, remote computing
10 services, or cybersecurity services under contract to
11 a Federal agency or department shall immediately
12 provide to such agency or department, and may pro-
13 vide to a cybersecurity center, any cyber threat in-
14 formation directly related to such contract that is
15 obtained, identified, or otherwise possessed by such
16 entity.

17 (2) DISCLOSURE TO CYBERSECURITY CEN-
18 TERS.—A Federal agency or department receiving
19 cyber threat information under paragraph (1) shall
20 immediately disclose such information to a cyberse-
21 curity center.

22 (c) INFORMATION SHARED WITH OR PROVIDED TO
23 A CYBERSECURITY CENTER.—Cyber threat information
24 provided to a cybersecurity center under this section—

25 (1) may be disclosed to and used by—

1 (A) any Federal agency or department,
2 component, officer, employee, or agent of the
3 Federal government for a cybersecurity pur-
4 pose, a national security purpose, or in order to
5 prevent, investigate, or prosecute any of the of-
6 fenses listed in section 2516 of title 18, United
7 States Code; or

8 (B) an entity that is acting as a provider
9 of electronic communication services, remote
10 computing service, or cybersecurity services to a
11 Federal agency or department for purposes re-
12 lated to such services;

13 (2) may, with the prior written consent of the
14 entity submitting such information, be disclosed to
15 and used by a State, tribal, or local government or
16 government agency for the purpose of protecting in-
17 formation systems, or in furtherance of preventing,
18 investigating, or prosecuting a criminal act, except
19 that if the need for immediate disclosure prevents
20 obtaining written consent, such consent may be pro-
21 vided orally with subsequent documentation of such
22 consent;

23 (3) shall be considered the commercial, finan-
24 cial, or proprietary information of the entity pro-
25 viding such information to the Federal government

1 and any disclosure outside the Federal government
2 may only be made upon the prior written consent by
3 such entity and shall not constitute a waiver of any
4 applicable privilege or protection provided by law,
5 except that if the need for immediate disclosure pre-
6 vents obtaining written consent, such consent may
7 be provided orally with subsequent documentation of
8 such consent;

9 (4) shall be deemed voluntarily shared informa-
10 tion and exempt from disclosure under section 552
11 of title 5, United States Code, and any State, tribal,
12 or local law requiring disclosure of information or
13 records;

14 (5) shall be, without discretion, withheld from
15 the public under section 552(b)(3)(B) of title 5,
16 United States Code, and any State, tribal, or local
17 law requiring disclosure of information or records;

18 (6) shall not be subject to the rules of any Fed-
19 eral agency or department or any judicial doctrine
20 regarding ex parte communications with a decision-
21 making official;

22 (7) shall not, if subsequently provided to a
23 State, tribal, or local government or government
24 agency, otherwise be disclosed or distributed to any
25 entity by such State, tribal, or local government or

1 government agency without the prior written consent
2 of the entity submitting such information, notwith-
3 standing any State, tribal, or local law requiring dis-
4 closure of information or records, except that if the
5 need for immediate disclosure prevents obtaining
6 written consent, such consent may be provided orally
7 with subsequent documentation of such consent; and

8 (8) shall not be directly used by any Federal,
9 State, tribal, or local department or agency to regu-
10 late the lawful activities of an entity, including ac-
11 tivities relating to obtaining, identifying, or other-
12 wise possessing cyber threat information, except that
13 the procedures required to be developed and imple-
14 mented under this title shall not be considered regu-
15 lations within the meaning of this paragraph.

16 (d) PROCEDURES RELATING TO INFORMATION SHAR-
17 ING WITH A CYBERSECURITY CENTER.—Not later than
18 60 days after the date of enactment of this Act, the heads
19 of each department or agency containing a cybersecurity
20 center shall jointly develop, promulgate, and submit to
21 Congress procedures to ensure that cyber threat informa-
22 tion shared with or provided to—

23 (1) a cybersecurity center under this section—
24 (A) may be submitted to a cybersecurity
25 center by an entity, to the greatest extent pos-

1 sible, through a uniform, publicly available
2 process or format that is easily accessible on
3 the website of such cybersecurity center, and
4 that includes the ability to provide relevant de-
5 tails about the cyber threat information and
6 written consent to any subsequent disclosures
7 authorized by this paragraph;

8 (B) shall immediately be further shared
9 with each cybersecurity center in order to pre-
10 vent, investigate, or otherwise mitigate threats
11 to information security across the Federal gov-
12 ernment;

13 (C) is handled by the Federal government
14 in a reasonable manner, including consideration
15 of the need to protect the privacy and civil lib-
16 erties of individuals through anonymization or
17 other appropriate methods, while fully accom-
18 plishing the objectives of this title; and

19 (D) except as provided in this section, shall
20 only be used, disclosed, or handled in accord-
21 ance with the provisions of subsection (c); and

22 (2) a Federal agency or department under sub-
23 section (b) is provided immediately to a cybersecu-
24 rity center in order to prevent, investigate, or other-

1 wise mitigate threats to information security across
2 the Federal government.

3 (e) INFORMATION SHARED BETWEEN PRIVATE EN-
4 TITIES.—

5 (1) IN GENERAL.—A private entity sharing
6 cyber threat information with another private entity
7 under this title may restrict the use or sharing of
8 such information by such other private entity.

9 (2) FURTHER SHARING.—Cyber threat informa-
10 tion shared by any private entity with another pri-
11 vate entity under this title—

12 (A) shall only be further shared in accord-
13 ance with any restrictions placed on the sharing
14 of such information by the private entity au-
15 thorizing such sharing, such as appropriate
16 anonymization of such information; and

17 (B) may not be used by any private entity
18 to gain an unfair competitive advantage to the
19 detriment of the private entity authorizing the
20 sharing of such information, except that the
21 conduct described in paragraph (3) shall not
22 constitute unfair competitive conduct.

23 (3) ANTITRUST EXEMPTION.—The exchange or
24 provision of cyber threat information or assistance
25 between 2 or more private entities under this title

1 shall not be considered a violation of any provision
2 of antitrust laws if exchanged or provided in order
3 to assist with—

4 (A) facilitating the prevention, investiga-
5 tion, or mitigation of threats to information se-
6 curity; or

7 (B) communicating or disclosing of cyber
8 threat information to help prevent, investigate
9 or otherwise mitigate the effects of a threat to
10 information security.

11 (f) FEDERAL PREEMPTION.—

12 (1) IN GENERAL.—This section supersedes any
13 statute or other law of a State or political subdivi-
14 sion of a State that restricts or otherwise expressly
15 regulates an activity authorized under this section.

16 (2) STATE LAW ENFORCEMENT.—Nothing in
17 this section shall be construed to supercede any stat-
18 ute or other law of a State or political subdivision
19 of a State concerning the use of authorized law en-
20 forcement techniques.

21 (3) PUBLIC DISCLOSURE.—No information
22 shared with or provided to a State, tribal, or local
23 government or government agency pursuant to this
24 section shall be made publicly available pursuant to

1 any State, tribal, or local law requiring disclosure of
2 information or records.

3 (g) CIVIL AND CRIMINAL LIABILITY.—

4 (1) GENERAL PROTECTIONS.—

5 (A) PRIVATE ENTITIES.—No cause of ac-
6 tion shall lie or be maintained in any court
7 against any private entity for—

8 (i) the use of countermeasures and cy-
9 bersecurity systems as authorized by this
10 title;

11 (ii) the use, receipt, or disclosure of
12 any cyber threat information as authorized
13 by this title; or

14 (iii) the subsequent actions or inac-
15 tions of any lawful recipient of cyber threat
16 information provided by such private enti-
17 ty.

18 (B) ENTITIES.—No cause of action shall
19 lie or be maintained in any court against any
20 entity for—

21 (i) the use, receipt, or disclosure of
22 any cyber threat information as authorized
23 by this title; or

1 (ii) the subsequent actions or inac-
2 tions of any lawful recipient of cyber threat
3 information provided by such entity.

4 (2) CONSTRUCTION.—Nothing in this sub-
5 section shall be construed as creating any immunity
6 against, or otherwise affecting, any action brought
7 by the Federal government, or any agency or depart-
8 ment thereof, to enforce any law, executive order, or
9 procedure governing the appropriate handling, dis-
10 closure, and use of classified information.

11 (h) OTHERWISE LAWFUL DISCLOSURES.—Nothing
12 in this section shall be construed to limit or prohibit other-
13 wise lawful disclosures of communications, records, or
14 other information by a private entity to any other govern-
15 mental or private entity not covered under this section.

16 (i) WHISTLEBLOWER PROTECTION.—Nothing in this
17 Act shall be construed to preempt or preclude any em-
18 ployee from exercising rights currently provided under any
19 whistleblower law, rule, or regulation.

20 **SEC. 103. INFORMATION SHARING BY THE FEDERAL GOV-**
21 **ERNMENT.**

22 (a) CLASSIFIED INFORMATION.—

23 (1) PROCEDURES.—Consistent with the protec-
24 tion of intelligence sources and methods, and as oth-
25 erwise determined appropriate, the Director of Na-

1 tional Intelligence and the Secretary of Defense
2 shall, in consultation with the heads of the appro-
3 priate Federal departments or agencies, develop and
4 promulgate procedures to facilitate and promote—

5 (A) the immediate sharing of classified
6 cyber threat information in the possession of
7 the Federal government with appropriately
8 cleared representatives of any appropriate enti-
9 ty; and

10 (B) the declassification and immediate
11 sharing with any entity or, if appropriate, pub-
12 lic availability of cyber threat information in the
13 possession of the Federal government;

14 (2) HANDLING OF CLASSIFIED INFORMATION.—

15 The procedures developed under paragraph (1) shall
16 ensure that each entity receiving classified cyber
17 threat information pursuant to this section has ac-
18 knowledged in writing the ongoing obligation to com-
19 ply with all laws, executive orders, and procedures
20 concerning the appropriate handling, disclosure, or
21 use of classified information.

22 (b) UNCLASSIFIED CYBER THREAT INFORMATION.—

23 The heads of each department or agency containing a cy-
24 bersecurity center shall jointly develop and promulgate
25 procedures that ensure that, consistent with the provisions

1 of this section, unclassified cyber threat information in the
2 possession of the Federal government—

3 (1) is shared in an immediate and adequate
4 manner with appropriate entities; and

5 (2) if appropriate, is made publicly available.

6 (c) SUBMISSION TO CONGRESS.—Not later than 60
7 days after the date of enactment of this Act, the Director
8 of National Intelligence, in coordination with the appro-
9 priate head of a department or an agency containing a
10 cybersecurity center, shall submit the procedures required
11 by this section to Congress.

12 (d) UTILIZING EXISTING PROCESSES.—Procedures
13 developed under this section shall coordinate with existing
14 processes utilized by sector specific information sharing
15 and analysis centers.

16 **SEC. 104. REPORT ON IMPLEMENTATION.**

17 (a) CONTENT OF REPORT.—Not later than 1 year
18 after the date of enactment of this Act, and biennially
19 thereafter, the heads of each department or agency con-
20 taining a cybersecurity center shall jointly submit, in co-
21 ordination with the privacy and civil liberties officials of
22 such departments or agencies and the Privacy and Civil
23 Liberties Oversight Board, a detailed report to Congress
24 concerning the implementation of this title, including—

1 (1) an assessment of the sufficiency of the pro-
2 cedures developed under section 103 of this Act in
3 ensuring that cyber threat information in the posses-
4 sion of the Federal government is provided in an im-
5 mediate and adequate manner to appropriate entities
6 or, if appropriate, is made publicly available;

7 (2) an assessment of whether information has
8 been appropriately classified and an accounting of
9 the number of security clearances authorized by the
10 Federal government for purposes of this title;

11 (3) a review of the type of cyber threat infor-
12 mation shared with a cybersecurity center under sec-
13 tion 102 of this Act, including whether such infor-
14 mation meets the definition of cyber threat informa-
15 tion under section 101, the degree to which such in-
16 formation may impact the privacy and civil liberties
17 of individuals, and the adequacy of any steps taken
18 to reduce such impact;

19 (4) a review of actions taken by the Federal
20 government based on information provided to a cy-
21 bersecurity center under section 102 of this Act, in-
22 cluding the appropriateness of any subsequent use
23 under section 102(c)(1)(A) of this Act;

24 (5) a description of any violations of the re-
25 quirements of this title by the Federal government;

1 (6) with respect to an entity providing elec-
2 tronic communication services, remote computing
3 service, or cybersecurity services to a Federal agency
4 or department, a description of any violations of the
5 requirements of subsection (b) or (c) of section 102
6 of this Act related to the performance of such serv-
7 ices;

8 (7) a list of entities that received classified in-
9 formation from the Federal government under sec-
10 tion 103 of this Act and a description of any indica-
11 tion that such information may not have been appro-
12 priately handled;

13 (8) a description of any breach of information
14 security, if known, attributable to a specific failure
15 by any entity or the Federal government to act on
16 cyber threat information in the possession of such
17 entity or the Federal government that resulted in
18 substantial economic harm or injury to a specific en-
19 tity or the Federal government; and

20 (9) any recommendation for improvements or
21 modifications to the authorities under this title.

22 (b) FORM OF REPORT.—The report under subsection
23 (a) shall be submitted in unclassified form, but may in-
24 clude a classified annex.

