

.....
(Original Signature of Member)

112TH CONGRESS
2D SESSION

H. R.

To improve information security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mrs. BONO MACK (for herself and Mrs. BLACKBURN) introduced the following bill; which was referred to the Committee on

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 the “SECURE IT Act of 2012”.

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. Inspector General review.
- Sec. 106. Technical amendments.
- Sec. 107. 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. Cloud computing services for research.
- Sec. 405. Cybersecurity university-industry task force.
- Sec. 406. Improving education of networking and information technology, including high performance computing.
- Sec. 407. Conforming and technical amendments to the High-Performance Computing Act of 1991.
- Sec. 408. Federal cyber scholarship-for-service program.
- Sec. 409. Study and analysis of certification and training of information infrastructure professionals.
- Sec. 410. Cybersecurity strategic research and development plan.
- Sec. 411. International cybersecurity technical standards.
- Sec. 412. Identity management research and development.
- Sec. 413. Federal cybersecurity research and development programs.
- Sec. 414. Cybersecurity automation and checklists for Government systems.
- Sec. 415. National Institute of Standards and Technology 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:

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

9 (2) **ANTITRUST LAWS.**—The term “antitrust
10 laws”—

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

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

17 (C) includes any State law that has the
18 same intent and effect as the laws under sub-
19 paragraphs (A) and (B).

20 (3) **COUNTERMEASURE.**—The term “counter-
21 measure” means an automated or a manual action
22 with defensive intent to mitigate cyber threats.

23 (4) **CYBER THREAT INFORMATION.**—The term
24 “cyber threat information” means information that
25 may be indicative of or describes—

1 (A) a technical or operation vulnerability
2 or a cyber threat mitigation measure;

3 (B) an action or operation to mitigate a
4 cyber threat;

5 (C) malicious reconnaissance, including
6 anomalous patterns of network activity that ap-
7 pear to be transmitted for the purpose of gath-
8 ering technical information related to a
9 cybersecurity threat;

10 (D) a method of defeating a technical con-
11 trol;

12 (E) a method of defeating an operational
13 control;

14 (F) network activity or protocols known to
15 be associated with a malicious cyber actor or
16 that signify malicious cyber intent;

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

23 (H) any other attribute of a cybersecurity
24 threat or cyber defense information that would
25 foster situational awareness of the United

1 States cybersecurity posture, if disclosure of
2 such attribute or information is not otherwise
3 prohibited by law;

4 (I) the actual or potential harm caused by
5 a cyber incident, including information
6 exfiltrated when it is necessary in order to iden-
7 tify or describe a cybersecurity threat; or

8 (J) any combination thereof.

9 (5) CYBERSECURITY CENTER.—The term
10 “cybersecurity center” means the Department of De-
11 fense Cyber Crime Center, the Intelligence Commu-
12 nity Incident Response Center, the United States
13 Cyber Command Joint Operations Center, the Na-
14 tional Cyber Investigative Joint Task Force, the Na-
15 tional Security Agency/Central Security Service
16 Threat Operations Center, the National
17 Cybersecurity and Communications Integration Cen-
18 ter, and any successor center.

19 (6) CYBERSECURITY SYSTEM.—The term
20 “cybersecurity system” means a system designed or
21 employed to ensure the integrity, confidentiality, or
22 availability of, or to safeguard, a system or network,
23 including measures intended to protect a system or
24 network from—

1 (A) efforts to degrade, disrupt, or destroy
2 such system or network; or

3 (B) theft or misappropriations of private
4 or government information, intellectual prop-
5 erty, or personally identifiable information.

6 (7) ENTITY.—The term “entity” means any
7 private entity, non-Federal Government agency or
8 department, or State, tribal, or local government
9 agency or department (including an officer, em-
10 ployee, or agent thereof).

11 (8) INFORMATION SECURITY.—The term “infor-
12 mation security” means protecting information and
13 information systems from disruption or unauthorized
14 access, use, disclosure, modification, or destruction
15 in order to provide—

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

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

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

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

4 (10) MALICIOUS RECONNAISSANCE.—The term
5 “malicious reconnaissance” means a method for ac-
6 tively probing or passively monitoring an information
7 system for the purpose of discerning technical
8 vulnerabilities of the information system, if such
9 method is associated with a known or suspected
10 cybersecurity threat.

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

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

19 (13) PRIVATE ENTITY.—The term “private en-
20 tity” means any individual or any private group, or-
21 ganization, or corporation, including an officer, em-
22 ployee, or agent thereof.

23 (14) TECHNICAL CONTROL.—The term “tech-
24 nical control” means a hardware or software restric-
25 tion on, or audit of, access or use of an information

1 system or information that is stored on, processed
2 by, or transiting an information system that is in-
3 tended to ensure the confidentiality, integrity, or
4 availability of that system.

5 (15) TECHNICAL VULNERABILITY.—The term
6 “technical vulnerability” means any attribute of
7 hardware or software that could enable or facilitate
8 the defeat of a technical control.

9 **SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT IN-**
10 **FORMATION.**

11 (a) VOLUNTARY DISCLOSURE.—

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

20 (2) ENTITIES.—Notwithstanding any other pro-
21 vision of law, an entity may disclose cyber threat in-
22 formation to—

23 (A) a cybersecurity center; or

1 (B) any other entity in order to assist with
2 preventing, investigating, or otherwise miti-
3 gating threats to information security.

4 (3) INFORMATION SECURITY PROVIDERS.—If
5 the cyber threat information described in paragraph
6 (1) is obtained, identified, or otherwise possessed in
7 the course of providing information security prod-
8 ucts or services under contract to another entity,
9 that entity shall, at any time prior to disclosure of
10 such information, be given a reasonable opportunity
11 to authorize or prevent such disclosure or to request
12 anonymization of such information.

13 (b) REQUIRED DISCLOSURE.—

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

23 (2) DISCLOSURE TO CYBERSECURITY CEN-
24 TERS.—A Federal agency or department receiving
25 cyber threat information under paragraph (1) shall

1 immediately disclose such information to a
2 cybersecurity center.

3 (3) LIMITATION ON APPLICATION.—This sub-
4 section shall not apply with respect to services pro-
5 vided under a contract in effect on the date of the
6 enactment of this Act.

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

10 (1) may be disclosed to and used by, consistent
11 with otherwise applicable law, any Federal agency or
12 department, component, officer, employee, or agent
13 of the Federal Government for a cybersecurity pur-
14 pose, a national security purpose, or in order to pre-
15 vent, investigate, or prosecute any of the offenses
16 listed in section 2516 of title 18, United States
17 Code;

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

1 vided orally with subsequent documentation of such
2 consent;

3 (3) shall be considered the commercial, finan-
4 cial, or proprietary information of the entity pro-
5 viding such information to the Federal Government
6 and any disclosure outside the Federal Government
7 may only be made upon the prior written consent by
8 such entity and shall not constitute a waiver of any
9 applicable privilege or protection provided by law,
10 except that if the need for immediate disclosure pre-
11 vents obtaining written consent, such consent may
12 be provided orally with subsequent documentation of
13 such consent;

14 (4) shall be deemed voluntarily shared informa-
15 tion and exempt from disclosure under section 552
16 of title 5, United States Code, and any State, tribal,
17 or local law requiring disclosure of information or
18 records;

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

23 (6) shall not be subject to the rules of any Fed-
24 eral agency or department or any judicial doctrine

1 regarding ex parte communications with a decision-
2 making official;

3 (7) shall not, if subsequently provided to a
4 State, tribal, or local government or government
5 agency, otherwise be disclosed or distributed to any
6 entity by such State, tribal, or local government or
7 government agency without the prior written consent
8 of the entity submitting such information, notwith-
9 standing any State, tribal, or local law requiring dis-
10 closure of information or records, except that if the
11 need for immediate disclosure prevents obtaining
12 written consent, such consent may be provided orally
13 with subsequent documentation of such consent; and

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

22 (d) PROCEDURES RELATING TO INFORMATION SHAR-
23 ING WITH A CYBERSECURITY CENTER.—Not later than
24 60 days after the date of enactment of this Act, the heads
25 of each department or agency containing a cybersecurity

1 center shall jointly develop, promulgate, and submit to
2 Congress procedures to ensure that cyber threat informa-
3 tion shared with or provided to—

4 (1) a cybersecurity center under this section—

5 (A) may be submitted to a cybersecurity
6 center by an entity, to the greatest extent pos-
7 sible, through a uniform, publicly available
8 process or format that is easily accessible on
9 the website of such cybersecurity center, and
10 that includes the ability to provide relevant de-
11 tails about the cyber threat information and
12 written consent to any subsequent disclosures
13 authorized by this paragraph;

14 (B) shall immediately be further shared
15 with each cybersecurity center in order to pre-
16 vent, investigate, or otherwise mitigate threats
17 to information security across the Federal Gov-
18 ernment;

19 (C) is handled by the Federal Government
20 in a reasonable manner, including consideration
21 of the need to protect the privacy and civil lib-
22 erties of individuals through anonymization or
23 other appropriate methods, while fully accom-
24 plishing the objectives of this title; and

1 (D) except as provided in this section, shall
2 only be used, disclosed, or handled in accord-
3 ance with the provisions of subsection (c); and
4 (2) a Federal agency or department under sub-
5 section (b) is provided immediately to a
6 cybersecurity center in order to prevent, investigate,
7 or otherwise mitigate threats to information security
8 across the Federal Government.

9 (e) INFORMATION SHARED BETWEEN PRIVATE EN-
10 TITIES.—

11 (1) IN GENERAL.—A private entity sharing
12 cyber threat information with another private entity
13 under this title may restrict the use or sharing of
14 such information by such other private entity.

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

18 (A) shall only be further shared in accord-
19 ance with any restrictions placed on the sharing
20 of such information by the private entity au-
21 thorizing such sharing, such as appropriate
22 anonymization of such information; and

23 (B) may not be used by any private entity
24 to gain an unfair competitive advantage to the
25 detriment of the private entity authorizing the

1 sharing of such information, except that the
2 conduct described in paragraph (3) shall not
3 constitute unfair competitive conduct.

4 (3) ANTITRUST EXEMPTION.—The exchange or
5 provision of cyber threat information or assistance
6 between 2 or more private entities under this title
7 shall not be considered a violation of any provision
8 of antitrust laws if exchanged or provided in order
9 to assist with—

10 (A) facilitating the prevention, investiga-
11 tion, or mitigation of threats to information se-
12 curity; or

13 (B) communicating or disclosing of cyber
14 threat information to help prevent, investigate
15 or otherwise mitigate the effects of a threat to
16 information security.

17 (f) FEDERAL PREEMPTION.—

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

22 (2) STATE LAW ENFORCEMENT.—Nothing in
23 this section shall be construed to supercede any stat-
24 ute or other law of a State or political subdivision

1 of a State concerning the use of authorized law en-
2 forcement techniques.

3 (3) PUBLIC DISCLOSURE.—No information
4 shared with or provided to a State, tribal, or local
5 government or government agency pursuant to this
6 section shall be made publicly available pursuant to
7 any State, tribal, or local law requiring disclosure of
8 information or records.

9 (g) CIVIL AND CRIMINAL LIABILITY.—

10 (1) GENERAL PROTECTIONS.—

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

14 (i) the use of countermeasures and
15 cybersecurity systems as authorized by this
16 title;

17 (ii) the use, receipt, or disclosure of
18 any cyber threat information as authorized
19 by this title; or

20 (iii) the subsequent actions or inac-
21 tions of any lawful recipient of cyber threat
22 information provided by such private enti-
23 ty.

1 (B) ENTITIES.—No cause of action shall
2 lie or be maintained in any court against any
3 entity for—

4 (i) the use, receipt, or disclosure of
5 any cyber threat information as authorized
6 by this title; or

7 (ii) the subsequent actions or inac-
8 tions of any lawful recipient of cyber threat
9 information provided by such entity.

10 (2) CONSTRUCTION.—Nothing in this sub-
11 section shall be construed as creating any immunity
12 against, or otherwise affecting, any action brought
13 by the Federal Government, or any agency or de-
14 partment thereof, to enforce any law, executive
15 order, or procedure governing the appropriate han-
16 dling, disclosure, and use of classified information.

17 (h) OTHERWISE LAWFUL DISCLOSURES.—Nothing
18 in this section shall be construed to limit or prohibit other-
19 wise lawful disclosures of communications, records, or
20 other information by a private entity to any other govern-
21 mental or private entity not covered under this section.

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

1 **SEC. 103. INFORMATION SHARING BY THE FEDERAL GOV-**
2 **ERNMENT.**

3 (a) CLASSIFIED INFORMATION.—

4 (1) PROCEDURES.—Consistent with the protec-
5 tion of intelligence sources and methods, and as oth-
6 erwise determined appropriate, the Director of Na-
7 tional Intelligence and the Secretary of Defense
8 shall, in consultation with the heads of the appro-
9 priate Federal departments or agencies, develop and
10 promulgate procedures to facilitate and promote—

11 (A) the immediate sharing, through the
12 cybersecurity centers, of classified cyber threat
13 information in the possession of the Federal
14 Government with appropriately cleared rep-
15 resentatives of any appropriate entity; and

16 (B) the declassification and immediate
17 sharing, through the cybersecurity centers, with
18 any entity or, if appropriate, public availability
19 of cyber threat information in the possession of
20 the Federal Government.

21 (2) HANDLING OF CLASSIFIED INFORMATION.—

22 The procedures developed under paragraph (1) shall
23 ensure that each entity receiving classified cyber
24 threat information pursuant to this section has ac-
25 knowledged in writing the ongoing obligation to com-
26 ply with all laws, executive orders, and procedures

1 concerning the appropriate handling, disclosure, or
2 use of classified information.

3 (b) UNCLASSIFIED CYBER THREAT INFORMATION.—

4 The head of each department or agency containing a
5 cybersecurity center shall jointly develop and promulgate
6 procedures that ensure that, consistent with the provisions
7 of this section, unclassified cyber threat information, in-
8 cluding sensitive but unclassified cyber information, in the
9 possession of the Federal Government—

10 (1) is shared in an immediate and adequate
11 manner with appropriate entities; and

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

13 (c) DEVELOPMENT OF PROCEDURES.—

14 (1) EXISTING PROCESSES.—The procedures de-
15 veloped under this section shall, to the greatest ex-
16 tent possible, incorporate existing processes utilized
17 by sector-specific information sharing and analysis
18 centers.

19 (2) COORDINATION WITH ENTITIES.—In devel-
20 oping the procedures required under this section, the
21 Director of National Intelligence and the head of
22 each department or agency containing a
23 cybersecurity center shall coordinate with appro-
24 priate entities to ensure that protocols are imple-
25 mented that will facilitate and promote the sharing

1 of cyber threat information by the Federal Govern-
2 ment.

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

9 **SEC. 104. REPORT ON IMPLEMENTATION.**

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

18 (1) an assessment of the sufficiency of the pro-
19 cedures developed under section 103 of this Act in
20 ensuring that cyber threat information in the posses-
21 sion of the Federal Government is provided in an
22 immediate and adequate manner to appropriate enti-
23 ties or, if appropriate, is made publicly available;

24 (2) an assessment of whether information has
25 been appropriately classified and an accounting of

1 the number of security clearances authorized by the
2 Federal Government for purposes of this title;

3 (3) a review of the type of cyber threat infor-
4 mation shared with a cybersecurity center under sec-
5 tion 102 of this Act, including whether such infor-
6 mation meets the definition of cyber threat informa-
7 tion under section 101, the degree to which such in-
8 formation may impact the privacy and civil liberties
9 of individuals, and the adequacy of any steps taken
10 to reduce such impact;

11 (4) a review of actions taken by the Federal
12 Government based on information provided to a
13 cybersecurity center under section 102 of this Act,
14 including the appropriateness of any subsequent use
15 under section 102(c)(1)(A) of this Act;

16 (5) a description of any violations of the re-
17 quirements of this title by the Federal Government;

18 (6) with respect to an entity providing elec-
19 tronic communication services, remote computing
20 service, or cybersecurity services to a Federal agency
21 or department, a description of any violations of the
22 requirements of subsection (b) or (c) of section 102
23 of this Act related to the performance of such serv-
24 ices;

1 (7) a classified list of entities that received clas-
2 sified information from the Federal Government
3 under section 103 of this Act and a description of
4 any indication that such information may not have
5 been appropriately handled;

6 (8) a summary of any breach of information se-
7 curity, if known, attributable to a specific failure by
8 the Federal Government to act on cyber threat infor-
9 mation in the possession of the Federal Government
10 that resulted in substantial economic harm or injury
11 to a specific entity or the Federal Government; and

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

14 (b) FORM OF REPORT.—The report under subsection
15 (a) shall be submitted in unclassified form, but shall in-
16 clude a classified annex.

17 **SEC. 105. INSPECTOR GENERAL REVIEW.**

18 (a) IN GENERAL.—The Council of the Inspectors
19 General on Integrity and Efficiency may review compli-
20 ance by the cybersecurity centers, and by any Federal de-
21 partment or agency receiving cyber threat information
22 from such cybersecurity centers, with the procedures re-
23 quired under section 102.

24 (b) CONSIDERATIONS.—Each review described in
25 subsection (a) shall consider whether the Federal Govern-

1 ment has handled such cyber threat information in a rea-
2 sonable manner, including consideration of the need to
3 protect the privacy and civil liberties of individuals
4 through anonymization or other appropriate methods,
5 while fully accomplishing the objectives of this title.

6 (c) SUBMISSION TO CONGRESS.—The Council shall
7 provide the results of any review conducted under this sec-
8 tion to Congress no later than 30 days after the date of
9 completion of the review.

10 **SEC. 106. TECHNICAL AMENDMENTS.**

11 Section 552(b) of title 5, United States Code, is
12 amended—

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

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

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

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

22 **SEC. 107. ACCESS TO CLASSIFIED INFORMATION.**

23 (a) AUTHORIZATION REQUIRED.—No person shall be
24 provided with access to classified information (as defined
25 in section 6.1 of Executive Order 13526 (50 U.S.C. 435

1 note; relating to classified national security information))
2 relating to cyber security threats or cyber security
3 vulnerabilities under this title without the appropriate se-
4 curity clearances.

5 (b) SECURITY CLEARANCES.—The appropriate Fed-
6 eral agencies or departments shall, consistent with appli-
7 cable procedures and requirements, and if otherwise
8 deemed appropriate, assist an individual in timely obtain-
9 ing an appropriate security clearance where such indi-
10 vidual has been determined to be eligible for such clear-
11 ance and has a need-to-know (as defined in section 6.1
12 of that Executive Order) classified information to carry
13 out this title.

14 **TITLE II—COORDINATION OF**
15 **FEDERAL INFORMATION SE-**
16 **CURITY POLICY**

17 **SEC. 201. COORDINATION OF FEDERAL INFORMATION SE-**
18 **CURITY POLICY.**

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

22 “SUBCHAPTER II—INFORMATION SECURITY
23 “§ 3551. **Purposes**

24 “The purposes of this subchapter are—

1 “(1) to provide a comprehensive framework for
2 ensuring the effectiveness of information security
3 controls over information resources that support
4 Federal operations and assets;

5 “(2) to recognize the highly networked nature
6 of the current Federal computing environment and
7 provide effective government-wide management of
8 policies, directives, standards, and guidelines, as well
9 as effective and nimble oversight of and response to
10 information security risks, including coordination of
11 information security efforts throughout the Federal
12 civilian, national security, and law enforcement com-
13 munities;

14 “(3) to provide for development and mainte-
15 nance of controls required to protect agency infor-
16 mation and information systems and contribute to
17 the overall improvement of agency information secu-
18 rity posture;

19 “(4) to provide for the development of tools and
20 methods to assess and respond to real-time situa-
21 tional risk for Federal information system operations
22 and assets; and

23 “(5) to provide a mechanism for improving
24 agency information security programs through con-
25 tinuous monitoring of agency information systems

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

3 **“§ 3552. Definitions**

4 “In this subchapter:

5 “(1) ADEQUATE SECURITY.—The term ‘ade-
6 quate security’ means security commensurate with
7 the risk and magnitude of the harm resulting from
8 the unauthorized access to or loss, misuse, destruc-
9 tion, or modification of information.