1 **SEC. 105. TECHNICAL AMENDMENTS.**

2 Section 552(b) of title 5, United States Code, is
3 amended—

4 (1) in paragraph (8), by striking “or”;

5 (2) in paragraph (9), by striking “wells.” and
6 inserting “wells; or”; and

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

8 “(10) information shared with or provided to a
9 cybersecurity center under section 102 of title I of
10 the Strengthening and Enhancing Cybersecurity by
11 Using Research, Education, Information, and Tech-
12 nology Act of 2012.”.

13 **SEC. 106. ACCESS TO CLASSIFIED INFORMATION.**

14 (a) **AUTHORIZATION REQUIRED.**—No person shall be
15 provided with access to classified information (as defined
16 in section 6.1 of Executive Order 13526 (50 U.S.C. 435
17 note; relating to classified national security information))
18 relating to cyber security threats or cyber security
19 vulnerabilities under this title without the appropriate se-
20 curity clearances.

21 (b) **SECURITY CLEARANCES.**—The appropriate Fed-
22 eral agencies or departments shall, consistent with appli-
23 cable procedures and requirements, and if otherwise
24 deemed appropriate, assist an individual in timely obtain-
25 ing an appropriate security clearance where such indi-
26 vidual has been determined to be eligible for such clear-

1 ance and has a need-to-know (as defined in section 6.1
2 of that Executive Order) classified information to carry
3 out this title.

4 **TITLE II—COORDINATION OF**
5 **FEDERAL INFORMATION SE-**
6 **CURITY POLICY**

7 **SEC. 201. COORDINATION OF FEDERAL INFORMATION SE-**
8 **CURITY POLICY.**

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

12 “SUBCHAPTER II—INFORMATION SECURITY

13 “§ 3551. **Purposes**

14 “The purposes of this subchapter are—

15 “(1) to provide a comprehensive framework for
16 ensuring the effectiveness of information security
17 controls over information resources that support
18 Federal operations and assets;

19 “(2) to recognize the highly networked nature
20 of the current Federal computing environment and
21 provide effective government-wide management of
22 policies, directives, standards, and guidelines, as well
23 as effective and nimble oversight of and response to
24 information security risks, including coordination of
25 information security efforts throughout the Federal

1 civilian, national security, and law enforcement com-
2 munities;

3 “(3) to provide for development and mainte-
4 nance of controls required to protect agency infor-
5 mation and information systems and contribute to
6 the overall improvement of agency information secu-
7 rity posture;

8 “(4) to provide for the development of tools and
9 methods to assess and respond to real-time situa-
10 tional risk for Federal information system operations
11 and assets; and

12 “(5) to provide a mechanism for improving
13 agency information security programs through con-
14 tinuous monitoring of agency information systems
15 and streamlined reporting requirements rather than
16 overly prescriptive manual reporting.

17 **“§ 3552. Definitions**

18 “In this subchapter:

19 “(1) ADEQUATE SECURITY.—The term ‘ade-
20 quate security’ means security commensurate with
21 the risk and magnitude of the harm resulting from
22 the unauthorized access to or loss, misuse, destruc-
23 tion, or modification of information.

24 “(2) AGENCY.—The term ‘agency’ has the
25 meaning given the term in section 3502 of title 44.

1 “(3) CYBERSECURITY CENTER.—The term ‘cy-
2 bersecurity center’ means the Department of De-
3 fense Cyber Crime Center, the Intelligence Commu-
4 nity Incident Response Center, the United States
5 Cyber Command Joint Operations Center, the Na-
6 tional Cyber Investigative Joint Task Force, the Na-
7 tional Security Agency/Central Security Service
8 Threat Operations Center, the National Cybersecu-
9 rity and Communications Integration Center, and
10 any successor center.

11 “(4) CYBER THREAT INFORMATION.—The term
12 ‘cyber threat information’ means information that
13 may be indicative of or describes—

14 “(A) a technical or operation vulnerability
15 or a cyber threat mitigation measure;

16 “(B) an action or operation to mitigate a
17 cyber threat;

18 “(C) malicious reconnaissance, including
19 anomalous patterns of network activity that ap-
20 pear to be transmitted for the purpose of gath-
21 ering technical information related to a cyberse-
22 curity threat;

23 “(D) a method of defeating a technical
24 control;

1 “(E) a method of defeating an operational
2 control;

3 “(F) network activity or protocols known
4 to be associated with a malicious cyber actor or
5 that may signify malicious intent;

6 “(G) a method of causing a user with le-
7 gitimate access to an information system or in-
8 formation that is stored on, processed by, or
9 transiting an information system to inadvert-
10 ently enable the defeat of a technical or oper-
11 ational control;

12 “(H) any other attribute of a cybersecurity
13 threat or information that would foster situa-
14 tional awareness of the United States security
15 posture, if disclosure of such attribute or infor-
16 mation is not otherwise prohibited by law;

17 “(I) the actual or potential harm caused by
18 a cyber incident, including information
19 exfiltrated when it is necessary in order to iden-
20 tify or describe a cybersecurity threat; or

21 “(J) any combination thereof.

22 “(5) DIRECTOR.—The term ‘Director’ means
23 the Director of the Office of Management and Budg-
24 et unless otherwise specified.

1 “(6) ENVIRONMENT OF OPERATION.—The term
2 ‘environment of operation’ means the information
3 system and environment in which those systems op-
4 erate, including changing threats, vulnerabilities,
5 technologies, and missions and business practices.

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

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

14 “(A) actually or imminently jeopardizes
15 the integrity, confidentiality, or availability of
16 an information system or the information that
17 system controls, processes, stores, or transmits;
18 or

19 “(B) constitutes a violation of law or an
20 imminent threat of violation of a law, a security
21 policy, a security procedure, or an acceptable
22 use policy.

23 “(9) INFORMATION RESOURCES.—The term ‘in-
24 formation resources’ has the meaning given the term
25 in section 3502 of title 44.

1 “(10) INFORMATION SECURITY.—The term ‘in-
2 formation security’ means protecting information
3 and information systems from disruption or unau-
4 thorized access, use, disclosure, modification, or de-
5 struction in order to provide—

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

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

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

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

19 “(12) INFORMATION TECHNOLOGY.—The term
20 ‘information technology’ has the meaning given the
21 term in section 11101 of title 40.

22 “(13) MALICIOUS RECONNAISSANCE.—The term
23 ‘malicious reconnaissance’ means a method for ac-
24 tively probing or passively monitoring an information
25 system for the purpose of discerning technical

1 vulnerabilities of the information system, if such
2 method is associated with a known or suspected cy-
3 bersecurity threat.

4 “(14) NATIONAL SECURITY SYSTEM.—

5 “(A) IN GENERAL.—The term ‘national se-
6 curity system’ means any information system
7 (including any telecommunications system) used
8 or operated by an agency or by a contractor of
9 an agency, or other organization on behalf of an
10 agency—

11 “(i) the function, operation, or use of
12 which—

13 “(I) involves intelligence activi-
14 ties;

15 “(II) involves cryptologic activi-
16 ties related to national security;

17 “(III) involves command and
18 control of military forces;

19 “(IV) involves equipment that is
20 an integral part of a weapon or weap-
21 ons system; or

22 “(V) subject to subparagraph
23 (B), is critical to the direct fulfillment
24 of military or intelligence missions; or

1 “(ii) is protected at all times by proce-
2 dures established for information that have
3 been specifically authorized under criteria
4 established by an Executive Order or an
5 Act of Congress to be kept classified in the
6 interest of national defense or foreign pol-
7 icy.

8 “(B) LIMITATION.—Subparagraph
9 (A)(i)(V) does not include a system that is to
10 be used for routine administrative and business
11 applications (including payroll, finance, logis-
12 tics, and personnel management applications).

13 “(15) OPERATIONAL CONTROL.—The term
14 ‘operational control’ means a security control for an
15 information system that primarily is implemented
16 and executed by people.

17 “(16) PERSON.—The term ‘person’ has the
18 meaning given the term in section 3502 of title 44.

19 “(17) SECRETARY.—The term ‘Secretary’
20 means the Secretary of Commerce unless otherwise
21 specified.

22 “(18) SECURITY CONTROL.—The term ‘security
23 control’ means the management, operational, and
24 technical controls, including safeguards or counter-
25 measures, prescribed for an information system to

1 protect the confidentiality, integrity, and availability
2 of the system and its information.

3 “(19) TECHNICAL CONTROL.—The term ‘tech-
4 nical control’ means a hardware or software restric-
5 tion on, or audit of, access or use of an information
6 system or information that is stored on, processed
7 by, or transiting an information system that is in-
8 tended to ensure the confidentiality, integrity, or
9 availability of that system.

10 **“§ 3553. Federal information security authority and**
11 **coordination**

12 “(a) IN GENERAL.—The Secretary, in consultation
13 with the Secretary of Homeland Security, shall—

14 “(1) issue compulsory and binding policies and
15 directives governing agency information security op-
16 erations, and require implementation of such policies
17 and directives, including—

18 “(A) policies and directives consistent with
19 the standards and guidelines promulgated
20 under section 11331 of title 40 to identify and
21 provide information security protections
22 prioritized and commensurate with the risk and
23 impact resulting from the unauthorized access,
24 use, disclosure, disruption, modification, or de-
25 struction of—

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

3 “(ii) information systems used or op-
4 erated by an agency or by a contractor of
5 an agency or other organization on behalf
6 of an agency;

7 “(B) minimum operational requirements
8 for Federal Government to protect agency in-
9 formation systems and provide common situa-
10 tional awareness across all agency information
11 systems;

12 “(C) reporting requirements, consistent
13 with relevant law, regarding information secu-
14 rity incidents and cyber threat information;

15 “(D) requirements for agencywide informa-
16 tion security programs;

17 “(E) performance requirements and
18 metrics for the security of agency information
19 systems;

20 “(F) training requirements to ensure that
21 agencies are able to fully and timely comply
22 with the policies and directives issued by the
23 Secretary under this subchapter;

24 “(G) training requirements regarding pri-
25 vacy, civil rights, and civil liberties, and infor-

1 mation oversight for agency information secu-
2 rity personnel;

3 “(H) requirements for the annual reports
4 to the Secretary under section 3554(d);

5 “(I) any other information security oper-
6 ations or information security requirements as
7 determined by the Secretary in coordination
8 with relevant agency heads; and

9 “(J) coordinating the development of
10 standards and guidelines under section 20 of
11 the National Institute of Standards and Tech-
12 nology Act (15 U.S.C. 278g-3) with agencies
13 and offices operating or exercising control of
14 national security systems (including the Na-
15 tional Security Agency) to assure, to the max-
16 imum extent feasible, that such standards and
17 guidelines are complementary with standards
18 and guidelines developed for national security
19 systems;

20 “(2) review the agencywide information security
21 programs under section 3554; and

22 “(3) designate an individual or an entity at
23 each cybersecurity center, among other responsibil-
24 ities—

1 “(A) to receive reports and information
2 about information security incidents, cyber
3 threat information, and deterioration of security
4 control affecting agency information systems;
5 and

6 “(B) to act on or share the information
7 under subparagraph (A) in accordance with this
8 subchapter.

9 “(b) CONSIDERATIONS.—When issuing policies and
10 directives under subsection (a), the Secretary shall con-
11 sider any applicable standards or guidelines developed by
12 the National Institute of Standards and Technology under
13 section 11331 of title 40.

14 “(c) LIMITATION OF AUTHORITY.—The authorities
15 of the Secretary under this section shall not apply to na-
16 tional security systems. Information security policies, di-
17 rectives, standards and guidelines for national security
18 systems shall be overseen as directed by the President and,
19 in accordance with that direction, carried out under the
20 authority of the heads of agencies that operate or exercise
21 authority over such national security systems.

22 “(d) STATUTORY CONSTRUCTION.—Nothing in this
23 subchapter shall be construed to alter or amend any law
24 regarding the authority of any head of an agency over
25 such agency.

1 **“§ 3554. Agency responsibilities**

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

3 “(1) be responsible for—

4 “(A) complying with the policies and direc-
5 tives issued under section 3553;

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

10 “(i) information collected or main-
11 tained by the agency or by a contractor of
12 an agency or other organization on behalf
13 of an agency; and

14 “(ii) information systems used or op-
15 erated by an agency or by a contractor of
16 an agency or other organization on behalf
17 of an agency;

18 “(C) complying with the requirements of
19 this subchapter, including—

20 “(i) information security standards
21 and guidelines promulgated under section
22 11331 of title 40;

23 “(ii) for any national security systems
24 operated or controlled by that agency, in-
25 formation security policies, directives,

1 standards and guidelines issued as directed
2 by the President; and

3 “(iii) for any non-national security
4 systems operated or controlled by that
5 agency, information security policies, direc-
6 tives, standards and guidelines issued
7 under section 3553;

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

12 “(E) reporting and sharing, for an agency
13 operating or exercising control of a national se-
14 curity system, information about information
15 security incidents, cyber threat information,
16 and deterioration of security controls to the in-
17 dividual or entity designated at each cybersecu-
18 rity center and to other appropriate entities
19 consistent with policies and directives for na-
20 tional security systems issued as directed by the
21 President; and

22 “(F) reporting and sharing, for those
23 agencies operating or exercising control of non-
24 national security systems, information about in-
25 formation security incidents, cyber threat infor-

1 mation, and deterioration of security controls to
2 the individual or entity designated at each cy-
3 bersecurity center and to other appropriate en-
4 tities consistent with policies and directives for
5 non-national security systems as prescribed
6 under section 3553(a); including information to
7 assist the Secretary of Homeland Security with
8 carrying out the ongoing security analysis
9 under section 3555.