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

12 “(3) CYBERSECURITY CENTER.—The term
13 ‘cybersecurity center’ means the Department of De-
14 fense Cyber Crime Center, the Intelligence Commu-
15 nity Incident Response Center, the United States
16 Cyber Command Joint Operations Center, the Na-
17 tional Cyber Investigative Joint Task Force, the Na-
18 tional Security Agency/Central Security Service
19 Threat Operations Center, the National
20 Cybersecurity and Communications Integration Cen-
21 ter, and any successor center.

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

1 “(A) a technical or operation vulnerability
2 or a cyber threat mitigation measure;

3 “(B) an action or operation to mitigate a
4 cyber threat;

5 “(C) malicious reconnaissance, including
6 anomalous patterns of network activity that ap-
7 pear to be transmitted for the purpose of gath-
8 ering technical information related to a
9 cybersecurity threat;

10 “(D) a method of defeating a technical
11 control;

12 “(E) a method of defeating an operational
13 control;

14 “(F) network activity or protocols known
15 to be associated with a malicious cyber actor or
16 that may signify malicious intent;

17 “(G) a method of causing a user with le-
18 gitimate access to an information system or in-
19 formation that is stored on, processed by, or
20 transiting an information system to inadvert-
21 ently enable the defeat of a technical or oper-
22 ational control;

23 “(H) any other attribute of a cybersecurity
24 threat or information that would foster situa-
25 tional awareness of the United States security

1 posture, if disclosure of such attribute or infor-
2 mation is not otherwise prohibited by law;

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

7 “(J) any combination thereof.

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

11 “(6) ENVIRONMENT OF OPERATION.—The term
12 ‘environment of operation’ means the information
13 system and environment in which those systems op-
14 erate, including changing threats, vulnerabilities,
15 technologies, and missions and business practices.

16 “(7) FEDERAL INFORMATION SYSTEM.—The
17 term ‘Federal information system’ means an infor-
18 mation system used or operated by an executive
19 agency, by a contractor of an executive agency, or by
20 another organization on behalf of an executive agen-
21 cy.

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

24 “(A) actually or imminently jeopardizes
25 the integrity, confidentiality, or availability of

1 an information system or the information that
2 system controls, processes, stores, or transmits;
3 or

4 “(B) constitutes a violation of law or an
5 imminent threat of violation of a law, a security
6 policy, a security procedure, or an acceptable
7 use policy.

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

11 “(10) INFORMATION SECURITY.—The term ‘in-
12 formation security’ means protecting information
13 and information systems from disruption or unau-
14 thorized access, use, disclosure, modification, or de-
15 struction in order to provide—

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

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

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

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

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

7 “(13) MALICIOUS RECONNAISSANCE.—The term
8 ‘malicious reconnaissance’ means a method for ac-
9 tively probing or passively monitoring an information
10 system for the purpose of discerning technical
11 vulnerabilities of the information system, if such
12 method is associated with a known or suspected
13 cybersecurity threat.

14 “(14) NATIONAL SECURITY SYSTEM.—

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

21 “(i) the function, operation, or use of
22 which—

23 “(I) involves intelligence activi-
24 ties;

1 “(II) involves cryptologic activi-
2 ties related to national security;

3 “(III) involves command and
4 control of military forces;

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

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

11 “(ii) is protected at all times by proce-
12 dures established for information that have
13 been specifically authorized under criteria
14 established by an Executive Order or an
15 Act of Congress to be kept classified in the
16 interest of national defense or foreign pol-
17 icy.

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

23 “(15) OPERATIONAL CONTROL.—The term
24 ‘operational control’ means a security control for an

1 information system that primarily is implemented
2 and executed by people.

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

5 “(17) SECRETARY.—The term ‘Secretary’
6 means the Secretary of Commerce unless otherwise
7 specified.

8 “(18) SECURITY CONTROL.—The term ‘security
9 control’ means the management, operational, and
10 technical controls, including safeguards or counter-
11 measures, prescribed for an information system to
12 protect the confidentiality, integrity, and availability
13 of the system and its information.

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

21 **“§ 3553. Federal information security authority and**
22 **coordination**

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

1 “(1) issue compulsory and binding policies and
2 directives governing agency information security op-
3 erations, and require implementation of such policies
4 and directives, including—

5 “(A) policies and directives consistent with
6 the standards and guidelines promulgated
7 under section 11331 of title 40 to identify and
8 provide information security protections
9 prioritized and commensurate with the risk and
10 impact resulting from the unauthorized access,
11 use, disclosure, disruption, modification, or de-
12 struction of—

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

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

19 “(B) minimum operational requirements
20 for Federal Government to protect agency in-
21 formation systems and provide common situa-
22 tional awareness across all agency information
23 systems;

1 “(C) reporting requirements, consistent
2 with relevant law, regarding information secu-
3 rity incidents and cyber threat information;

4 “(D) requirements for agencywide informa-
5 tion security programs;

6 “(E) performance requirements and
7 metrics for the security of agency information
8 systems;

9 “(F) training requirements to ensure that
10 agencies are able to fully and timely comply
11 with the policies and directives issued by the
12 Secretary under this subchapter;

13 “(G) training requirements regarding pri-
14 vacy, civil rights, and civil liberties, and infor-
15 mation oversight for agency information secu-
16 rity personnel;

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

19 “(I) any other information security oper-
20 ations or information security requirements as
21 determined by the Secretary in coordination
22 with relevant agency heads; and

23 “(J) coordinating the development of
24 standards and guidelines under section 20 of
25 the National Institute of Standards and Tech-

1 nology Act (15 U.S.C. 278g–3) with agencies
2 and offices operating or exercising control of
3 national security systems (including the Na-
4 tional Security Agency) to assure, to the max-
5 imum extent feasible, that such standards and
6 guidelines are complementary with standards
7 and guidelines developed for national security
8 systems;

9 “(2) review the agencywide information security
10 programs under section 3554; and

11 “(3) designate an individual or an entity at
12 each cybersecurity center, among other responsibil-
13 ities—

14 “(A) to receive reports and information
15 about information security incidents, cyber
16 threat information, and deterioration of security
17 control affecting agency information systems;
18 and

19 “(B) to act on or share the information
20 under subparagraph (A) in accordance with this
21 subchapter.

22 “(b) CONSIDERATIONS.—When issuing policies and
23 directives under subsection (a), the Secretary shall con-
24 sider any applicable standards or guidelines developed by

1 the National Institute of Standards and Technology under
2 section 11331 of title 40.

3 “(c) LIMITATION OF AUTHORITY.—The authorities
4 of the Secretary under this section shall not apply to na-
5 tional security systems. Information security policies, di-
6 rectives, standards and guidelines for national security
7 systems shall be overseen as directed by the President and,
8 in accordance with that direction, carried out under the
9 authority of the heads of agencies that operate or exercise
10 authority over such national security systems.

11 “(d) STATUTORY CONSTRUCTION.—Nothing in this
12 subchapter shall be construed to alter or amend any law
13 regarding the authority of any head of an agency over
14 such agency.

15 **“§ 3554. Agency responsibilities**

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

17 “(1) be responsible for—

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

20 “(B) providing information security protec-
21 tions commensurate with the risk resulting
22 from unauthorized access, use, disclosure, dis-
23 ruption, modification, or destruction of—

24 “(i) information collected or main-
25 tained by the agency or by a contractor of

1 an agency or other organization on behalf
2 of an agency; and

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

9 “(i) information security standards
10 and guidelines promulgated under section
11 11331 of title 40;

12 “(ii) for any national security systems
13 operated or controlled by that agency, in-
14 formation security policies, directives,
15 standards and guidelines issued as directed
16 by the President; and

17 “(iii) for any non-national security
18 systems operated or controlled by that
19 agency, information security policies, direc-
20 tives, standards and guidelines issued
21 under section 3553;

22 “(D) ensuring that information security
23 management processes are integrated with
24 agency strategic and operational planning pro-
25 cesses;

1 “(E) reporting and sharing, for an agency
2 operating or exercising control of a national se-
3 curity system, information about information
4 security incidents, cyber threat information,
5 and deterioration of security controls to the in-
6 dividual or entity designated at each
7 cybersecurity center and to other appropriate
8 entities consistent with policies and directives
9 for national security systems issued as directed
10 by the President; and

11 “(F) reporting and sharing, for those
12 agencies operating or exercising control of non-
13 national security systems, information about in-
14 formation security incidents, cyber threat infor-
15 mation, and deterioration of security controls to
16 the individual or entity designated at each
17 cybersecurity center and to other appropriate
18 entities consistent with policies and directives
19 for non-national security systems as prescribed
20 under section 3553(a); including information to
21 assist the Secretary of Homeland Security with
22 carrying out the ongoing security analysis
23 under section 3555.