10 “(2) ensure that each senior agency official pro-
11 vides information security for the information and
12 information systems that support the operations and
13 assets under the senior agency official’s control, in-
14 cluding by—

15 “(A) assessing the risk and impact that
16 could result from the unauthorized access, use,
17 disclosure, disruption, modification, or destruc-
18 tion of such information or information sys-
19 tems;

20 “(B) determining the level of information
21 security appropriate to protect such information
22 and information systems in accordance with
23 policies and directives issued under section
24 3553(a), and standards and guidelines promul-
25 gated under section 11331 of title 40 for infor-

1 mation security classifications and related re-
2 quirements;

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

6 “(D) actively monitoring the effective im-
7 plementation of information security controls
8 and techniques; and

9 “(E) reporting information about informa-
10 tion security incidents, cyber threat informa-
11 tion, and deterioration of security controls in a
12 timely and adequate manner to the entity des-
13 ignated under section 3553(a)(3) in accordance
14 with paragraph (1);

15 “(3) assess and maintain the resiliency of infor-
16 mation technology systems critical to agency mission
17 and operations;

18 “(4) designate the agency Inspector General (or
19 an independent entity selected in consultation with
20 the Director and the Council of Inspectors General
21 on Integrity and Efficiency if the agency does not
22 have an Inspector General) to conduct the annual
23 independent evaluation required under section 3556,
24 and allow the agency Inspector General to contract

1 with an independent entity to perform such evalua-
2 tion;

3 “(5) delegate to the Chief Information Officer
4 or equivalent (or to a senior agency official who re-
5 ports to the Chief Information Officer or equiva-
6 lent)—

7 “(A) the authority and primary responsi-
8 bility to implement an agencywide information
9 security program; and

10 “(B) the authority to provide information
11 security for the information collected and main-
12 tained by the agency (or by a contractor, other
13 agency, or other source on behalf of the agency)
14 and for the information systems that support
15 the operations, assets, and mission of the agen-
16 cy (including any information system provided
17 or managed by a contractor, other agency, or
18 other source on behalf of the agency);

19 “(6) delegate to the appropriate agency official
20 (who is responsible for a particular agency system or
21 subsystem) the responsibility to ensure and enforce
22 compliance with all requirements of the agency’s
23 agencywide information security program in coordi-
24 nation with the Chief Information Officer or equiva-
25 lent (or the senior agency official who reports to the

1 Chief Information Officer or equivalent) under para-
2 graph (5);

3 “(7) ensure that an agency has trained per-
4 sonnel who have obtained any necessary security
5 clearances to permit them to assist the agency in
6 complying with this subchapter;

7 “(8) ensure that the Chief Information Officer
8 or equivalent (or the senior agency official who re-
9 ports to the Chief Information Officer or equivalent)
10 under paragraph (5), in coordination with other sen-
11 ior agency officials, reports to the agency head on
12 the effectiveness of the agencywide information secu-
13 rity program, including the progress of any remedial
14 actions; and

15 “(9) ensure that the Chief Information Officer
16 or equivalent (or the senior agency official who re-
17 ports to the Chief Information Officer or equivalent)
18 under paragraph (5) has the necessary qualifications
19 to administer the functions described in this sub-
20 chapter and has information security duties as a pri-
21 mary duty of that official.

22 “(b) CHIEF INFORMATION OFFICERS.—Each Chief
23 Information Officer or equivalent (or the senior agency of-
24 ficial who reports to the Chief Information Officer or
25 equivalent) under subsection (a)(5) shall—

1 “(1) establish and maintain an enterprise secu-
2 rity operations capability that on a continuous
3 basis—

4 “(A) detects, reports, contains, mitigates,
5 and responds to information security incidents
6 that impair adequate security of the agency’s
7 information or information system in a timely
8 manner and in accordance with the policies and
9 directives under section 3553; and

10 “(B) reports any information security inci-
11 dent under subparagraph (A) to the entity des-
12 ignated under section 3555;

13 “(2) develop, maintain, and oversee an agency-
14 wide information security program;

15 “(3) develop, maintain, and oversee information
16 security policies, procedures, and control techniques
17 to address applicable requirements, including re-
18 quirements under section 3553 of this title and sec-
19 tion 11331 of title 40; and

20 “(4) train and oversee the agency personnel
21 who have significant responsibility for information
22 security with respect to that responsibility.

23 “(c) AGENCYWIDE INFORMATION SECURITY PRO-
24 GRAMS.—

1 “(1) IN GENERAL.—Each agencywide informa-
2 tion security program under subsection (b)(2) shall
3 include—

4 “(A) security engineering throughout the
5 development and acquisition lifecycle;

6 “(B) security testing commensurate with
7 risk and impact;

8 “(C) mitigation of deterioration of security
9 controls commensurate with risk and impact;

10 “(D) risk-based continuous monitoring of
11 the operational status and security of agency
12 information systems to enable evaluation of the
13 effectiveness of and compliance with informa-
14 tion security policies, procedures, and practices,
15 including a relevant and appropriate selection of
16 security controls of information systems identi-
17 fied in the inventory under section 3505(c);

18 “(E) operation of appropriate technical ca-
19 pabilities in order to detect, mitigate, report,
20 and respond to information security incidents,
21 cyber threat information, and deterioration of
22 security controls in a manner that is consistent
23 with the policies and directives under section
24 3553, including—

1 “(i) mitigating risks associated with
2 such information security incidents;

3 “(ii) notifying and consulting with the
4 entity designated under section 3555; and

5 “(iii) notifying and consulting with, as
6 appropriate—

7 “(I) law enforcement and the rel-
8 evant Office of the Inspector General;
9 and

10 “(II) any other entity, in accord-
11 ance with law and as directed by the
12 President;

13 “(F) a process to ensure that remedial ac-
14 tion is taken to address any deficiencies in the
15 information security policies, procedures, and
16 practices of the agency; and

17 “(G) a plan and procedures to ensure the
18 continuity of operations for information systems
19 that support the operations and assets of the
20 agency.

21 “(2) RISK MANAGEMENT STRATEGIES.—Each
22 agencywide information security program under sub-
23 section (b)(2) shall include the development and
24 maintenance of a risk management strategy for in-

1 formation security. The risk management strategy
2 shall include—

3 “(A) consideration of information security
4 incidents, cyber threat information, and deterio-
5 ration of security controls; and

6 “(B) consideration of the consequences
7 that could result from the unauthorized access,
8 use, disclosure, disruption, modification, or de-
9 struction of information and information sys-
10 tems that support the operations and assets of
11 the agency, including any information system
12 provided or managed by a contractor, other
13 agency, or other source on behalf of the agency;

14 “(3) POLICIES AND PROCEDURES.—Each agen-
15 cywide information security program under sub-
16 section (b)(2) shall include policies and procedures
17 that—

18 “(A) are based on the risk management
19 strategy under paragraph (2);

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

22 “(C) ensure that cost-effective and ade-
23 quate information security is addressed
24 throughout the life cycle of each agency infor-
25 mation system; and

1 “(D) ensure compliance with—

2 “(i) this subchapter; and

3 “(ii) any other applicable require-
4 ments.

5 “(4) TRAINING REQUIREMENTS.—Each agency-
6 wide information security program under subsection
7 (b)(2) shall include information security, privacy,
8 civil rights, civil liberties, and information oversight
9 training that meets any applicable requirements
10 under section 3553. The training shall inform each
11 information security personnel that has access to
12 agency information systems (including contractors
13 and other users of information systems that support
14 the operations and assets of the agency) of—

15 “(A) the information security risks associ-
16 ated with the information security personnel’s
17 activities; and

18 “(B) the individual’s responsibility to com-
19 ply with the agency policies and procedures that
20 reduce the risks under subparagraph (A).

21 “(d) ANNUAL REPORT.—Each agency shall submit a
22 report annually to the Secretary of Homeland Security on
23 its agencywide information security program and informa-
24 tion systems.

1 **“§ 3555. Multiagency ongoing threat assessment**

2 “(a) PURPOSE.—The purpose of this section is to
3 provide a framework for each agency to provide to the des-
4 ignee of the Secretary of Homeland Security under sub-
5 section (b)—

6 “(1) timely and actionable cyber threat infor-
7 mation; and

8 “(2) information on the environment of oper-
9 ation of an agency information system.

10 “(b) DESIGNEE.—The Secretary of Homeland Secu-
11 rity shall designate an entity within the Department of
12 Homeland Security—

13 “(1) to conduct ongoing security analysis con-
14 cerning agency information systems—

15 “(A) based on cyber threat information;

16 “(B) based on agency information system
17 and environment of operation changes, includ-
18 ing—

19 “(i) an ongoing evaluation of the in-
20 formation system security controls; and

21 “(ii) the security state, risk level, and
22 environment of operation of an agency in-
23 formation system, including—

24 “(I) a change in risk level due to
25 a new cyber threat;

1 “(II) a change resulting from a
2 new technology;

3 “(III) a change resulting from
4 the agency’s mission; and

5 “(IV) a change resulting from
6 the business practice; and

7 “(C) using automated processes to the
8 maximum extent possible—

9 “(i) to increase information system se-
10 curity;

11 “(ii) to reduce paper-based reporting
12 requirements; and

13 “(iii) to maintain timely and action-
14 able knowledge of the state of the informa-
15 tion system security.

16 “(2) STANDARDS.—The National Institute of
17 Standards and Technology may promulgate stand-
18 ards, in coordination with the Secretary of Home-
19 land Security, to assist an agency with its duties
20 under this section.

21 “(3) COMPLIANCE.—The head of each appro-
22 priate agency shall be responsible for ensuring com-
23 pliance with this section. The Secretary of Home-
24 land Security, in consultation with the head of each
25 appropriate agency, shall—

1 “(A) monitor compliance under this sec-
2 tion;

3 “(B) develop a timeline for each agency—

4 “(i) to adopt any technology, system,
5 or method that facilitates continuous moni-
6 toring of an agency information system;
7 and

8 “(ii) to adopt any technology, system,
9 or method that satisfies a requirement
10 under this section.

11 “(4) LIMITATION OF AUTHORITY.—The au-
12 thorities of the Secretary of Homeland Security
13 under this section shall not apply to national secu-
14 rity systems.

15 “(5) REPORT.—Not later than 6 months after
16 the date of enactment of the Strengthening and En-
17 hancing Cybersecurity by Using Research, Edu-
18 cation, Information, and Technology Act of 2012,
19 the Secretary of Homeland Security shall report to
20 Congress each agency’s status toward implementing
21 this section.

22 **“§ 3556. Independent evaluations**

23 “(a) IN GENERAL.—The Council of Inspectors Gen-
24 eral on Integrity and Efficiency, in consultation with the
25 Director and the Secretary of Homeland Security, the Sec-

1 retary of Commerce, and the Secretary of Defense, shall
2 issue and maintain criteria for the timely, cost-effective,
3 risk-based, and independent evaluation of each agencywide
4 information security program (and practices) to determine
5 the effectiveness of the agencywide information security
6 program (and practices). The criteria shall include meas-
7 ures to assess any conflicts of interest in the performance
8 of the evaluation and whether the agencywide information
9 security program includes appropriate safeguards against
10 disclosure of information where such disclosure may ad-
11 versely affect information security.

12 “(b) ANNUAL INDEPENDENT EVALUATIONS.—Each
13 agency shall perform an annual independent evaluation of
14 its agencywide information security program (and prac-
15 tices) in accordance with the criteria under subsection (a).

16 “(c) DISTRIBUTION OF REPORTS.—Not later than 30
17 days after receiving an independent evaluation under sub-
18 section (b), each agency head shall transmit a copy of the
19 independent evaluation to the Secretary of Homeland Se-
20 curity, the Secretary of Commerce, and the Secretary of
21 Defense.

22 “(d) NATIONAL SECURITY SYSTEMS.—Evaluations
23 involving national security systems shall be conducted as
24 directed by President.

1 **“§ 3557. National security systems.**

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

5 “(1) provides information security protections
6 commensurate with the risk and magnitude of the
7 harm resulting from the unauthorized access, use,
8 disclosure, disruption, modification, or destruction of
9 the information contained in such system; and

10 “(2) implements information security policies
11 and practices as required by standards and guide-
12 lines for national security systems, issued in accord-
13 ance with law and as directed by the President.”.

14 (b) SAVINGS PROVISIONS.—

15 (1) POLICY AND COMPLIANCE GUIDANCE.—Pol-
16 icy and compliance guidance issued by the Director
17 before the date of enactment of this Act under sec-
18 tion 3543(a)(1) of title 44, United States Code (as
19 in effect on the day before the date of enactment of
20 this Act), shall continue in effect, according to its
21 terms, until modified, terminated, superseded, or re-
22 pealed pursuant to section 3553(a)(1) of title 44,
23 United States Code.

24 (2) STANDARDS AND GUIDELINES.—Standards
25 and guidelines issued by the Secretary of Commerce
26 or by the Director before the date of enactment of

1 this Act under section 11331(a)(1) of title 40,
2 United States Code, (as in effect on the day before
3 the date of enactment of this Act) shall continue in
4 effect, according to their terms, until modified, ter-
5 minated, superseded, or repealed pursuant to section
6 11331(a)(1) of title 40, United States Code, as
7 amended by this Act.

8 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

9 (1) CHAPTER ANALYSIS.—The chapter analysis
10 for chapter 35 of title 44, United States Code, is
11 amended—

12 (A) by striking the items relating to sec-
13 tions 3531 through 3538;

14 (B) by striking the items relating to sec-
15 tions 3541 through 3549; and

16 (C) by inserting the following:

“3551. Purposes.

“3552. Definitions.

“3553. Federal information security authority and coordination.

“3554. Agency responsibilities.

“3555. Multiagency ongoing threat assessment.

“3556. Independent evaluations.

“3557. National security systems.”.

17 (2) OTHER REFERENCES.—

18 (A) Section 1001(c)(1)(A) of the Home-
19 land Security Act of 2002 (6 U.S.C. 511(1)(A))
20 is amended by striking “section 3532(3)” and
21 inserting “section 3552”.

1 (B) Section 2222(j)(5) of title 10, United
2 States Code, is amended by striking “section
3 3542(b)(2)” and inserting “section 3552”.

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 3552”.

7 (D) Section 2315 of title 10, United States
8 Code, is amended by striking “section
9 3542(b)(2)” and inserting “section 3552”.

10 (E) Section 20 of the National Institute of
11 Standards and Technology Act (15 U.S.C.
12 278g–3) is amended—

13 (i) in subsection (a)(2), by striking
14 “section 3532(b)(2)” and inserting “sec-
15 tion 3552”;

16 (ii) in subsection (c)(3), by striking
17 “Director of the Office of Management and
18 Budget” and inserting “Secretary of Com-
19 merce”;

20 (iii) in subsection (d)(1), by striking
21 “Director of the Office of Management and
22 Budget” and inserting “Secretary of Com-
23 merce”;

24 (iv) in subsection (d)(8) by striking
25 “Director of the Office of Management and

1 Budget” and inserting “Secretary of Com-
2 merce”;

3 (v) in subsection (d)(8), by striking
4 “submitted to the Director” and inserting
5 “submitted to the Secretary”;

6 (vi) in subsection (e)(2), by striking
7 “section 3532(1) of such title” and insert-
8 ing “section 3552 of title 44”; and

9 (vii) in subsection (e)(5), by striking
10 “section 3532(b)(2) of such title” and in-
11 serting “section 3552 of title 44”.

12 (F) Section 8(d)(1) of the Cyber Security
13 Research and Development Act (15 U.S.C.
14 7406(d)(1)) is amended by striking “section
15 3534(b)” and inserting “section 3554(b)(2)”.

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

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

19 **“§ 11331. Responsibilities for Federal information sys-
20 tems standards**

21 “(a) STANDARDS AND GUIDELINES.—

22 “(1) AUTHORITY TO PRESCRIBE.—Except as
23 provided under paragraph (2), the Secretary of
24 Commerce shall prescribe standards and guidelines
25 pertaining to Federal information systems—

1 “(A) in consultation with the Secretary of
2 Homeland Security; and

3 “(B) on the basis of standards and guide-
4 lines developed by the National Institute of
5 Standards and Technology under paragraphs
6 (2) and (3) of section 20(a) of the National In-
7 stitute of Standards and Technology Act (15
8 U.S.C. 278g-3(a)(2) and (a)(3)).

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

14 “(b) MANDATORY STANDARDS AND GUIDELINES.—

15 “(1) AUTHORITY TO MAKE MANDATORY STAND-
16 ARDS AND GUIDELINES.—The Secretary of Com-
17 merce shall make standards and guidelines under
18 subsection (a)(1) compulsory and binding to the ex-
19 tent determined necessary by the Secretary of Com-
20 merce to improve the efficiency of operation or secu-
21 rity of Federal information systems.

22 “(2) REQUIRED MANDATORY STANDARDS AND
23 GUIDELINES.—

1 “(A) IN GENERAL.—Standards and guide-
2 lines under subsection (a)(1) shall include infor-
3 mation security standards that—

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

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

12 “(B) BINDING EFFECT.—Information se-
13 curity standards under subparagraph (A) shall
14 be compulsory and binding.

15 “(c) EXERCISE OF AUTHORITY.—To ensure fiscal
16 and policy consistency, the Secretary of Commerce shall
17 exercise the authority conferred by this section subject to
18 direction by the President and in coordination with the
19 Director.

20 “(d) APPLICATION OF MORE STRINGENT STAND-
21 ARDS AND GUIDELINES.—The head of an executive agen-
22 cy may employ standards for the cost-effective information
23 security for information systems within or under the su-
24 pervision of that agency that are more stringent than the
25 standards and guidelines the Secretary of Commerce pre-

1 scribes under this section if the more stringent standards
2 and guidelines—

3 “(1) contain at least the applicable standards
4 and guidelines made compulsory and binding by the
5 Secretary of Commerce; and

6 “(2) are otherwise consistent with the policies,
7 directives, and implementation memoranda issued
8 under section 3553(a) of title 44.

9 “(e) DECISIONS ON PROMULGATION OF STANDARDS
10 AND GUIDELINES.—The decision by the Secretary of
11 Commerce regarding the promulgation of any standard or
12 guideline under this section shall occur not later than 6
13 months after the date of submission of the proposed stand-
14 ard to the Secretary of Commerce by the National Insti-
15 tute of Standards and Technology under section 20 of the
16 National Institute of Standards and Technology Act (15
17 U.S.C. 278g-3).

18 “(f) NOTICE AND COMMENT.—A decision by the Sec-
19 retary of Commerce to significantly modify, or not promul-
20 gate, a proposed standard submitted to the Secretary by
21 the National Institute of Standards and Technology under
22 section 20 of the National Institute of Standards and
23 Technology Act (15 U.S.C. 278g-3) shall be made after
24 the public is given an opportunity to comment on the Sec-
25 retary’s proposed decision.

1 “(g) DEFINITIONS.—In this section:

2 “(1) FEDERAL INFORMATION SYSTEM.—The
3 term ‘Federal information system’ has the meaning
4 given the term in section 3552 of title 44.

5 “(2) INFORMATION SECURITY.—The term ‘in-
6 formation security’ has the meaning given the term
7 in section 3552 of title 44.

8 “(3) NATIONAL SECURITY SYSTEM.—The term
9 ‘national security system’ has the meaning given the
10 term in section 3552 of title 44.”.

11 **SEC. 203. NO NEW FUNDING.**

12 An applicable Federal agency shall carry out the pro-
13 visions of this title with existing facilities and funds other-
14 wise available, through such means as the head of the
15 agency considers appropriate.

16 **SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.**

17 Section 21(b) of the National Institute of Standards
18 and Technology Act (15 U.S.C. 278g-4(b)) is amended—

19 (1) in paragraph (2), by striking “and the Di-
20 rector of the Office of Management and Budget”
21 and inserting “, the Secretary of Commerce, and the
22 Secretary of Homeland Security”; and

23 (2) in paragraph (3), by inserting “, the Sec-
24 retary of Homeland Security,” after “the Secretary
25 of Commerce”.

1 **TITLE III—CRIMINAL PENALTIES**

2 **SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY**

3 **IN CONNECTION WITH COMPUTERS.**

4 Section 1030(c) of title 18, United States Code, is
5 amended to read as follows:

6 “(c) The punishment for an offense under subsection
7 (a) or (b) of this section is—

8 “(1) a fine under this title or imprisonment for
9 not more than 20 years, or both, in the case of an
10 offense under subsection (a)(1) of this section;

11 “(2)(A) except as provided in subparagraph
12 (B), a fine under this title or imprisonment for not
13 more than 3 years, or both, in the case of an offense
14 under subsection (a)(2); or

15 “(B) a fine under this title or imprison-
16 ment for not more than ten years, or both, in
17 the case of an offense under subsection (a)(2)
18 of this section, if—

19 “(i) the offense was committed for
20 purposes of commercial advantage or pri-
21 vate financial gain;

22 “(ii) the offense was committed in the
23 furtherance of any criminal or tortious act
24 in violation of the Constitution or laws of
25 the United States, or of any State; or

1 “(iii) the value of the information ob-
2 tained, or that would have been obtained if
3 the offense was completed, exceeds \$5,000;

4 “(3) a fine under this title or imprisonment for
5 not more than 10 years, or both, in the case of an
6 offense under subsection (a)(3) of this section;

7 “(4) a fine under this title or imprisonment of
8 not more than 20 years, or both, in the case of an
9 offense under subsection (a)(4) of this section;

10 “(5)(A) except as provided in subparagraph
11 (C), a fine under this title, imprisonment for not
12 more than 20 years, or both, in the case of an of-
13 fense under subsection (a)(5)(A) of this section, if
14 the offense caused—

15 “(i) loss to 1 or more persons during
16 any 1-year period (and, for purposes of an
17 investigation, prosecution, or other pro-
18 ceeding brought by the United States only,
19 loss resulting from a related course of con-
20 duct affecting 1 or more other protected
21 computers) aggregating at least \$5,000 in
22 value;

23 “(ii) the modification or impairment,
24 or potential modification or impairment, of

1 the medical examination, diagnosis, treat-
2 ment, or care of 1 or more individuals;
3 “(iii) physical injury to any person;
4 “(iv) a threat to public health or safe-
5 ty;
6 “(v) damage affecting a computer
7 used by, or on behalf of, an entity of the
8 United States Government in furtherance
9 of the administration of justice, national
10 defense, or national security; or
11 “(vi) damage affecting 10 or more
12 protected computers during any 1-year pe-
13 riod;
14 “(B) a fine under this title, imprisonment
15 for not more than 20 years, or both, in the case
16 of an offense under subsection (a)(5)(B), if the
17 offense caused a harm provided in clause (i)
18 through (vi) of subparagraph (A) of this sub-
19 section;
20 “(C) if the offender attempts to cause or
21 knowingly or recklessly causes death from con-
22 duct in violation of subsection (a)(5)(A), a fine
23 under this title, imprisonment for any term of
24 years or for life, or both;

1 “(D) a fine under this title, imprisonment
2 for not more than 10 years, or both, for any
3 other offense under subsection (a)(5);

4 “(E) a fine under this title or imprison-
5 ment for not more than 10 years, or both, in
6 the case of an offense under subsection (a)(6)
7 of this section; or

8 “(F) a fine under this title or imprison-
9 ment for not more than 10 years, or both, in
10 the case of an offense under subsection (a)(7)
11 of this section.”.

12 **SEC. 302. TRAFFICKING IN PASSWORDS.**

13 Section 1030(a)(6) of title 18, United States Code,
14 is amended to read as follows:

15 “(6) knowingly and with intent to defraud traf-
16 fics (as defined in section 1029) in any password or
17 similar information or means of access through
18 which a protected computer (as defined in subpara-
19 graphs (A) and (B) of subsection (e)(2)) may be
20 accessed without authorization.”.

21 **SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER**
22 **FRAUD OFFENSES.**

23 Section 1030(b) of title 18, United States Code, is
24 amended by inserting “as if for the completed offense”
25 after “punished as provided”.

1 **SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD**
2 **AND RELATED ACTIVITY IN CONNECTION**
3 **WITH COMPUTERS.**

4 Section 1030 of title 18, United States Code, is
5 amended by striking subsections (i) and (j) and inserting
6 the following:

7 “(i) CRIMINAL FORFEITURE.—

8 “(1) The court, in imposing sentence on any
9 person convicted of a violation of this section, or
10 convicted of conspiracy to violate this section, shall
11 order, in addition to any other sentence imposed and
12 irrespective of any provision of State law, that such
13 person forfeit to the United States—

14 “(A) such persons interest in any property,
15 real or personal, that was used, or intended to
16 be used, to commit or facilitate the commission
17 of such violation; and

18 “(B) any property, real or personal, consti-
19 tuting or derived from any gross proceeds, or
20 any property traceable to such property, that
21 such person obtained, directly or indirectly, as
22 a result of such violation.

23 “(2) The criminal forfeiture of property under
24 this subsection, including any seizure and disposition
25 of the property, and any related judicial or adminis-
26 trative proceeding, shall be governed by the provi-

1 sions of section 413 of the Comprehensive Drug
2 Abuse Prevention and Control Act of 1970 (21
3 U.S.C. 853), except subsection (d) of that section.

4 “(j) CIVIL FORFEITURE.—

5 “(1) The following shall be subject to forfeiture
6 to the United States and no property right, real or
7 personal, shall exist in them:

8 “(A) Any property, real or personal, that
9 was used, or intended to be used, to commit or
10 facilitate the commission of any violation of this
11 section, or a conspiracy to violate this section.

12 “(B) Any property, real or personal, con-
13 stituting or derived from any gross proceeds ob-
14 tained directly or indirectly, or any property
15 traceable to such property, as a result of the
16 commission of any violation of this section, or
17 a conspiracy to violate this section.