24 “(2) ensure that each senior agency official pro-
25 vides information security for the information and

1 information systems that support the operations and
2 assets under the senior agency official's control, in-
3 cluding by—

4 “(A) assessing the risk and impact that
5 could result from the unauthorized access, use,
6 disclosure, disruption, modification, or destruc-
7 tion of such information or information sys-
8 tems;

9 “(B) determining the level of information
10 security appropriate to protect such information
11 and information systems in accordance with
12 policies and directives issued under section
13 3553(a), and standards and guidelines promul-
14 gated under section 11331 of title 40 for infor-
15 mation security classifications and related re-
16 quirements;

17 “(C) implementing policies, procedures,
18 and capabilities to reduce risks to an acceptable
19 level in a cost-effective manner;

20 “(D) actively monitoring the effective im-
21 plementation of information security controls
22 and techniques; and

23 “(E) reporting information about informa-
24 tion security incidents, cyber threat informa-
25 tion, and deterioration of security controls in a

1 timely and adequate manner to the entity des-
2 ignated under section 3553(a)(3) in accordance
3 with paragraph (1);

4 “(3) assess and maintain the resiliency of infor-
5 mation technology systems critical to agency mission
6 and operations;

7 “(4) designate the agency Inspector General (or
8 an independent entity selected in consultation with
9 the Director and the Council of Inspectors General
10 on Integrity and Efficiency if the agency does not
11 have an Inspector General) to conduct the annual
12 independent evaluation required under section 3556,
13 and allow the agency Inspector General to contract
14 with an independent entity to perform such evalua-
15 tion;

16 “(5) delegate to the Chief Information Officer
17 or equivalent (or to a senior agency official who re-
18 ports to the Chief Information Officer or equiva-
19 lent)—

20 “(A) the authority and primary responsi-
21 bility to implement an agencywide information
22 security program; and

23 “(B) the authority to provide information
24 security for the information collected and main-
25 tained by the agency (or by a contractor, other

1 agency, or other source on behalf of the agency)
2 and for the information systems that support
3 the operations, assets, and mission of the agen-
4 cy (including any information system provided
5 or managed by a contractor, other agency, or
6 other source on behalf of the agency);

7 “(6) delegate to the appropriate agency official
8 (who is responsible for a particular agency system or
9 subsystem) the responsibility to ensure and enforce
10 compliance with all requirements of the agency’s
11 agencywide information security program in coordi-
12 nation with the Chief Information Officer or equiva-
13 lent (or the senior agency official who reports to the
14 Chief Information Officer or equivalent) under para-
15 graph (5);

16 “(7) ensure that an agency has trained per-
17 sonnel who have obtained any necessary security
18 clearances to permit them to assist the agency in
19 complying with this subchapter;

20 “(8) ensure that the Chief Information Officer
21 or equivalent (or the senior agency official who re-
22 ports to the Chief Information Officer or equivalent)
23 under paragraph (5), in coordination with other sen-
24 ior agency officials, reports to the agency head on
25 the effectiveness of the agencywide information secu-

1 rity program, including the progress of any remedial
2 actions; and

3 “(9) ensure that the Chief Information Officer
4 or equivalent (or the senior agency official who re-
5 ports to the Chief Information Officer or equivalent)
6 under paragraph (5) has the necessary qualifications
7 to administer the functions described in this sub-
8 chapter and has information security duties as a pri-
9 mary duty of that official.

10 “(b) CHIEF INFORMATION OFFICERS.—Each Chief
11 Information Officer or equivalent (or the senior agency of-
12 ficial who reports to the Chief Information Officer or
13 equivalent) under subsection (a)(5) shall—

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

17 “(A) detects, reports, contains, mitigates,
18 and responds to information security incidents
19 that impair adequate security of the agency’s
20 information or information system in a timely
21 manner and in accordance with the policies and
22 directives under section 3553; and

23 “(B) reports any information security inci-
24 dent under subparagraph (A) to the entity des-
25 ignated under section 3555;

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

3 “(3) develop, maintain, and oversee information
4 security policies, procedures, and control techniques
5 to address applicable requirements, including re-
6 quirements under section 3553 of this title and sec-
7 tion 11331 of title 40; and

8 “(4) train and oversee the agency personnel
9 who have significant responsibility for information
10 security with respect to that responsibility.

11 “(c) AGENCYWIDE INFORMATION SECURITY PRO-
12 GRAMS.—

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

16 “(A) security engineering throughout the
17 development and acquisition lifecycle;

18 “(B) security testing commensurate with
19 risk and impact;

20 “(C) mitigation of deterioration of security
21 controls commensurate with risk and impact;

22 “(D) risk-based continuous monitoring of
23 the operational status and security of agency
24 information systems to enable evaluation of the
25 effectiveness of and compliance with informa-

1 tion security policies, procedures, and practices,
2 including a relevant and appropriate selection of
3 security controls of information systems identi-
4 fied in the inventory under section 3505(c);

5 “(E) operation of appropriate technical ca-
6 pabilities in order to detect, mitigate, report,
7 and respond to information security incidents,
8 cyber threat information, and deterioration of
9 security controls in a manner that is consistent
10 with the policies and directives under section
11 3553, including—

12 “(i) mitigating risks associated with
13 such information security incidents;

14 “(ii) notifying and consulting with the
15 entity designated under section 3555; and

16 “(iii) notifying and consulting with, as
17 appropriate—

18 “(I) law enforcement and the rel-
19 evant Office of the Inspector General;
20 and

21 “(II) any other entity, in accord-
22 ance with law and as directed by the
23 President;

24 “(F) a process to ensure that remedial ac-
25 tion is taken to address any deficiencies in the

1 information security policies, procedures, and
2 practices of the agency; and

3 “(G) a plan and procedures to ensure the
4 continuity of operations for information systems
5 that support the operations and assets of the
6 agency.

7 “(2) RISK MANAGEMENT STRATEGIES.—Each
8 agencywide information security program under sub-
9 section (b)(2) shall include the development and
10 maintenance of a risk management strategy for in-
11 formation security. The risk management strategy
12 shall include—

13 “(A) consideration of information security
14 incidents, cyber threat information, and deterio-
15 ration of security controls; and

16 “(B) consideration of the consequences
17 that could result from the unauthorized access,
18 use, disclosure, disruption, modification, or de-
19 struction of information and information sys-
20 tems that support the operations and assets of
21 the agency, including any information system
22 provided or managed by a contractor, other
23 agency, or other source on behalf of the agency;

24 “(3) POLICIES AND PROCEDURES.—Each agen-
25 cywide information security program under sub-

1 section (b)(2) shall include policies and procedures
2 that—

3 “(A) are based on the risk management
4 strategy under paragraph (2);

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

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

11 “(D) ensure compliance with—

12 “(i) this subchapter; and

13 “(ii) any other applicable require-
14 ments.

15 “(4) TRAINING REQUIREMENTS.—Each agency-
16 wide information security program under subsection
17 (b)(2) shall include information security, privacy,
18 civil rights, civil liberties, and information oversight
19 training that meets any applicable requirements
20 under section 3553. The training shall inform each
21 information security personnel that has access to
22 agency information systems (including contractors
23 and other users of information systems that support
24 the operations and assets of the agency) of—

1 “(A) the information security risks associ-
2 ated with the information security personnel’s
3 activities; and

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

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

11 **“§ 3555. Multiagency ongoing threat assessment**

12 “(a) PURPOSE.—The purpose of this section is to
13 provide a framework for each agency to provide to the des-
14 ignee of the Secretary of Homeland Security under sub-
15 section (b)—

16 “(1) timely and actionable cyber threat infor-
17 mation; and

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

20 “(b) DESIGNEE.—The Secretary of Homeland Secu-
21 rity shall designate an entity within the Department of
22 Homeland Security—

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

25 “(A) based on cyber threat information;

1 “(B) based on agency information system
2 and environment of operation changes, includ-
3 ing—

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

6 “(ii) the security state, risk level, and
7 environment of operation of an agency in-
8 formation system, including—

9 “(I) a change in risk level due to
10 a new cyber threat;

11 “(II) a change resulting from a
12 new technology;

13 “(III) a change resulting from
14 the agency’s mission; and

15 “(IV) a change resulting from
16 the business practice; and

17 “(C) using automated processes to the
18 maximum extent possible—

19 “(i) to increase information system se-
20 curity;

21 “(ii) to reduce paper-based reporting
22 requirements; and

23 “(iii) to maintain timely and action-
24 able knowledge of the state of the informa-
25 tion system security.

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

6 “(3) COMPLIANCE.—The head of each appro-
7 priate agency shall be responsible for ensuring com-
8 pliance with this section. The Secretary of Home-
9 land Security, in consultation with the head of each
10 appropriate agency, shall—

11 “(A) monitor compliance under this sec-
12 tion;

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

14 “(i) to adopt any technology, system,
15 or method that facilitates continuous moni-
16 toring of an agency information system;
17 and

18 “(ii) to adopt any technology, system,
19 or method that satisfies a requirement
20 under this section.

21 “(4) LIMITATION OF AUTHORITY.—The au-
22 thorities of the Secretary of Homeland Security
23 under this section shall not apply to national secu-
24 rity systems.

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

8 **“§ 3556. Independent evaluations**

9 “(a) IN GENERAL.—The Council of Inspectors Gen-
10 eral on Integrity and Efficiency, in consultation with the
11 Director and the Secretary of Homeland Security, the Sec-
12 retary of Commerce, and the Secretary of Defense, shall
13 issue and maintain criteria for the timely, cost-effective,
14 risk-based, and independent evaluation of each agencywide
15 information security program (and practices) to determine
16 the effectiveness of the agencywide information security
17 program (and practices). The criteria shall include meas-
18 ures to assess any conflicts of interest in the performance
19 of the evaluation and whether the agencywide information
20 security program includes appropriate safeguards against
21 disclosure of information where such disclosure may ad-
22 versely affect information security.

23 “(b) ANNUAL INDEPENDENT EVALUATIONS.—Each
24 agency shall perform an annual independent evaluation of

1 its agencywide information security program (and prac-
2 tices) in accordance with the criteria under subsection (a).

3 “(c) DISTRIBUTION OF REPORTS.—Not later than 30
4 days after receiving an independent evaluation under sub-
5 section (b), each agency head shall transmit a copy of the
6 independent evaluation to the Secretary of Homeland Se-
7 curity, the Secretary of Commerce, and the Secretary of
8 Defense.

9 “(d) NATIONAL SECURITY SYSTEMS.—Evaluations
10 involving national security systems shall be conducted as
11 directed by President.

12 **“§ 3557. National security systems.**

13 “The head of each agency operating or exercising
14 control of a national security system shall be responsible
15 for ensuring that the agency—

16 “(1) provides information security protections
17 commensurate with the risk and magnitude of the
18 harm resulting from the unauthorized access, use,
19 disclosure, disruption, modification, or destruction of
20 the information contained in such system; and

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

25 (b) SAVINGS PROVISIONS.—

1 (1) POLICY AND COMPLIANCE GUIDANCE.—Pol-
2 icy and compliance guidance issued by the Director
3 before the date of enactment of this Act under sec-
4 tion 3543(a)(1) of title 44, United States Code, (as
5 in effect on the day before the date of enactment of
6 this Act) shall continue in effect, according to its
7 terms, until modified, terminated, superseded, or re-
8 pealed pursuant to section 3553(a)(1) of title 44,
9 United States Code.

10 (2) STANDARDS AND GUIDELINES.—Standards
11 and guidelines issued by the Secretary of Commerce
12 or by the Director before the date of enactment of
13 this Act under section 11331(a)(1) of title 40,
14 United States Code, (as in effect on the day before
15 the date of enactment of this Act) shall continue in
16 effect, according to their terms, until modified, ter-
17 minated, superseded, or repealed pursuant to section
18 11331(a)(1) of title 40, United States Code, as
19 amended by this Act.

20 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

21 (1) CHAPTER ANALYSIS.—The chapter analysis
22 for chapter 35 of title 44, United States Code, is
23 amended—

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

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

3 (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.”.

4 (2) OTHER REFERENCES.—

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

9 (B) Section 2222(j)(5) of title 10, United
10 States Code, is amended by striking “section
11 3542(b)(2)” and inserting “section 3552”.

12 (C) Section 2223(c)(3) of title 10, United
13 States Code, is amended, by striking “section
14 3542(b)(2)” and inserting “section 3552”.

15 (D) Section 2315 of title 10, United States
16 Code, is amended by striking “section
17 3542(b)(2)” and inserting “section 3552”.

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

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

4 (ii) in subsection (c)(3), by striking
5 “Director of the Office of Management and
6 Budget” and inserting “Secretary of Com-
7 merce”;

8 (iii) in subsection (d)(1), by striking
9 “Director of the Office of Management and
10 Budget” and inserting “Secretary of Com-
11 merce”;

12 (iv) in subsection (d)(8) by striking
13 “Director of the Office of Management and
14 Budget” and inserting “Secretary of Com-
15 merce”;

16 (v) in subsection (d)(8), by striking
17 “submitted to the Director” and inserting
18 “submitted to the Secretary”;

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

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

1 (F) Section 8(d)(1) of the Cyber Security
2 Research and Development Act (15 U.S.C.
3 7406(d)(1)) is amended by striking “section
4 3534(b)” and inserting “section 3554(b)(2)”.

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

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

8 **“§ 11331. Responsibilities for Federal information sys-**
9 **tems standards**

10 “(a) STANDARDS AND GUIDELINES.—

11 “(1) AUTHORITY TO PRESCRIBE.—Except as
12 provided under paragraph (2), the Secretary of
13 Commerce shall prescribe standards and guidelines
14 pertaining to Federal information systems—

15 “(A) in consultation with the Secretary of
16 Homeland Security; and

17 “(B) on the basis of standards and guide-
18 lines developed by the National Institute of
19 Standards and Technology under paragraphs
20 (2) and (3) of section 20(a) of the National In-
21 stitute of Standards and Technology Act (15
22 U.S.C. 278g-3(a)(2) and (a)(3)) .

23 “(2) NATIONAL SECURITY SYSTEMS.—Stand-
24 ards and guidelines for national security systems
25 shall be developed, prescribed, enforced, and over-

1 seen as otherwise authorized by law and as directed
2 by the President.

3 “(b) MANDATORY STANDARDS AND GUIDELINES.—

4 “(1) AUTHORITY TO MAKE MANDATORY STAND-
5 ARDS AND GUIDELINES.—The Secretary of Com-
6 merce shall make standards and guidelines under
7 subsection (a)(1) compulsory and binding to the ex-
8 tent determined necessary by the Secretary of Com-
9 merce to improve the efficiency of operation or secu-
10 rity of Federal information systems.

11 “(2) REQUIRED MANDATORY STANDARDS AND
12 GUIDELINES.—

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

16 “(i) provide minimum information se-
17 curity requirements as determined under
18 section 20(b) of the National Institute of
19 Standards and Technology Act (15 U.S.C.
20 278g-3(b)); and

21 “(ii) are otherwise necessary to im-
22 prove the security of Federal information
23 and information systems.

1 “(B) BINDING EFFECT.—Information se-
2 curity standards under subparagraph (A) shall
3 be compulsory and binding.

4 “(c) EXERCISE OF AUTHORITY.—To ensure fiscal
5 and policy consistency, the Secretary of Commerce shall
6 exercise the authority conferred by this section subject to
7 direction by the President and in coordination with the
8 Director.

9 “(d) APPLICATION OF MORE STRINGENT STAND-
10 ARDS AND GUIDELINES.—The head of an executive agen-
11 cy may employ standards for the cost-effective information
12 security for information systems within or under the su-
13 pervision of that agency that are more stringent than the
14 standards and guidelines the Secretary of Commerce pre-
15 scribes under this section if the more stringent standards
16 and guidelines—

17 “(1) contain at least the applicable standards
18 and guidelines made compulsory and binding by the
19 Secretary of Commerce; and

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

23 “(e) DECISIONS ON PROMULGATION OF STANDARDS
24 AND GUIDELINES.—The decision by the Secretary of
25 Commerce regarding the promulgation of any standard or

1 guideline under this section shall occur not later than 6
2 months after the date of submission of the proposed stand-
3 ard to the Secretary of Commerce by the National Insti-
4 tute of Standards and Technology under section 20 of the
5 National Institute of Standards and Technology Act (15
6 U.S.C. 278g-3).

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

15 “(g) DEFINITIONS.—In this section:

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

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

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

1 **SEC. 203. NO NEW FUNDING.**

2 An applicable Federal agency shall carry out the pro-
3 visions of this title with existing facilities and funds other-
4 wise available, through such means as the head of the
5 agency considers appropriate.

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

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

9 (1) in paragraph (2), by striking “and the Di-
10 rector of the Office of Management and Budget”
11 and inserting “, the Secretary of Commerce, and the
12 Secretary of Homeland Security”; and

13 (2) in paragraph (3), by inserting “, the Sec-
14 retary of Homeland Security,” after “the Secretary
15 of Commerce”.

16 **TITLE III—CRIMINAL PENALTIES**

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

18 **IN CONNECTION WITH COMPUTERS.**

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

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

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

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

5 “(B) a fine under this title or imprisonment for
6 not more than ten years, or both, in the case of an
7 offense under paragraph (a)(2) of this section, if—

8 “(i) the offense was committed for pur-
9 poses of commercial advantage or private finan-
10 cial gain;

11 “(ii) the offense was committed in the fur-
12 therance of any criminal or tortuous act in vio-
13 lation of the Constitution or laws of the United
14 States, or of any State; or

15 “(iii) the value of the information obtained,
16 or that would have been obtained if the offense
17 was completed, exceeds \$5,000;

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

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

24 “(5)(A) except as provided in subparagraph
25 (C), a fine under this title, imprisonment for not

1 more than 20 years, or both, in the case of an of-
2 fense under subsection (a)(5)(A) of this section, if
3 the offense caused—

4 “(i) loss to 1 or more persons during any
5 1-year period (and, for purposes of an inves-
6 tigation, prosecution, or other proceeding
7 brought by the United States only, loss result-
8 ing from a related course of conduct affecting
9 1 or more other protected computers) aggreg-
10 ating at least \$5,000 in value;

11 “(ii) the modification or impairment, or
12 potential modification or impairment, of the
13 medical examination, diagnosis, treatment, or
14 care of 1 or more individuals;

15 “(iii) physical injury to any person;

16 “(iv) a threat to public health or safety;

17 “(v) damage affecting a computer used by,
18 or on behalf of, an entity of the United States
19 Government in furtherance of the administra-
20 tion of justice, national defense, or national se-
21 curity; or

22 “(vi) damage affecting 10 or more pro-
23 tected computers during any 1-year period;

24 “(B) a fine under this title, imprisonment for
25 not more than 20 years, or both, in the case of an

1 offense under subsection (a)(5)(B), if the offense
2 caused a harm provided in clause (i) through (vi) of
3 subparagraph (A) of this subsection;

4 “(C) if the offender attempts to cause or know-
5 ingly or recklessly causes death from conduct in vio-
6 lation of subsection (a)(5)(A), a fine under this title,
7 imprisonment for any term of years or for life, or
8 both;

9 “(D) a fine under this title, imprisonment for
10 not more than 10 years, or both, for any other of-
11 fense under subsection (a)(5);

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

15 “(F) a fine under this title or imprisonment for
16 not more than 10 years, or both, in the case of an
17 offense under subsection (a)(7) of this section.”.

18 **SEC. 302. TRAFFICKING IN PASSWORDS.**

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

21 “(6) knowingly and with intent to defraud traf-
22 fics (as defined in section 1029) in any password or
23 similar information or means of access through
24 which a protected computer (as defined in subpara-

1 graphs (A) and (B) of subsection (e)(2)) may be
2 accessed without authorization.”.

3 **SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER**
4 **FRAUD OFFENSES.**

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

8 **SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD**
9 **AND RELATED ACTIVITY IN CONNECTION**
10 **WITH COMPUTERS.**

11 Section 1030 of title 18, United States Code, is
12 amended by striking subsections (i) and (j) and inserting
13 the following:

14 “(i) CRIMINAL FORFEITURE.—

15 “(1) The court, in imposing sentence on any
16 person convicted of a violation of this section, or
17 convicted of conspiracy to violate this section, shall
18 order, in addition to any other sentence imposed and
19 irrespective of any provision of State law, that such
20 person forfeit to the United States—

21 “(A) such persons interest in any property,
22 real or personal, that was used, or intended to
23 be used, to commit or facilitate the commission
24 of such violation; and

1 “(B) any property, real or personal, consti-
2 tuting or derived from any gross proceeds, or
3 any property traceable to such property, that
4 such person obtained, directly or indirectly, as
5 a result of such violation.

6 “(2) The criminal forfeiture of property under
7 this subsection, including any seizure and disposition
8 of the property, and any related judicial or adminis-
9 trative proceeding, shall be governed by the provi-
10 sions of section 413 of the Comprehensive Drug
11 Abuse Prevention and Control Act of 1970 (21
12 U.S.C. 853), except subsection (d) of that section.

13 “(j) CIVIL FORFEITURE.—

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

17 “(A) Any property, real or personal, that
18 was used, or intended to be used, to commit or
19 facilitate the commission of any violation of this
20 section, or a conspiracy to violate this section.