18 “(2) Seizures and forfeitures under this sub-
19 section shall be governed by the provisions in chap-
20 ter 46 relating to civil forfeitures, except that such
21 duties as are imposed on the Secretary of the Treas-
22 ury under the customs laws described in section
23 981(d) shall be performed by such officers, agents
24 and other persons as may be designated for that

1 purpose by the Secretary of Homeland Security or
2 the Attorney General.”.

3 **SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COM-**
4 **PUTERS.**

5 (a) IN GENERAL.—Chapter 47 of title 18, United
6 States Code, is amended by inserting after section 1030
7 the following:

8 **“§ 1030A. Aggravated damage to a critical infrastruc-**
9 **ture computer**

10 “(a) DEFINITIONS.—In this section—

11 “(1) the term ‘computer’ has the meaning given
12 the term in section 1030;

13 “(2) the term ‘critical infrastructure computer’
14 means a computer that manages or controls systems
15 or assets vital to national defense, national security,
16 national economic security, public health or safety,
17 or any combination of those matters, whether pub-
18 licly or privately owned or operated, including—

19 “(A) gas and oil production, storage, and
20 delivery systems;

21 “(B) water supply systems;

22 “(C) telecommunication networks;

23 “(D) electrical power delivery systems;

24 “(E) finance and banking systems;

25 “(F) emergency services;

1 “(G) transportation systems and services;
2 and

3 “(H) government operations that provide
4 essential services to the public; and

5 “(3) the term ‘damage’ has the meaning given
6 the term in section 1030.

7 “(b) OFFENSE.—It shall be unlawful, during and in
8 relation to a felony violation of section 1030, to knowingly
9 cause or attempt to cause damage to a critical infrastruc-
10 ture computer if the damage results in (or, in the case
11 of an attempt, if completed, would have resulted in) the
12 substantial impairment—

13 “(1) of the operation of the critical infrastruc-
14 ture computer; or

15 “(2) of the critical infrastructure associated
16 with the computer.

17 “(c) PENALTY.—Any person who violates subsection
18 (b) shall be—

19 “(1) fined under this title;

20 “(2) imprisoned for not less than 3 years but
21 not more than 20 years; or

22 “(3) penalized under paragraphs (1) and (2).

23 “(d) CONSECUTIVE SENTENCE.—Notwithstanding
24 any other provision of law—

1 “(1) a court shall not place on probation any
2 person convicted of a violation of this section;

3 “(2) except as provided in paragraph (4), no
4 term of imprisonment imposed on a person under
5 this section shall run concurrently with any other
6 term of imprisonment, including any term of impris-
7 onment imposed on the person under any other pro-
8 vision of law, including any term of imprisonment
9 imposed for a felony violation of section 1030;

10 “(3) in determining any term of imprisonment
11 to be imposed for a felony violation of section 1030,
12 a court shall not in any way reduce the term to be
13 imposed for such crime so as to compensate for, or
14 otherwise take into account, any separate term of
15 imprisonment imposed or to be imposed for a viola-
16 tion of this section; and

17 “(4) a term of imprisonment imposed on a per-
18 son for a violation of this section may, in the discre-
19 tion of the court, run concurrently, in whole or in
20 part, only with another term of imprisonment that
21 is imposed by the court at the same time on that
22 person for an additional violation of this section,
23 provided that such discretion shall be exercised in
24 accordance with any applicable guidelines and policy

1 statements issued by the United States Sentencing
2 Commission pursuant to section 994 of title 28.”.

3 (b) **TECHNICAL AND CONFORMING AMENDMENT.**—

4 The chapter analysis for chapter 47 of title 18, United
5 States Code, is amended by inserting after the item relat-
6 ing to section 1030 the following:

“1030A. Aggravated damage to a critical infrastructure computer.”.

7 **SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHOR-**
8 **IZED USE.**

9 Section 1030(e)(6) of title 18, United States Code,
10 is amended by striking “alter;” and inserting “alter, but
11 does not include access in violation of a contractual obliga-
12 tion or agreement, such as an acceptable use policy or
13 terms of service agreement, with an Internet service pro-
14 vider, Internet website, or non-government employer, if
15 such violation constitutes the sole basis for determining
16 that access to a protected computer is unauthorized;”.

17 **TITLE IV—CYBERSECURITY**
18 **RESEARCH AND DEVELOPMENT**

19 **SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING**
20 **PROGRAM PLANNING AND COORDINATION.**

21 (a) **GOALS AND PRIORITIES.**—Section 101 of the
22 High-Performance Computing Act of 1991 (15 U.S.C.
23 5511) is amended by adding at the end the following:

24 “(d) **GOALS AND PRIORITIES.**—The goals and prior-
25 ities for Federal high-performance computing research,

1 development, networking, and other activities under sub-
2 section (a)(2)(A) shall include—

3 “(1) encouraging and supporting mechanisms
4 for interdisciplinary research and development in
5 networking and information technology, including—

6 “(A) through collaborations across agen-
7 cies;

8 “(B) through collaborations across Pro-
9 gram Component Areas;

10 “(C) through collaborations with industry;

11 “(D) through collaborations with institu-
12 tions of higher education;

13 “(E) through collaborations with Federal
14 laboratories (as defined in section 4 of the Ste-
15 venson-Wylder Technology Innovation Act of
16 1980 (15 U.S.C. 3703)); and

17 “(F) through collaborations with inter-
18 national organizations;

19 “(2) addressing national, multi-agency, multi-
20 faceted challenges of national importance; and

21 “(3) fostering the transfer of research and de-
22 velopment results into new technologies and applica-
23 tions for the benefit of society.”.

24 (b) DEVELOPMENT OF STRATEGIC PLAN.—Section
25 101 of the High-Performance Computing Act of 1991 (15

1 U.S.C. 5511) is amended by adding at the end the fol-
2 lowing:

3 “(e) STRATEGIC PLAN.—

4 “(1) IN GENERAL.—Not later than 1 year after
5 the date of enactment of the Strengthening and En-
6 hancing Cybersecurity by Using Research, Edu-
7 cation, Information, and Technology Act of 2012,
8 the agencies under subsection (a)(3)(B), working
9 through the National Science and Technology Coun-
10 cil and with the assistance of the Office of Science
11 and Technology Policy shall develop a 5-year stra-
12 tegic plan to guide the activities under subsection
13 (a)(1).

14 “(2) CONTENTS.—The strategic plan shall
15 specify—

16 “(A) the near-term objectives for the Pro-
17 gram;

18 “(B) the long-term objectives for the Pro-
19 gram;

20 “(C) the anticipated time frame for achiev-
21 ing the near-term objectives;

22 “(D) the metrics that will be used to as-
23 sess any progress made toward achieving the
24 near-term objectives and the long-term objec-
25 tives; and

1 “(E) how the Program will achieve the
2 goals and priorities under subsection (d).

3 “(3) IMPLEMENTATION ROADMAP.—

4 “(A) IN GENERAL.—The agencies under
5 subsection (a)(3)(B) shall develop and annually
6 update an implementation roadmap for the
7 strategic plan.

8 “(B) REQUIREMENTS.—The information in
9 the implementation roadmap shall be coordi-
10 nated with the database under section 102(c)
11 and the annual report under section 101(a)(3).
12 The implementation roadmap shall—

13 “(i) specify the role of each Federal
14 agency in carrying out or sponsoring re-
15 search and development to meet the re-
16 search objectives of the strategic plan, in-
17 cluding a description of how progress to-
18 ward the research objectives will be evalu-
19 ated, with consideration of any relevant
20 recommendations of the advisory com-
21 mittee;

22 “(ii) specify the funding allocated to
23 each major research objective of the stra-
24 tegic plan and the source of funding by
25 agency for the current fiscal year; and

1 “(iii) estimate the funding required
2 for each major research objective of the
3 strategic plan for the next 3 fiscal years.

4 “(4) RECOMMENDATIONS.—The agencies under
5 subsection (a)(3)(B) shall take into consideration
6 when developing the strategic plan under paragraph
7 (1) the recommendations of—

8 “(A) the advisory committee under sub-
9 section (b); and

10 “(B) the stakeholders under section
11 102(a)(3).

12 “(5) REPORT TO CONGRESS.—The Director of
13 the Office of Science and Technology Policy shall
14 transmit the strategic plan under this subsection, in-
15 cluding the implementation roadmap and any up-
16 dates under paragraph (3), to—

17 “(A) the advisory committee under sub-
18 section (b);

19 “(B) the Committee on Commerce,
20 Science, and Transportation of the Senate; and

21 “(C) the Committee on Science and Tech-
22 nology of the House of Representatives.”.

23 (c) PERIODIC REVIEWS.—Section 101 of the High-
24 Performance Computing Act of 1991 (15 U.S.C. 5511)
25 is amended by adding at the end the following:

1 “(f) PERIODIC REVIEWS.—The agencies under sub-
2 section (a)(3)(B) shall—

3 “(1) periodically assess the contents and fund-
4 ing levels of the Program Component Areas and re-
5 structure the Program when warranted, taking into
6 consideration any relevant recommendations of the
7 advisory committee under subsection (b); and

8 “(2) ensure that the Program includes national,
9 multi-agency, multi-faceted research and develop-
10 ment activities, including activities described in sec-
11 tion 104.”.

12 (d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—
13 Section 101(a)(2) of the High-Performance Computing
14 Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

15 (1) by redesignating subparagraphs (E) and
16 (F) as subparagraphs (G) and (H), respectively; and

17 (2) by inserting after subparagraph (D) the fol-
18 lowing:

19 “(E) encourage and monitor the efforts of
20 the agencies participating in the Program to al-
21 locate the level of resources and management
22 attention necessary—

23 “(i) to ensure that the strategic plan
24 under subsection (e) is developed and exe-
25 cuted effectively; and

1 “(ii) to ensure that the objectives of
2 the Program are met;

3 “(F) working with the Office of Manage-
4 ment and Budget and in coordination with the
5 creation of the database under section 102(c),
6 direct the Office of Science and Technology Pol-
7 icy and the agencies participating in the Pro-
8 gram to establish a mechanism (consistent with
9 existing law) to track all ongoing and completed
10 research and development projects and associ-
11 ated funding;”.

12 (e) ADVISORY COMMITTEE.—Section 101(b) of the
13 High-Performance Computing Act of 1991 (15 U.S.C.
14 5511(b)) is amended—

15 (1) in paragraph (1)—

16 (A) by inserting after the first sentence the
17 following: “The co-chairs of the advisory com-
18 mittee shall meet the qualifications of com-
19 mittee members and may be members of the
20 Presidents Council of Advisors on Science and
21 Technology.”; and

22 (B) by striking “high-performance” in sub-
23 paragraph (D) and inserting “high-end”; and

24 (2) by amending paragraph (2) to read as fol-
25 lows:

1 “(2) In addition to the duties under paragraph
2 (1), the advisory committee shall conduct periodic
3 evaluations of the funding, management, coordina-
4 tion, implementation, and activities of the Program.
5 The advisory committee shall report its findings and
6 recommendations not less frequently than once every
7 3 fiscal years to the Committee on Commerce,
8 Science, and Transportation of the Senate and the
9 Committee on Science and Technology of the House
10 of Representatives. The report shall be submitted in
11 conjunction with the update of the strategic plan.”.

12 (f) REPORT.—Section 101(a)(3) of the High-Per-
13 formance Computing Act of 1991 (15 U.S.C. 5511(a)(3))
14 is amended—

15 (1) in subparagraph (C)—

16 (A) by striking “is submitted,” and insert-
17 ing “is submitted, the levels for the previous
18 fiscal year,”; and

19 (B) by striking “each Program Component
20 Area” and inserting “each Program Component
21 Area and each research area supported in ac-
22 cordance with section 104”;

23 (2) in subparagraph (D)—

24 (A) by striking “each Program Component
25 Area,” and inserting “each Program Compo-

1 nent Area and each research area supported in
2 accordance with section 104,”;

3 (B) by striking “is submitted,” and insert-
4 ing “is submitted, the levels for the previous
5 fiscal year,”; and

6 (C) by striking “and” after the semicolon;

7 (3) by redesignating subparagraph (E) as sub-
8 paragraph (G); and

9 (4) by inserting after subparagraph (D) the fol-
10 lowing:

11 “(E) include a description of how the ob-
12 jectives for each Program Component Area, and
13 the objectives for activities that involve multiple
14 Program Component Areas, relate to the objec-
15 tives of the Program identified in the strategic
16 plan under subsection (e);

17 “(F) include—

18 “(i) a description of the funding re-
19 quired by the Office of Science and Tech-
20 nology Policy to perform the functions
21 under subsections (a) and (c) of section
22 102 for the next fiscal year by category of
23 activity;

24 “(ii) a description of the funding re-
25 quired by the Office of Science and Tech-

1 nology Policy to perform the functions
2 under subsections (a) and (c) of section
3 102 for the current fiscal year by category
4 of activity; and

5 “(iii) the amount of funding provided
6 for the Office of Science and Technology
7 Policy for the current fiscal year by each
8 agency participating in the Program; and”.