21 “(B) Any property, real or personal, con-
22 stituting or derived from any gross proceeds ob-
23 tained directly or indirectly, or any property
24 traceable to such property, as a result of the

1 or any combination of those matters, whether pub-
2 licly or privately owned or operated, including—

3 “(A) gas and oil production, storage, con-
4 version, and delivery systems;

5 “(B) water supply systems;

6 “(C) telecommunication networks;

7 “(D) electrical power generation and deliv-
8 ery systems;

9 “(E) finance and banking systems;

10 “(F) emergency services;

11 “(G) transportation systems and services;

12 and

13 “(H) government operations that provide
14 essential services to the public; and

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

17 “(b) OFFENSE.—It shall be unlawful, during and in
18 relation to a felony violation of section 1030, to knowingly
19 cause or attempt to cause damage to a critical infrastruc-
20 ture computer if the damage results in (or, in the case
21 of an attempt, if completed, would have resulted in) the
22 substantial impairment—

23 “(1) of the operation of the critical infrastruc-
24 ture computer; or

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

3 “(c) PENALTY.—Any person who violates subsection
4 (b) shall be—

5 “(1) fined under this title;

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

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

9 “(d) CONSECUTIVE SENTENCE.—Notwithstanding
10 any other provision of law—

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

13 “(2) except as provided in paragraph (4), no
14 term of imprisonment imposed on a person under
15 this section shall run concurrently with any other
16 term of imprisonment, including any term of impris-
17 onment imposed on the person under any other pro-
18 vision of law, including any term of imprisonment
19 imposed for a felony violation of section 1030;

20 “(3) in determining any term of imprisonment
21 to be imposed for a felony violation of section 1030,
22 a court shall not in any way reduce the term to be
23 imposed for such crime so as to compensate for, or
24 otherwise take into account, any separate term of

1 imprisonment imposed or to be imposed for a viola-
2 tion of this section; and

3 “(4) a term of imprisonment imposed on a per-
4 son for a violation of this section may, in the discre-
5 tion of the court, run concurrently, in whole or in
6 part, only with another term of imprisonment that
7 is imposed by the court at the same time on that
8 person for an additional violation of this section,
9 provided that such discretion shall be exercised in
10 accordance with any applicable guidelines and policy
11 statements issued by the United States Sentencing
12 Commission pursuant to section 994 of title 28.”

13 (b) **TECHNICAL AND CONFORMING AMENDMENT.**—
14 The chapter analysis for chapter 47 of title 18, United
15 States Code, is amended by inserting after the item relat-
16 ing to section 1030 the following:

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

17 **SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHOR-**
18 **IZED USE.**

19 Section 1030(e)(6) of title 18, United States Code,
20 is amended by striking “alter;” and inserting “alter, but
21 does not include access in violation of a contractual obliga-
22 tion or agreement, such as an acceptable use policy or
23 terms of service agreement, with an Internet service pro-
24 vider, Internet website, or non-government employer, if

1 such violation constitutes the sole basis for determining
2 that access to a protected computer is unauthorized;”.

3 **TITLE IV—CYBERSECURITY**
4 **RESEARCH AND DEVELOPMENT**

5 **SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING**
6 **PROGRAM PLANNING AND COORDINATION.**

7 (a) GOALS AND PRIORITIES.—Section 101 of the
8 High-Performance Computing Act of 1991 (15 U.S.C.
9 5511) is amended by adding at the end the following:

10 “(d) GOALS AND PRIORITIES.—The goals and prior-
11 ities for Federal high-performance computing research,
12 development, networking, and other activities under sub-
13 section (a)(2)(A) shall include—

14 “(1) encouraging and supporting mechanisms
15 for interdisciplinary research and development in
16 networking and information technology, including
17 through collaborations—

18 “(A) across agencies;

19 “(B) across Program Component Areas;

20 “(C) with industry;

21 “(D) with institutions of higher education;

22 “(E) with Federal laboratories (as defined
23 in section 4 of the Stevenson-Wydler Tech-
24 nology Innovation Act of 1980 (15 U.S.C.
25 3703)); and

1 “(F) with international organizations;
2 “(2) addressing national, multi-agency, multi-
3 faceted challenges of national importance; and
4 “(3) fostering the transfer of research and de-
5 velopment results into new technologies and applica-
6 tions for the benefit of society.”.

7 (b) DEVELOPMENT OF STRATEGIC PLAN.—Section
8 101 of the High-Performance Computing Act of 1991 (15
9 U.S.C. 5511) is further amended by adding at the end
10 the following:

11 “(e) STRATEGIC PLAN.—

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

22 “(2) CONTENTS.—The strategic plan shall
23 specify—

24 “(A) the near-term objectives for the Pro-
25 gram;

1 “(B) the long-term objectives for the Pro-
2 gram;

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

5 “(D) the metrics that will be used to as-
6 sess any progress made toward achieving the
7 near-term objectives and the long-term objec-
8 tives; and

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

11 “(3) RECOMMENDATIONS.—When developing
12 the strategic plan under paragraph (1), such agen-
13 cies shall take into consideration the recommenda-
14 tions of—

15 “(A) the advisory committee under sub-
16 section (b); and

17 “(B) the stakeholders whose input was so-
18 licited by the National Coordination Office, as
19 required under section 102(b)(3).

20 “(4) IMPLEMENTATION ROADMAP.—Such agen-
21 cies shall develop and annually update an implemen-
22 tation roadmap for the strategic plan, which shall—

23 “(A) specify the role of each Federal agen-
24 cy in carrying out or sponsoring research and
25 development to meet the research objectives of

1 the strategic plan, including a description of
2 how progress toward the research objectives will
3 be evaluated, with consideration of any relevant
4 recommendations of the advisory committee;

5 “(B) specify the funding allocated to each
6 major research objective of the strategic plan
7 and the source of funding by agency for the
8 current fiscal year; and

9 “(C) estimate the funding required for
10 each major research objective of the strategic
11 plan for the next 3 fiscal years.

12 “(5) REPORT TO CONGRESS.—The Director of
13 the National Coordination Office shall transmit the
14 strategic plan under this subsection, including the
15 implementation roadmap and any updates under
16 paragraph (4), 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, Space, and
22 Technology 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 further 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 the
20 agencies participating in the Program to allocate the
21 level of resources and management attention nec-
22 essary to ensure that—

23 “(i) the strategic plan under subsection (e)
24 is developed and executed effectively; and

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

3 “(F) working with the Office of Management
4 and Budget, direct the Office of Science and Tech-
5 nology Policy and the agencies participating in the
6 Program to establish a mechanism (consistent with
7 existing law) to track all ongoing and completed re-
8 search and development projects and associated
9 funding;”.

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

13 (1) in paragraph (1)—

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

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

22 (2) by amending paragraph (2) to read as fol-
23 lows:

24 “(2) In addition to the duties under paragraph (1),
25 the advisory committee shall conduct periodic evaluations

1 of the funding, management, coordination, implementa-
2 tion, and activities of the Program. The advisory com-
3 mittee shall report its findings and recommendations not
4 less frequently than once every 3 fiscal years to the Com-
5 mittee on Commerce, Science, and Transportation of the
6 Senate and the Committee on Science, Space, and Tech-
7 nology of the House of Representatives. The report shall
8 be submitted in conjunction with the update of the stra-
9 tegic plan.”.

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

13 (1) in subparagraph (C)—

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

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

21 (2) in subparagraph (D)—

22 (A) by striking “each Program Component
23 Area,” and inserting “each Program Compo-
24 nent Area and each research area supported in
25 accordance with section 104,”;

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

4 (C) by striking “and” after the semicolon;
5 (3) by redesignating subparagraph (E) as sub-
6 paragraph (G); and

7 (4) by inserting after subparagraph (D) the fol-
8 lowing:

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

15 “(F) include—

16 “(i) a description of the funding required
17 by the Office of Science and Technology Policy
18 to perform the functions under section 102(b)
19 for the next fiscal year by category of activity;

20 “(ii) a description of the funding required
21 by the Office of Science and Technology Policy
22 to perform the functions under section 102(b)
23 for the current fiscal year by category of activ-
24 ity; and

1 “(iii) the amount of funding provided for
2 the Office of Science and Technology Policy for
3 the current fiscal year by each agency partici-
4 pating in the Program; and”.

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

8 (1) by redesignating paragraphs (6) and (7) as
9 paragraphs (7) and (8), respectively;

10 (2) by redesignating paragraph (3) as para-
11 graph (6);

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

14 (4) by inserting before paragraph (2), as redes-
15 ignated, the following:

16 “(1) ‘cyber-physical systems’ means physical or
17 engineered systems whose networking and informa-
18 tion technology functions and physical elements are
19 deeply integrated and are actively connected to the
20 physical world through sensors, actuators, or other
21 means to perform monitoring and control func-
22 tions;”;

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

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

2 (A) by striking “high-performance com-
3 puting” and inserting “networking and infor-
4 mation technology”; and

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

7 (7) in paragraph (5), by striking “network re-
8 ferred to as” and all that follows through “section
9 102” and inserting “network, including advanced
10 computer networks of Federal agencies and depart-
11 ments”; and

12 (8) in paragraph (7), as redesignated, by strik-
13 ing “National High-Performance Computing Pro-
14 gram” and inserting “networking and information
15 technology research and development program”.

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

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

21 **“SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPOR-
22 TANCE.**

23 “(a) IN GENERAL.—The Program shall encourage
24 agencies under section 101(a)(3)(B) to support, maintain,
25 and improve national, multi-agency, multi-faceted, re-

1 search and development activities in networking and infor-
2 mation technology directed toward application areas that
3 have the potential for significant contributions to national
4 economic competitiveness and for other significant societal
5 benefits.

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

10 “(c) CHARACTERISTICS.—

11 “(1) IN GENERAL.—Research and development
12 activities under this section—

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

16 “(B) shall leverage, when possible, Federal
17 investments through collaboration with related
18 State initiatives;

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

1 “(D) shall involve collaborations among re-
2 searchers in institutions of higher education
3 and industry; and

4 “(E) may involve collaborations among
5 nonprofit research institutions and Federal lab-
6 oratories, as appropriate.

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

11 “(3) AGENCY COLLABORATION.—If 2 or more
12 agencies identified in section 101(a)(3)(B), or other
13 appropriate agencies, are working on large-scale re-
14 search and development activities in the same area
15 of national importance, then such agencies shall
16 strive to collaborate through joint solicitation and se-
17 lection of applications for support and subsequent
18 funding of projects.

19 “(4) MULTIDISCIPLINARY RESEARCH CEN-
20 TERS.—Research and development activities under
21 this section shall be supported through multidisci-
22 plinary research centers, including Federal labora-
23 tories, that are organized to investigate basic re-
24 search questions and carry out technology dem-
25 onstration activities in areas described in subsection

1 (a). Research may be carried out through existing
2 multidisciplinary centers, including those authorized
3 under section 7024(b)(2) of the America COM-
4 PETES Act (42 U.S.C. 1862o-10(2)).”.

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

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

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

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

13 “(J) provide for increased understanding of the
14 scientific principles of cyber-physical systems and
15 improve the methods available for the design, devel-
16 opment, and operation of cyber-physical systems
17 that are characterized by high reliability, safety, and
18 security; and

19 “(K) provide for research and development on
20 human-computer interactions, visualization, and big
21 data.”.

22 (c) TASK FORCE.—Title I of the High-Performance
23 Computing Act of 1991 (15 U.S.C. 5511 et seq.) is further
24 amended by adding at the end the following:

1 **“SEC. 105. CYBER-PHYSICAL SYSTEMS UNIVERSITY-INDUS-**
2 **TRY TASK FORCE.**

3 “(a) ESTABLISHMENT.—Not later than 180 days
4 after the date of enactment of the Strengthening and En-
5 hancing Cybersecurity by Using Research, Education, In-
6 formation, and Technology Act of 2012, the Director of
7 the National Coordination Office under section 102 shall
8 convene a task force to explore mechanisms for carrying
9 out collaborative research and development activities for
10 cyber-physical systems (including the related technologies
11 required to enable these systems) through a consortium
12 or other appropriate entity with participants from institu-
13 tions of higher education, Federal laboratories, and indus-
14 try.

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

16 “(1) develop options for a collaborative model
17 and an organizational structure for such entity
18 under which the joint research and development ac-
19 tivities could be planned, managed, and conducted
20 effectively, including mechanisms for the allocation
21 of resources among the participants in such entity
22 for support of such activities;

23 “(2) propose a process for developing a re-
24 search and development agenda for such entity, in-
25 cluding guidelines to ensure an appropriate scope of
26 work focused on nationally significant challenges and

1 requiring collaboration and to ensure the develop-
2 ment of related scientific and technological mile-
3 stones;

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

7 “(4) propose guidelines for assigning intellec-
8 tual property rights and for transferring research re-
9 sults to the private sector; and

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

13 “(c) COMPOSITION.—In establishing the task force
14 under subsection (a), the Director of the National Coordi-
15 nation Office shall appoint an equal number of individuals
16 from institutions of higher education and from industry
17 with knowledge and expertise in cyber-physical systems,
18 and may appoint not more than 2 individuals from Fed-
19 eral laboratories.

20 “(d) REPORT.—Not later than 1 year after the date
21 of enactment of the Strengthening and Enhancing
22 Cybersecurity by Using Research, Education, Information,
23 and Technology Act of 2012, the Director of the National
24 Coordination Office shall transmit to the Committee on
25 Commerce, Science, and Transportation of the Senate and

1 the Committee on Science, Space, and Technology of the
2 House of Representatives a report describing the findings
3 and recommendations of the task force.

4 “(e) **TERMINATION.**—The task force shall terminate
5 upon transmittal of the report required under subsection
6 (d).

7 “(f) **COMPENSATION AND EXPENSES.**—Members of
8 the task force shall serve without compensation.”.

9 **SEC. 403. PROGRAM IMPROVEMENTS.**

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

12 **“SEC. 102. NATIONAL COORDINATION OFFICE.**

13 “(a) **OFFICE.**—The Director shall continue a Na-
14 tional Coordination Office with a Director and full-time
15 staff.

16 “(b) **FUNCTIONS.**—The National Coordination Office
17 shall—

18 “(1) provide technical and administrative sup-
19 port to—

20 “(A) the agencies participating in planning
21 and implementing the Program, including such
22 support as needed in the development of the
23 strategic plan under section 101(e); and

24 “(B) the advisory committee established
25 under section 101(b);

1 “(2) serve as the primary point of contact on
2 Federal networking and information technology ac-
3 tivities for government organizations, academia, in-
4 dustry, professional societies, State computing and
5 networking technology programs, interested citizen
6 groups, and others to exchange technical and pro-
7 grammatic information;

8 “(3) solicit input and recommendations from a
9 wide range of stakeholders during the development
10 of each strategic plan required under section 101(e)
11 through the convening of at least 1 workshop with
12 invitees from academia, industry, Federal labora-
13 tories, and other relevant organizations and institu-
14 tions;

15 “(4) conduct public outreach, including the dis-
16 semination of findings and recommendations of the
17 advisory committee, as appropriate; and

18 “(5) promote access to and early application of
19 the technologies, innovations, and expertise derived
20 from Program activities to agency missions and sys-
21 tems across the Federal Government and to United
22 States industry.

23 “(c) SOURCE OF FUNDING.—

24 “(1) IN GENERAL.—The operation of the Na-
25 tional Coordination Office shall be supported by

1 funds from each agency participating in the Pro-
2 gram.

3 “(2) SPECIFICATIONS.—The portion of the total
4 budget of such Office that is provided by each agen-
5 cy for each fiscal year shall be in the same propor-
6 tion as each such agency’s share of the total budget
7 for the Program for the previous fiscal year, as spec-
8 ified in the report required under section
9 101(a)(3).”.

10 **SEC. 404. CLOUD COMPUTING SERVICES FOR RESEARCH.**

11 Title I of the High-Performance Computing Act of
12 1991 (15 U.S.C. 5511) is further amended by adding at
13 the end the following:

14 **“SEC. 106. CLOUD COMPUTING SERVICES FOR RESEARCH.**

15 “(a) INTERAGENCY WORKING GROUP.—Not later
16 than 180 days after the date of enactment of the
17 Strengthening and Enhancing Cybersecurity by Using Re-
18 search, Education, Information, and Technology Act of
19 2012, the Director of the National Coordination Office,
20 working through the National Science and Technology
21 Council, shall convene an interagency working group to
22 examine—

23 “(1) the research and development needed—

24 “(A) to enhance the effectiveness and effi-
25 ciency of cloud computing environments;

1 “(B) to increase the trustworthiness of
2 cloud applications and infrastructure; and

3 “(C) to enhance the foundations of cloud
4 architectures, programming models, and inter-
5 operability; and

6 “(2) the potential use of cloud computing for
7 federally-funded science and engineering research,
8 including issues around funding mechanisms and
9 policies for the use of cloud computing services for
10 such research.

11 “(b) CONSULTATION.—In carrying out the tasks in
12 paragraphs (1) and (2) of subsection (a), the working
13 group shall consult with academia, industry, Federal lab-
14 oratories, and other relevant organizations and institu-
15 tions, as appropriate.

16 “(c) REPORT.—Not later than 1 year after the date
17 of enactment of the Strengthening and Enhancing
18 Cybersecurity by Using Research, Education, Information,
19 and Technology Act of 2012, the Director of the National
20 Coordination Office shall transmit to the Committee on
21 Science, Space, and Technology of the House of Rep-
22 resentatives and the Committee on Commerce, Science,
23 and Transportation of the Senate a report describing the
24 findings and any recommendations of the working group.

1 “(d) **TERMINATION.**—The interagency working group
2 shall terminate upon transmittal of the report required
3 under subsection (c).”.

4 **SEC. 405. CYBERSECURITY UNIVERSITY-INDUSTRY TASK**
5 **FORCE.**

6 (a) **ESTABLISHMENT OF UNIVERSITY-INDUSTRY**
7 **TASK FORCE.**—Not later than 180 days after the date of
8 enactment of this Act, the Director of the Office of Science
9 and Technology Policy shall convene a task force to ex-
10 plore mechanisms for carrying out collaborative research,
11 development, education, and training activities for
12 cybersecurity through a consortium or other appropriate
13 entity with participants from institutions of higher edu-
14 cation and industry.

15 (b) **FUNCTIONS.**—The task force shall—

16 (1) develop options for a collaborative model
17 and an organizational structure for such entity
18 under which the joint research and development ac-
19 tivities could be planned, managed, and conducted
20 effectively, including mechanisms for the allocation
21 of resources among the participants in such entity
22 for support of such activities;

23 (2) propose a process for developing a research
24 and development agenda for such entity, including
25 guidelines to ensure an appropriate scope of work fo-

1 cused on nationally significant challenges and requir-
2 ing collaboration;

3 (3) define the roles and responsibilities for the
4 participants from institutions of higher education
5 and industry in such entity;

6 (4) propose guidelines for assigning intellectual
7 property rights, for the transfer of research and de-
8 velopment results to the private sector; and

9 (5) make recommendations for how such entity
10 could be funded from Federal, State, and nongovern-
11 mental sources.

12 (c) COMPOSITION.—In establishing the task force
13 under subsection (a), the Director of the Office of Science
14 and Technology Policy shall appoint an equal number of
15 individuals from institutions of higher education, including
16 minority-serving institutions and community colleges, and
17 from industry with knowledge and expertise in
18 cybersecurity.

19 (d) REPORT.—Not later than 12 months after the
20 date of enactment of this Act, the Director of the Office
21 of Science and Technology Policy shall transmit to the
22 Congress a report describing the findings and rec-
23 ommendations of the task force.

1 (e) TERMINATION.—The task force shall terminate
2 upon transmittal of the report required under subsection
3 (d).

4 (f) COMPENSATION AND EXPENSES.—Members of
5 the task force shall serve without compensation.