9 (g) DEFINITIONS.—Section 4 of the High-Perform-
10 ance Computing Act of 1991 (15 U.S.C. 5503) is amend-
11 ed—

12 (1) by redesignating paragraphs (1) and (2) as
13 paragraphs (2) and (3), respectively;

14 (2) by redesignating paragraph (3) as para-
15 graph (6);

16 (3) by redesignating paragraphs (6) and (7) as
17 paragraphs (7) and (8), respectively;

18 (4) by inserting before paragraph (2), as reded-
19 icated, the following:

20 “(1) ‘cyber-physical systems’ means physical or
21 engineered systems whose networking and informa-
22 tion technology functions and physical elements are
23 deeply integrated and are actively connected to the
24 physical world through sensors, actuators, or other

1 means to perform monitoring and control func-
2 tions;”;

3 (5) in paragraph (3), as redesignated, by strik-
4 ing “high-performance computing” and inserting
5 “networking and information technology”;

6 (6) in paragraph (6), as redesignated—

7 (A) by striking “high-performance com-
8 puting” and inserting “networking and infor-
9 mation technology”; and

10 (B) by striking “supercomputer” and in-
11 serting “high-end computing”;

12 (7) in paragraph (5), by striking “network re-
13 ferred to as” and all that follows through the semi-
14 colon and inserting “network, including advanced
15 computer networks of Federal agencies and depart-
16 ments”; and

17 (8) in paragraph (7), as redesignated, by strik-
18 ing “National High-Performance Computing Pro-
19 gram” and inserting “networking and information
20 technology research and development program”.

21 **SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.**

22 (a) RESEARCH IN AREAS OF NATIONAL IMPOR-
23 TANCE.—Title I of the High-Performance Computing Act
24 of 1991 (15 U.S.C. 5511 et seq.) is amended by adding
25 at the end the following:

1 **“SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPOR-**
2 **TANCE.**

3 “(a) IN GENERAL.—The Program shall encourage
4 agencies under section 101(a)(3)(B) to support, maintain,
5 and improve national, multi-agency, multi-faceted, re-
6 search and development activities in networking and infor-
7 mation technology directed toward application areas that
8 have the potential for significant contributions to national
9 economic competitiveness and for other significant societal
10 benefits.

11 “(b) TECHNICAL SOLUTIONS.—An activity under
12 subsection (a) shall be designed to advance the develop-
13 ment of research discoveries by demonstrating technical
14 solutions to important problems in areas including—

15 “(1) cybersecurity;

16 “(2) health care;

17 “(3) energy management and low-power sys-
18 tems and devices;

19 “(4) transportation, including surface and air
20 transportation;

21 “(5) cyber-physical systems;

22 “(6) large-scale data analysis and modeling of
23 physical phenomena;

24 “(7) large scale data analysis and modeling of
25 behavioral phenomena;

26 “(8) supply chain quality and security; and

1 “(9) privacy protection and protected disclosure
2 of confidential data.

3 “(c) RECOMMENDATIONS.—The advisory committee
4 under section 101(b) shall make recommendations to the
5 Program for candidate research and development areas for
6 support under this section.

7 “(d) CHARACTERISTICS.—

8 “(1) IN GENERAL.—Research and development
9 activities under this section—

10 “(A) shall include projects selected on the
11 basis of applications for support through a com-
12 petitive, merit-based process;

13 “(B) shall leverage, when possible, Federal
14 investments through collaboration with related
15 State initiatives;

16 “(C) shall include a plan for fostering the
17 transfer of research discoveries and the results
18 of technology demonstration activities, including
19 from institutions of higher education and Fed-
20 eral laboratories, to industry for commercial de-
21 velopment;

22 “(D) shall involve collaborations among re-
23 searchers in institutions of higher education
24 and industry; and

1 “(E) may involve collaborations among
2 nonprofit research institutions and Federal lab-
3 oratories, as appropriate.

4 “(2) COST-SHARING.—In selecting applications
5 for support, the agencies under section 101(a)(3)(B)
6 shall give special consideration to projects that in-
7 clude cost sharing from non-Federal sources.

8 “(3) MULTIDISCIPLINARY RESEARCH CEN-
9 TERS.—Research and development activities under
10 this section shall be supported through multidisci-
11 plinary research centers, including Federal labora-
12 tories, that are organized to investigate basic re-
13 search questions and carry out technology dem-
14 onstration activities in areas described in subsection
15 (a). Research may be carried out through existing
16 multidisciplinary centers, including those authorized
17 under section 7024(b)(2) of the America COM-
18 PETES Act (42 U.S.C. 1862o–10(2)).”.

19 (b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1)
20 of the High-Performance Computing Act of 1991 (15
21 U.S.C. 5511(a)(1)) is amended—

22 (1) in subparagraph (H), by striking “and”
23 after the semicolon;

24 (2) in subparagraph (I), by striking the period
25 at the end and inserting a semicolon; and

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

2 “(J) provide for increased understanding
3 of the scientific principles of cyber-physical sys-
4 tems and improve the methods available for the
5 design, development, and operation of cyber-
6 physical systems that are characterized by high
7 reliability, safety, and security; and

8 “(K) provide for research and development
9 on human-computer interactions, visualization,
10 and big data.”.

11 (c) TASK FORCE.—Title I of the High-Performance
12 Computing Act of 1991 (15 U.S.C. 5511 et seq.), as
13 amended by section 402(a) of this Act, is amended by add-
14 ing at the end the following:

15 **“SEC. 105. TASK FORCE.**

16 “(a) ESTABLISHMENT.—Not later than 180 days
17 after the date of enactment the Strengthening and En-
18 hancing Cybersecurity by Using Research, Education, In-
19 formation, and Technology Act of 2012, the Director of
20 the Office of Science and Technology Policy under section
21 102 shall convene a task force to explore mechanisms for
22 carrying out collaborative research and development activi-
23 ties for cyber-physical systems (including the related tech-
24 nologies required to enable these systems) through a con-
25 sortium or other appropriate entity with participants from

1 institutions of higher education, Federal laboratories, and
2 industry.

3 “(b) FUNCTIONS.—The task force shall—

4 “(1) develop options for a collaborative model
5 and an organizational structure for such entity
6 under which the joint research and development ac-
7 tivities could be planned, managed, and conducted
8 effectively, including mechanisms for the allocation
9 of resources among the participants in such entity
10 for support of such activities;

11 “(2) propose a process for developing a re-
12 search and development agenda for such entity, in-
13 cluding guidelines to ensure an appropriate scope of
14 work focused on nationally significant challenges and
15 requiring collaboration and to ensure the develop-
16 ment of related scientific and technological mile-
17 stones;

18 “(3) define the roles and responsibilities for the
19 participants from institutions of higher education,
20 Federal laboratories, and industry in such entity;

21 “(4) propose guidelines for assigning intellec-
22 tual property rights and for transferring research re-
23 sults to the private sector; and

1 “(5) make recommendations for how such enti-
2 ty could be funded from Federal, State, and non-
3 governmental sources.

4 “(c) COMPOSITION.—In establishing the task force
5 under subsection (a), the Director of the Office of Science
6 and Technology Policy shall appoint an equal number of
7 individuals from institutions of higher education and from
8 industry with knowledge and expertise in cyber-physical
9 systems, and may appoint not more than 2 individuals
10 from Federal laboratories.

11 “(d) REPORT.—Not later than 1 year after the date
12 of enactment of the Strengthening and Enhancing Cyber-
13 security by Using Research, Education, Information, and
14 Technology Act of 2012, the Director of the Office of
15 Science and Technology Policy shall transmit to the Com-
16 mittee on Commerce, Science, and Transportation of the
17 Senate and the Committee on Science and Technology of
18 the House of Representatives a report describing the find-
19 ings and recommendations of the task force.

20 “(e) TERMINATION.—The task force shall terminate
21 upon transmittal of the report required under subsection
22 (d).

23 “(f) COMPENSATION AND EXPENSES.—Members of
24 the task force shall serve without compensation.”.

1 **SEC. 403. PROGRAM IMPROVEMENTS.**

2 Section 102 of the High-Performance Computing Act
3 of 1991 (15 U.S.C. 5512) is amended to read as follows:

4 **“SEC. 102. PROGRAM IMPROVEMENTS.**

5 “(a) FUNCTIONS.—The Director of the Office of
6 Science and Technology Policy shall continue—

7 “(1) to provide technical and administrative
8 support to—

9 “(A) the agencies participating in planning
10 and implementing the Program, including sup-
11 port needed to develop the strategic plan under
12 section 101(e); and

13 “(B) the advisory committee under section
14 101(b);

15 “(2) to serve as the primary point of contact on
16 Federal networking and information technology ac-
17 tivities for government agencies, academia, industry,
18 professional societies, State computing and net-
19 working technology programs, interested citizen
20 groups, and others to exchange technical and pro-
21 grammatic information;

22 “(3) to solicit input and recommendations from
23 a wide range of stakeholders during the development
24 of each strategic plan under section 101(e) by con-
25 vening at least 1 workshop with invitees from aca-

1 demia, industry, Federal laboratories, and other rel-
2 evant organizations and institutions;

3 “(4) to conduct public outreach, including the
4 dissemination of the advisory committee’s findings
5 and recommendations, as appropriate;

6 “(5) to promote access to and early application
7 of the technologies, innovations, and expertise de-
8 rived from Program activities to agency missions
9 and systems across the Federal Government and to
10 United States industry;

11 “(6) to ensure accurate and detailed budget re-
12 porting of networking and information technology
13 research and development investment; and

14 “(7) to encourage agencies participating in the
15 Program to use existing programs and resources to
16 strengthen networking and information technology
17 education and training, and increase participation in
18 such fields, including by women and underrep-
19 resented minorities.

20 “(b) SOURCE OF FUNDING.—

21 “(1) IN GENERAL.—The functions under this
22 section shall be supported by funds from each agen-
23 cy participating in the Program.

24 “(2) SPECIFICATIONS.—The portion of the total
25 budget of the Office of Science and Technology Pol-

1 icy that is provided by each agency participating in
2 the Program for each fiscal year shall be in the
3 same proportion as each agency's share of the total
4 budget for the Program for the previous fiscal year,
5 as specified in the database under section 102(c).

6 “(c) DATABASE.—

7 “(1) IN GENERAL.—The Director of the Office
8 of Science and Technology Policy shall develop and
9 maintain a database of projects funded by each
10 agency for the fiscal year for each Program Compo-
11 nent Area.

12 “(2) PUBLIC ACCESSIBILITY.—The Director of
13 the Office of Science and Technology Policy shall
14 make the database accessible to the public.

15 “(3) DATABASE CONTENTS.—The database
16 shall include, for each project in the database—

17 “(A) a description of the project;

18 “(B) each agency, industry, institution of
19 higher education, Federal laboratory, or inter-
20 national institution involved in the project;

21 “(C) the source funding of the project (set
22 forth by agency);

23 “(D) the funding history of the project;

24 and

1 “(E) whether the project has been com-
2 pleted.”.

3 **SEC. 404. IMPROVING EDUCATION OF NETWORKING AND**
4 **INFORMATION TECHNOLOGY, INCLUDING**
5 **HIGH PERFORMANCE COMPUTING.**

6 Section 201(a) of the High-Performance Computing
7 Act of 1991 (15 U.S.C. 5521(a)) is amended—

8 (1) by redesignating paragraphs (2) through
9 (4) as paragraphs (3) through (5), respectively; and
10 (2) by inserting after paragraph (1) the fol-
11 lowing new paragraph:

12 “(2) the National Science Foundation shall use
13 its existing programs, in collaboration with other
14 agencies, as appropriate, to improve the teaching
15 and learning of networking and information tech-
16 nology at all levels of education and to increase par-
17 ticipation in networking and information technology
18 fields;”.

19 **SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO**
20 **THE HIGH-PERFORMANCE COMPUTING ACT**
21 **OF 1991.**

22 (a) SECTION 3.—Section 3 of the High-Performance
23 Computing Act of 1991 (15 U.S.C. 5502) is amended—

1 (1) in the matter preceding paragraph (1), by
2 striking “high-performance computing” and insert-
3 ing “networking and information technology”;

4 (2) in paragraph (1)—

5 (A) in the matter preceding subparagraph
6 (A), by striking “high-performance computing”
7 and inserting “networking and information
8 technology”;

9 (B) in subparagraphs (A), (F), and (G), by
10 striking “high-performance computing” each
11 place it appears and inserting “networking and
12 information technology”; and

13 (C) in subparagraph (H), by striking
14 “high-performance” and inserting “high-end”;
15 and

16 (3) in paragraph (2)—

17 (A) by striking “high-performance com-
18 puting and” and inserting “networking and in-
19 formation technology, and”; and

20 (B) by striking “high-performance com-
21 puting network” and inserting “networking and
22 information technology”.

23 (b) TITLE HEADING.—The heading of title I of the
24 High-Performance Computing Act of 1991 (105 Stat.
25 1595) is amended by striking “**HIGH-PERFORM-**

1 **ANCE COMPUTING**” and inserting **“NET-**
 2 **WORKING AND INFORMATION TECH-**
 3 **NOLOGY**”.

4 (c) SECTION 101.—Section 101 of the High-Perform-
 5 ance Computing Act of 1991 (15 U.S.C. 5511) is amend-
 6 ed—

7 (1) in the section heading, by striking **“HIGH-**
 8 **PERFORMANCE COMPUTING**” and inserting
 9 **“NETWORKING AND INFORMATION TECH-**
 10 **NOLOGY RESEARCH AND DEVELOPMENT**”;

11 (2) in subsection (a)—

12 (A) in the subsection heading, by striking
 13 **“NATIONAL HIGH-PERFORMANCE COMPUTING**”
 14 and inserting **“NETWORKING AND INFORMA-**
 15 **TION TECHNOLOGY RESEARCH AND DEVELOP-**
 16 **MENT**”;

17 (B) in paragraph (1)—

18 (i) by striking **“National High-Per-**
 19 **formance Computing Program**” and insert-
 20 ing **“networking and information tech-**
 21 **nology research and development pro-**
 22 **gram**”;

23 (ii) in subparagraph (A), by striking
 24 **“high-performance computing, including**

1 networking” and inserting “networking
2 and information technology”;

3 (iii) in subparagraphs (B) and (G), by
4 striking “high-performance” each place it
5 appears and inserting “high-end”; and

6 (iv) in subparagraph (C), by striking
7 “high-performance computing and net-
8 working” and inserting “high-end com-
9 puting, distributed, and networking”; and
10 (C) in paragraph (2)—

11 (i) in subparagraphs (A) and (C)—

12 (I) by striking “high-performance
13 computing” each place it appears and
14 inserting “networking and information
15 technology”; and

16 (II) by striking “development,
17 networking,” each place it appears
18 and inserting “development,”; and

19 (ii) in subparagraphs (G) and (H), as
20 redesignated by section 401(d) of this Act,
21 by striking “high-performance” each place
22 it appears and inserting “high-end”;

23 (3) in subsection (b)(1), in the matter pre-
24 ceding subparagraph (A), by striking “high-perform-

1 ance computing” each place it appears and inserting
2 “networking and information technology”; and

3 (4) in subsection (c)(1)(A), by striking “high-
4 performance computing” and inserting “networking
5 and information technology”.

6 (d) SECTION 201.—Section 201(a)(1) of the High-
7 Performance Computing Act of 1991 (15 U.S.C.
8 5521(a)(1)) is amended by striking “high-performance
9 computing and advanced high-speed computer net-
10 working” and inserting “networking and information tech-
11 nology research and development”.

12 (e) SECTION 202.—Section 202(a) of the High-Per-
13 formance Computing Act of 1991 (15 U.S.C. 5522(a)) is
14 amended by striking “high-performance computing” and
15 inserting “networking and information technology”.

16 (f) SECTION 203.—Section 203(a) of the High-Per-
17 formance Computing Act of 1991 (15 U.S.C. 5523(a)) is
18 amended—

19 (1) in paragraph (1), by striking “high-per-
20 formance computing and networking” and inserting
21 “networking and information technology”; and

22 (2) in paragraph (2)(A), by striking “high-per-
23 formance” and inserting “high-end”.

1 (g) SECTION 204.—Section 204 of the High-Per-
2 formance Computing Act of 1991 (15 U.S.C. 5524) is
3 amended—

4 (1) in subsection (a)(1)—

5 (A) in subparagraph (A), by striking
6 “high-performance computing systems and net-
7 works” and inserting “networking and informa-
8 tion technology systems and capabilities”;

9 (B) in subparagraph (B), by striking
10 “interoperability of high-performance com-
11 puting systems in networks and for common
12 user interfaces to systems” and inserting
13 “interoperability and usability of networking
14 and information technology systems”; and

15 (C) in subparagraph (C), by striking
16 “high-performance computing” and inserting
17 “networking and information technology”; and

18 (2) in subsection (b)—

19 (A) by striking “HIGH-PERFORMANCE
20 COMPUTING AND NETWORK” in the heading
21 and inserting “NETWORKING AND INFORMA-
22 TION TECHNOLOGY”; and

23 (B) by striking “sensitive”.

24 (h) SECTION 205.—Section 205(a) of the High-Per-
25 formance Computing Act of 1991 (15 U.S.C. 5525(a)) is

1 amended by striking “computational” and inserting “net-
2 working and information technology”.

3 (i) SECTION 206.—Section 206(a) of the High-Per-
4 formance Computing Act of 1991 (15 U.S.C. 5526(a)) is
5 amended by striking “computational research” and insert-
6 ing “networking and information technology research”.

7 (j) SECTION 207.—Section 207 of the High-Perform-
8 ance Computing Act of 1991 (15 U.S.C. 5527) is amended
9 by striking “high-performance computing” and inserting
10 “networking and information technology”.

11 (k) SECTION 208.—Section 208 of the High-Per-
12 formance Computing Act of 1991 (15 U.S.C. 5528) is
13 amended—

14 (1) in the section heading, by striking “**HIGH-**
15 **PERFORMANCE COMPUTING**” and inserting
16 “**NETWORKING AND INFORMATION TECH-**
17 **NOLOGY**”; and

18 (2) in subsection (a)—

19 (A) in paragraph (1), by striking “High-
20 performance computing and associated” and in-
21 serting “Networking and information”;

22 (B) in paragraph (2), by striking “high-
23 performance computing” and inserting “net-
24 working and information technologies”;

1 (C) in paragraph (3), by striking “high-
2 performance” and inserting “high-end”;

3 (D) in paragraph (4), by striking “high-
4 performance computers and associated” and in-
5 serting “networking and information”; and

6 (E) in paragraph (5), by striking “high-
7 performance computing and associated” and in-
8 serting “networking and information”.

9 **SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
10 **PROGRAM.**

11 (a) IN GENERAL.—The Director of the National
12 Science Foundation shall continue a Federal Cyber Schol-
13 arship-for-Service program under section 5(a) of the
14 Cyber Security Research and Development Act (15 U.S.C.
15 7404(a)) to increase the capacity of the higher education
16 system to produce an information technology workforce
17 with the skills necessary to enhance the security of the
18 Nation’s communications and information infrastructure
19 and to recruit and train the next generation of information
20 technology professionals and security managers to meet
21 the needs of the cybersecurity mission for Federal, State,
22 local, and tribal governments.

23 (b) PROGRAM DESCRIPTION AND COMPONENTS.—
24 The program shall—

1 (1) provide, through qualified institutions of
2 higher education, scholarships that provide tuition,
3 fees, and a competitive stipend for up to 2 years to
4 students pursuing a bachelor's or master's degree
5 and up to 3 years to students pursuing a doctoral
6 degree in a cybersecurity field;

7 (2) provide the scholarship recipients with sum-
8 mer internship opportunities or other meaningful
9 temporary appointments in the Federal information
10 technology workforce;

11 (3) require each scholarship recipient, as a con-
12 dition of receiving a scholarship under the program,
13 to serve in a Federal information technology work-
14 force for a period equal to one and one-half times
15 the length of the study following graduation in that
16 field;

17 (4) increase the capacity of institutions of high-
18 er education throughout all regions of the United
19 States to produce highly qualified cybersecurity pro-
20 fessionals, through the award of competitive, merit-
21 reviewed grants that support such activities as—

22 (A) faculty professional development, in-
23 cluding technical, hands-on experiences in the
24 private sector or government, workshops, semi-
25 nars, conferences, and other professional devel-

1 opment opportunities that will result in im-
2 proved instructional capabilities;

3 (B) institutional partnerships, including
4 minority serving institutions and community
5 colleges; and

6 (C) development of cybersecurity-related
7 courses and curricula;

8 (5) provide a procedure for the National
9 Science Foundation or a Federal agency, consistent
10 with regulations of the Office of Personnel Manage-
11 ment, to request and fund a security clearance for
12 a scholarship recipient, including providing for clear-
13 ance during a summer internship and upon gradua-
14 tion; and

15 (6) provide opportunities for students to receive
16 temporary appointments for meaningful employment
17 in the Federal information technology workforce
18 during school vacation periods and for internships.

19 (c) HIRING AUTHORITY.—

20 (1) IN GENERAL.—For purposes of any law or
21 regulation governing the appointment of an indi-
22 vidual in the Federal civil service, upon the success-
23 ful completion of the degree, a student receiving a
24 scholarship under the program may—

1 (A) be hired under section 213.3102(r) of
2 title 5, Code of Federal Regulations; and

3 (B) be exempt from competitive service.

4 (2) COMPETITIVE SERVICE.—Upon satisfactory
5 fulfillment of the service term under paragraph (1),
6 an individual may be converted to a competitive
7 service position without competition if the individual
8 meets the requirements for that position.

9 (d) ELIGIBILITY.—A scholarship under this section
10 shall be available only to a student who—

11 (1) is a citizen or permanent resident of the
12 United States;

13 (2) is a full time student in an eligible degree
14 program, as determined by the Director, that is fo-
15 cused on computer security or information assurance
16 at an awardee institution;

17 (3) accepts the terms of a scholarship under
18 this section;

19 (4) obtains a minimum SAT/College Board
20 score of 1600 (1100 Critical Reading and Math, 500
21 in Writing) or ACT score of 25;

22 (5) maintains a GPA of 3.0 or above on a 4.0
23 scale;

1 (6) demonstrates a commitment to a career in
2 improving the security of the information infrastruc-
3 ture; and

4 (7) has demonstrated a level of proficiency in
5 math or computer sciences.

6 (e) SERVICE OBLIGATION.—

7 (1) IN GENERAL.—If an individual receives a
8 scholarship under this section, as a condition of re-
9 ceiving such scholarship, the individual upon comple-
10 tion of the degree must serve as a cybersecurity pro-
11 fessional within the Federal workforce for a period
12 of time as provided in subsection (g).

13 (2) NOT OFFERED EMPLOYMENT.—If a scholar-
14 ship recipient is not offered employment by a Fed-
15 eral agency or a federally funded research and devel-
16 opment center, the service requirement can be satis-
17 fied at the Director’s discretion by—

18 (A) serving as a cybersecurity professional
19 in a State, local, or tribal government agency;
20 or

21 (B) teaching cybersecurity courses at an
22 institution of higher education.

23 (f) CONDITIONS OF SUPPORT.—As a condition of ac-
24 ceptance of a scholarship under this section, a scholarship
25 recipient shall agree to provide the awardee institution

1 with annual verifiable documentation of employment and
2 up-to-date contact information.

3 (g) LENGTH OF SERVICE.—The length of service re-
4 quired in exchange for a scholarship under this section
5 shall be 1 year more than the number of years for which
6 the scholarship was received.

7 (h) FAILURE TO COMPLETE SERVICE OBLIGA-
8 TION.—

9 (1) GENERAL RULE.—A scholarship recipient
10 under this section shall be liable to the United
11 States under paragraph (3) if the scholarship recipi-
12 ent—

13 (A) fails to maintain an acceptable level of
14 academic standing in the educational institution
15 in which the individual is enrolled, as deter-
16 mined by the Director;

17 (B) is dismissed from such educational in-
18 stitution for disciplinary reasons;

19 (C) withdraws from the program for which
20 the award was made before the completion of
21 such program;

22 (D) declares that the individual does not
23 intend to fulfill the service obligation under this
24 section; or

1 (E) fails to fulfill the service obligation of
2 the individual under this section.

3 (2) MONITORING COMPLIANCE.—As a condition
4 of participating in the program, a qualified institu-
5 tion of higher education receiving a grant under this
6 section shall—

7 (A) enter into an agreement with the Di-
8 rector of the National Science Foundation to
9 monitor the compliance of scholarship recipients
10 with respect to their service obligations; and

11 (B) provide to the Director, on an annual
12 basis, post-award employment information for
13 scholarship recipients through the completion of
14 their service obligations.

15 (3) REPAYMENT AMOUNTS.—

16 (A) LESS THAN 1 YEAR OF SERVICE.—If a
17 circumstance under paragraph (1) occurs before
18 the completion of 1 year of a service obligation
19 under this section, the total amount of awards
20 received by the individual under this section
21 shall be repaid or such amount shall be treated
22 as a loan to be repaid in accordance with sub-
23 paragraph (C).

24 (B) ONE OR MORE YEARS OF SERVICE.—
25 If a circumstance described in subparagraph

1 (D) or (E) of paragraph (1) occurs after the
2 completion of 1 year of a service obligation
3 under this section, the total amount of scholar-
4 ship awards received by the individual under
5 this section, reduced by the ratio of the number
6 of years of service completed divided by the
7 number of years of service required, shall be re-
8 paid or such amount shall be treated as a loan
9 to be repaid in accordance with subparagraph
10 (C).

11 (C) REPAYMENTS.—A loan described
12 under subparagraph (A) or (B) shall be treated
13 as a Federal Direct Unsubsidized Stafford
14 Loan under part D of title IV of the Higher
15 Education Act of 1965 (20 U.S.C. 1087a et
16 seq.), and shall be subject to repayment, to-
17 gether with interest thereon accruing from the
18 date of the scholarship award, in accordance
19 with terms and conditions specified by the Di-
20 rector (in consultation with the Secretary of
21 Education) in regulations promulgated to carry
22 out this paragraph.

23 (4) COLLECTION OF REPAYMENT.—

24 (A) IN GENERAL.—In the event that a
25 scholarship recipient is required to repay the

1 scholarship under this subsection, the institu-
2 tion providing the scholarship shall—

3 (i) be responsible for determining the
4 repayment amounts and for notifying the
5 scholarship recipient and the Director of
6 the amount owed; and

7 (ii) collect such repayment amount
8 within a period of time as determined
9 under the agreement under paragraph (2)
10 or the repayment amount shall be treated
11 as a loan in accordance with paragraph
12 (3)(C).

13 (B) RETURNED TO TREASURY.—Except as
14 provided in subparagraph (C), any such repay-
15 ment shall be returned to the Treasury of the
16 United States.

17 (C) RETAIN PERCENTAGE.—An institution
18 of higher education may retain a percentage of
19 any repayment the institution collects under
20 this paragraph to defray administrative costs
21 associated with the collection. The Director
22 shall establish a single, fixed percentage that
23 will apply to all eligible entities.

24 (5) EXCEPTIONS.—The Director may provide
25 for the partial or total waiver or suspension of any

1 service or payment obligation by an individual under
2 this section if—

3 (A) compliance by the individual with the
4 obligation is impossible;

5 (B) compliance by the individual would in-
6 volve extreme hardship to the individual; or

7 (C) enforcement of such obligation with re-
8 spect to the individual would be unconscionable.

9 (i) EVALUATION AND REPORT.—The Director of the
10 National Science Foundation shall—

11 (1) evaluate the success of recruiting individ-
12 uals for scholarships under this section and of hiring
13 and retaining those individuals in the public sector
14 workforce, including the annual cost and an assess-
15 ment of how the program actually improves the Fed-
16 eral workforce; and

17 (2) periodically report the findings under para-
18 graph (1) to Congress.

19 (j) AUTHORIZATION OF APPROPRIATIONS.—From
20 amounts made available under section 503 of the America
21 COMPETES Reauthorization Act of 2010 (124 Stat.
22 4005), the Secretary may use funds to carry out the re-
23 quirements of this section for fiscal years 2012 through
24 2013.

1 **SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND**
2 **TRAINING OF INFORMATION INFRASTRUC-**
3 **TURE PROFESSIONALS.**

4 (a) **STUDY.**—The President shall enter into an agree-
5 ment with the National Academies to conduct a com-
6 prehensive study of government, academic, and private-
7 sector accreditation, training, and certification programs
8 for personnel working in information infrastructure. The
9 agreement shall require the National Academies to consult
10 with sector coordinating councils and relevant govern-
11 mental agencies, regulatory entities, and nongovernmental
12 organizations in the course of the study.

13 (b) **SCOPE.**—The study shall include—

14 (1) an evaluation of the body of knowledge and
15 various skills that specific categories of personnel
16 working in information infrastructure should possess
17 in order to secure information systems;

18 (2) an assessment of whether existing govern-
19 ment, academic, and private-sector accreditation,
20 training, and certification programs provide the body
21 of knowledge and various skills described in para-
22 graph (1);

23 (3) an analysis of any barriers to the Federal
24 Government recruiting and hiring cybersecurity tal-
25 ent, including barriers relating to compensation, the

1 hiring process, job classification, and hiring flexi-
2 bility; and

3 (4) an analysis of the sources and availability of
4 cybersecurity talent, a comparison of the skills and
5 expertise sought by the Federal Government and the
6 private sector, an examination of the current and fu-
7 ture capacity of United States institutions of higher
8 education, including community colleges, to provide
9 current and future cybersecurity professionals,
10 through education and training activities, with those
11 skills sought by the Federal Government, State and
12 local entities, and the private sector.

13 (c) REPORT.—Not later than 1 year after the date
14 of enactment of this Act, the National Academies shall
15 submit to the President and Congress a report on the re-
16 sults of the study. The report shall include—

17 (1) findings regarding the state of information
18 infrastructure accreditation, training, and certifi-
19 cation programs, including specific areas of defi-
20 ciency and demonstrable progress; and

21 (2) recommendations for the improvement of in-
22 formation infrastructure accreditation, training, and
23 certification programs.

1 **SEC. 408. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
2 **VELOPMENT PLAN.**

3 (a) IN GENERAL.—Not later than 12 months after
4 the date of enactment of this Act, the agencies designated
5 under subsection 101(a)(3)(B) (i) through (xi) of the
6 High-Performance Computing Act of 1991 (15 U.S.C.
7 5511(a)(3)(B) (i) through (xi)) (working through the Na-
8 tional Science and Technology Council) shall transmit to
9 Congress a strategic plan based on an assessment of cy-
10 bersecurity risk to guide the overall direction of Federal
11 cybersecurity and information assurance research and de-
12 velopment for information technology and networking sys-
13 tems. Once every 3 years after the initial strategic plan
14 is transmitted to Congress under this section, the agencies
15 shall prepare and transmit to Congress an update of the
16 strategic plan.

17 (b) CONTENTS OF PLAN.—The strategic plan under
18 subsection (a) shall—

19 (1) specify and prioritize—

20 (A) near-term, mid-term, and long-term re-
21 search objectives, including objectives associated
22 with the research areas identified in section
23 4(a)(1) of the Cyber Security Research and De-
24 velopment Act (15 U.S.C. 7403(a)(1)); and

1 (B) how the near-term objectives com-
2 plement research and development areas in
3 which the private sector is actively engaged;

4 (2) describe how the National Networking and
5 Information Technology Research and Development
6 Program will focus on innovative, transformational
7 technologies with the potential to enhance the secu-
8 rity, reliability, resilience, and trustworthiness of the
9 digital infrastructure, and to protect consumer pri-
10 vacy;

11 (3) describe how the Program will foster the
12 rapid transfer of research and development results
13 into new cybersecurity technologies and applications
14 for the timely benefit of society and the national in-
15 terest, including through the dissemination of best
16 practices and other outreach activities;

17 (4) describe how the Program will establish and
18 maintain a national research infrastructure for cre-
19 ating, testing, and evaluating the next generation of
20 secure networking and information technology sys-
21 tems;

22 (5) describe how the Program will facilitate ac-
23 cess by academic researchers to the infrastructure
24 described in paragraph (4), as well as to relevant
25 data, including event data; and

1 (6) describe how the Program will engage fe-
2 males and individuals identified in section 33 or 34
3 of the Science and Engineering Equal Opportunities
4 Act (42 U.S.C. 1885a and 1885b) to foster a more
5 diverse workforce in this area.

6 (c) DEVELOPMENT OF IMPLEMENTATION ROAD-
7 MAP.—The agencies described in subsection (a) shall de-
8 velop and annually update an implementation roadmap for
9 the strategic plan under this section. The implementation
10 roadmap shall—

11 (1) specify the role of each Federal agency in
12 carrying out or sponsoring research and development
13 to meet the research objectives of the strategic plan,
14 including a description of how progress toward the
15 research objectives will be evaluated;

16 (2) specify the funding allocated to each major
17 research objective of the strategic plan and the
18 source of funding by agency for the current fiscal
19 year; and

20 (3) estimate the funding required for each
21 major research objective of the strategic plan for the
22 following 3 fiscal years.

23 (d) RECOMMENDATIONS.—In developing and updat-
24 ing the strategic plan under subsection (a), the agencies
25 involved shall solicit recommendations and advice from—

1 (1) the advisory committee established under
2 section 101(b)(1) of the High-Performance Com-
3 puting Act of 1991 (15 U.S.C. 5511(b)(1)); and

4 (2) a wide range of stakeholders, including in-
5 dustry, academia (including representatives of mi-
6 nority serving institutions and community colleges),
7 National Laboratories, and other relevant organiza-
8 tions and institutions.

9 (e) REPORT APPENDIX.—The implementation road-
10 map under subsection (c), and its annual updates, shall
11 be appended to the report under section 101(a)(2)(D) of
12 the High-Performance Computing Act of 1991 (15 U.S.C.
13 5511(a)(2)(D)).

14 (f) AUTHORIZATION OF APPROPRIATIONS.—From
15 amounts made available under section 503 of the America
16 COMPETES Reauthorization Act of 2010 (124 Stat.
17 4005), the Secretary may use funds to carry out the re-
18 quirements of this section for fiscal years 2012 through
19 2013.

20 **SEC. 409. INTERNATIONAL CYBERSECURITY TECHNICAL**
21 **STANDARDS.**

22 (a) IN GENERAL.—The Director of the National In-
23 stitute of Standards and Technology, in coordination with
24 appropriate Federal authorities, shall—

1 (1) as appropriate, ensure coordination of Fed-
 2 eral agencies engaged in the development of inter-
 3 national technical standards related to information
 4 system security; and

5 (2) not later than 1 year after the date of en-
 6 actment of this Act, develop and transmit to Con-
 7 gress a plan for ensuring such Federal agency co-
 8 ordination.

9 (b) CONSULTATION WITH THE PRIVATE SECTOR.—

10 In carrying out the activities under subsection (a)(1), the
 11 Director shall ensure consultation with appropriate private
 12 sector stakeholders.

13 **SEC. 410. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
 14 **OPMENT.**

15 The Director of the National Institute of Standards
 16 and Technology shall continue a program to support the
 17 development of technical standards, metrology, testbeds,
 18 and conformance criteria, taking into account appropriate
 19 user concerns—

20 (1) to improve interoperability among identity
 21 management technologies;

22 (2) to strengthen authentication methods of
 23 identity management systems;

24 (3) to improve privacy protection in identity
 25 management systems, including health information

1 technology systems, through authentication and se-
2 curity protocols; and

3 (4) to improve the usability of identity manage-
4 ment systems.

5 **SEC. 411. FEDERAL CYBERSECURITY RESEARCH AND DE-**
6 **VELOPMENT.**

7 (a) NATIONAL SCIENCE FOUNDATION COMPUTER
8 AND NETWORK SECURITY RESEARCH GRANT AREAS.—
9 Section 4(a)(1) of the Cyber Security Research and Devel-
10 opment Act (15 U.S.C. 7403(a)(1)) is amended—

11 (1) in subparagraph (H), by striking “and”
12 after the semicolon;

13 (2) in subparagraph (I), by striking “property.”
14 and inserting “property;”; and

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

16 “(J) secure fundamental protocols that are
17 at the heart of inter-network communications
18 and data exchange;

19 “(K) system security that addresses the
20 building of secure systems from trusted and
21 untrusted components;

22 “(L) monitoring and detection; and

23 “(M) resiliency and rapid recovery meth-
24 ods.”.

1 (b) NATIONAL SCIENCE FOUNDATION COMPUTER
2 AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of
3 the Cyber Security Research and Development Act (15
4 U.S.C. 7403(a)(3)) is amended—

5 (1) in subparagraph (D), by striking “and”;

6 (2) in subparagraph (E), by striking “2007.”

7 and inserting “2007;”; and

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

9 “(F) such funds from amounts made avail-
10 able under section 503 of the America COM-
11 PETES Reauthorization Act of 2010 (124
12 Stat. 4005), as the Secretary finds necessary to
13 carry out the requirements of this subsection
14 for fiscal years 2012 through 2013.”.

15 (c) COMPUTER AND NETWORK SECURITY CEN-
16 TERS.—Section 4(b)(7) of the Cyber Security Research
17 and Development Act (15 U.S.C. 7403(b)(7)) is amend-
18 ed—

19 (1) in subparagraph (D), by striking “and”;

20 (2) in subparagraph (E), by striking “2007.”

21 and inserting “2007;”; and

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

23 “(F) such funds from amounts made avail-
24 able under section 503 of the America COM-
25 PETES Reauthorization Act of 2010 (124

1 Stat. 4005), as the Secretary finds necessary to
2 carry out the requirements of this subsection
3 for fiscal years 2012 through 2013.”.

4 (d) COMPUTER AND NETWORK SECURITY CAPACITY
5 BUILDING GRANTS.—Section 5(a)(6) of the Cyber Secu-
6 rity Research and Development Act (15 U.S.C.
7 7404(a)(6)) is amended—

8 (1) in subparagraph (D), by striking “and”;

9 (2) in subparagraph (E), by striking “2007.”
10 and inserting “2007;”; and

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

12 “(F) such funds from amounts made avail-
13 able under section 503 of the America COM-
14 PETES Reauthorization Act of 2010 (124
15 Stat. 4005), as the Secretary finds necessary to
16 carry out the requirements of this subsection
17 for fiscal years 2012 through 2013.”.

18 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
19 GRANTS.—Section 5(b)(2) of the Cyber Security Research
20 and Development Act (15 U.S.C. 7404(b)(2)) is amend-
21 ed—

22 (1) in subparagraph (D), by striking “and”;

23 (2) in subparagraph (E), by striking “2007.”
24 and inserting “2007;”; and

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

1 “(F) such funds from amounts made avail-
2 able under section 503 of the America COM-
3 PETES Reauthorization Act of 2010 (124
4 Stat. 4005), as the Secretary finds necessary to
5 carry out the requirements of this subsection
6 for fiscal years 2012 through 2013.”.

7 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
8 NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the
9 Cyber Security Research and Development Act (15 U.S.C.
10 7404(c)(7)) is amended—

11 (1) in subparagraph (D), by striking “and”;

12 (2) in subparagraph (E), by striking “2007.”

13 and inserting “2007;”; and

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

15 “(F) such funds from amounts made avail-
16 able under section 503 of the America COM-
17 PETES Reauthorization Act of 2010 (124
18 Stat. 4005), as the Secretary finds necessary to
19 carry out the requirements of this subsection
20 for fiscal years 2012 through 2013.”.

21 (g) CYBERSECURITY FACULTY DEVELOPMENT
22 TRAINEESHIP PROGRAM.—Section 5(e)(9) of the Cyber
23 Security Research and Development Act (15 U.S.C.

1 7404(e)(9)) is amended by striking “2007” and inserting
2 “2007 and for each of fiscal years 2012 through 2014”.

○