6 **SEC. 406. IMPROVING EDUCATION OF NETWORKING AND**
7 **INFORMATION TECHNOLOGY, INCLUDING**
8 **HIGH PERFORMANCE COMPUTING.**

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

11 (1) by redesignating paragraphs (2) through
12 (4) as paragraphs (3) through (5), respectively; and

13 (2) by inserting after paragraph (1) the fol-
14 lowing new paragraph:

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

1 **SEC. 407. CONFORMING AND TECHNICAL AMENDMENTS TO**
2 **THE HIGH-PERFORMANCE COMPUTING ACT**
3 **OF 1991.**

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

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

9 (2) in paragraph (1)—

10 (A) in the matter preceding subparagraph
11 (A), by striking “high-performance computing”
12 and inserting “networking and information
13 technology”;

14 (B) in subparagraphs (A), (F), and (G), by
15 striking “high-performance computing” each
16 place it appears and inserting “networking and
17 information technology”; and

18 (C) in subparagraph (H), by striking
19 “high-performance” and inserting “high-end”;
20 and

21 (3) in paragraph (2)—

22 (A) by striking “high-performance com-
23 puting and” and inserting “networking and in-
24 formation technology, and”; and

1 (B) by striking “high-performance com-
2 puting network” and inserting “networking and
3 information technology”.

4 (b) TITLE HEADING.—The heading of title I of the
5 High-Performance Computing Act of 1991 (105 Stat.
6 1595) is amended by striking “**HIGH-PERFORM-**
7 **ANCE COMPUTING**” and inserting “**NET-**
8 **WORKING AND INFORMATION TECH-**
9 **NOLOGY**”.

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

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

17 (2) in subsection (a)—

18 (A) in the subsection heading, by striking
19 “NATIONAL HIGH-PERFORMANCE COMPUTING”
20 and inserting “NETWORKING AND INFORMA-
21 TION TECHNOLOGY RESEARCH AND DEVELOP-
22 MENT”;

23 (B) in paragraph (1)—

24 (i) by striking “National High-Per-
25 formance Computing Program” and insert-

1 ing “networking and information tech-
2 nology research and development pro-
3 gram”;

4 (ii) in subparagraph (A), by striking
5 “high-performance computing, including
6 networking” and inserting “networking
7 and information technology”;

8 (iii) in subparagraphs (B) and (G), by
9 striking “high-performance” each place it
10 appears and inserting “high-end”; and

11 (iv) in subparagraph (C), by striking
12 “high-performance computing and net-
13 working” and inserting “high-end com-
14 puting, distributed, and networking”; and
15 (C) in paragraph (2)—

16 (i) in subparagraphs (A) and (C)—

17 (I) by striking “high-performance
18 computing” each place it appears and
19 inserting “networking and information
20 technology”; and

21 (II) by striking “development,
22 networking,” each place it appears
23 and inserting “development,”; and

24 (ii) in subparagraphs (G) and (H), as
25 redesignated by section 401(d) of this Act,

1 by striking “high-performance” each place
2 it appears and inserting “high-end”;

3 (3) in subsection (b)(1), in the matter pre-
4 ceding subparagraph (A), by striking “high-perform-
5 ance computing” each place it appears and inserting
6 “networking and information technology”; and

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

10 (d) SECTION 201.—Section 201(a)(1) of the High-
11 Performance Computing Act of 1991 (15 U.S.C.
12 5521(a)(1)) is amended by striking “high-performance
13 computing and advanced high-speed computer net-
14 working” and inserting “networking and information tech-
15 nology research and development”.

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

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

23 (1) in paragraph (1), by striking “high-per-
24 formance computing and networking” and inserting
25 “networking and information technology”; and

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

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

6 (1) in subsection (a)(1)—

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

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

17 (C) in subparagraph (C), by striking
18 “high-performance computing” and inserting
19 “networking and information technology”; and
20 (2) in subsection (b)—

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

25 (B) by striking “sensitive”.

1 (h) SECTION 205.—Section 205(a) of the High-Per-
2 formance Computing Act of 1991 (15 U.S.C. 5525(a)) is
3 amended by striking “computational” and inserting “net-
4 working and information technology”.

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

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

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

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

20 (2) in subsection (a)—

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

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

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

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

9 (E) in paragraph (5), by striking “high-
10 performance computing and associated” and in-
11 serting “networking and information”.

12 **SEC. 408. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
13 **PROGRAM.**

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

1 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

2 The program shall—

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

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

13 (3) increase the capacity of institutions of high-
14 er education throughout all regions of the United
15 States to produce highly qualified cybersecurity pro-
16 fessionals, through the award of competitive, merit-
17 reviewed grants that support such activities as—

18 (A) faculty professional development, in-
19 cluding technical, hands-on experiences in the
20 private sector or government, workshops, semi-
21 nars, conferences, and other professional devel-
22 opment opportunities that will result in im-
23 proved instructional capabilities;

1 (B) institutional partnerships, including
2 minority serving institutions and community
3 colleges; and

4 (C) development of cybersecurity-related
5 courses and curricula;

6 (4) provide a procedure for the hiring Federal
7 agency, consistent with regulations of the Office of
8 Personnel Management, to request and fund a secu-
9 rity clearance for a scholarship recipient, including
10 providing for clearance during a summer internship
11 and upon graduation; and

12 (5) provide opportunities for students to receive
13 temporary appointments for meaningful employment
14 in the Federal information technology workforce
15 during school vacation periods and for internships.

16 (c) HIRING AUTHORITY.—

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

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

24 (B) be exempt from competitive service.

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

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

8 (1) is a citizen or permanent resident of the
9 United States;

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

14 (3) accepts the terms of a scholarship under
15 this section;

16 (4) maintains a GPA of 3.0 or above on a 4.0
17 scale; and

18 (5) has demonstrated a level of proficiency in
19 math or computer sciences.

20 (e) SERVICE OBLIGATION.—

21 (1) IN GENERAL.—If an individual receives a
22 scholarship under this section, as a condition of re-
23 ceiving such scholarship, the individual upon comple-
24 tion of the degree must serve as a cybersecurity pro-

1 fessional within the Federal workforce for a period
2 of time as provided in subsection (g).

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

8 (A) serving as a cybersecurity professional
9 in a State, local, or tribal government agency;
10 or

11 (B) teaching cybersecurity courses at an
12 institution of higher education.

13 (f) CONDITIONS OF SUPPORT.—As a condition of ac-
14 ceptance of a scholarship under this section, a scholarship
15 recipient shall agree to provide the awardee institution
16 with annual verifiable documentation of employment and
17 up-to-date contact information.

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

22 (h) FAILURE TO COMPLETE SERVICE OBLIGATION.—

23 (1) GENERAL RULE.—A scholarship recipient
24 under this section shall be liable to the United

1 States under paragraph (3) if the scholarship recipi-
2 ent—

3 (A) fails to maintain an acceptable level of
4 academic standing in the educational institution
5 in which the individual is enrolled, as deter-
6 mined by the Director;

7 (B) is dismissed from such educational in-
8 stitution for disciplinary reasons;

9 (C) withdraws from the program for which
10 the award was made before the completion of
11 such program;

12 (D) declares that the individual does not
13 intend to fulfill the service obligation under this
14 section; or

15 (E) fails to fulfill the service obligation of
16 the individual under this section.

17 (2) MONITORING COMPLIANCE.—As a condition
18 of participating in the program, a qualified institu-
19 tion of higher education receiving a grant under this
20 section shall—

21 (A) enter into an agreement with the Di-
22 rector of the National Science Foundation to
23 monitor the compliance of scholarship recipients
24 with respect to their service obligations; and

1 (B) provide to the Director, on an annual
2 basis, post-award employment information for
3 scholarship recipients through the completion of
4 their service obligations.

5 (3) REPAYMENT AMOUNTS.—

6 (A) LESS THAN 1 YEAR OF SERVICE.—If a
7 circumstance under paragraph (1) occurs before
8 the completion of 1 year of a service obligation
9 under this section, the total amount of awards
10 received by the individual under this section
11 shall be repaid or such amount shall be treated
12 as a loan to be repaid in accordance with sub-
13 paragraph (C).

14 (B) ONE OR MORE YEARS OF SERVICE.—
15 If a circumstance described in subparagraph
16 (D) or (E) of paragraph (1) occurs after the
17 completion of 1 year of a service obligation
18 under this section, the total amount of scholar-
19 ship awards received by the individual under
20 this section, reduced by the ratio of the number
21 of years of service completed divided by the
22 number of years of service required, shall be re-
23 paid or such amount shall be treated as a loan
24 to be repaid in accordance with subparagraph
25 (C).

1 (C) REPAYMENTS.—A loan described
2 under subparagraph (A) or (B) shall be treated
3 as a Federal Direct Unsubsidized Stafford
4 Loan under part D of title IV of the Higher
5 Education Act of 1965 (20 U.S.C. 1087a et
6 seq.), and shall be subject to repayment, to-
7 gether with interest thereon accruing from the
8 date of the scholarship award, in accordance
9 with terms and conditions specified by the Di-
10 rector (in consultation with the Secretary of
11 Education) in regulations promulgated to carry
12 out this paragraph.

13 (4) COLLECTION OF REPAYMENT.—

14 (A) IN GENERAL.—In the event that a
15 scholarship recipient is required to repay the
16 scholarship under this subsection, the institu-
17 tion providing the scholarship shall—

18 (i) be responsible for determining the
19 repayment amounts and for notifying the
20 scholarship recipient and the Director of
21 the amount owed; and

22 (ii) collect such repayment amount
23 within a period of time as determined
24 under the agreement under paragraph (2)
25 or the repayment amount shall be treated

1 as a loan in accordance with paragraph
2 (3)(C).

3 (B) RETURNED TO TREASURY.—Except as
4 provided in subparagraph (C), any such repay-
5 ment shall be returned to the Treasury of the
6 United States.

7 (C) RETAIN PERCENTAGE.—An institution
8 of higher education may retain a percentage of
9 any repayment the institution collects under
10 this paragraph to defray administrative costs
11 associated with the collection. The Director
12 shall establish a single, fixed percentage that
13 will apply to all eligible entities.

14 (5) EXCEPTIONS.—The Director may provide
15 for the partial or total waiver or suspension of any
16 service or payment obligation by an individual under
17 this section if—

18 (A) compliance by the individual with the
19 obligation is impossible;

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

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

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

1 mental agencies, regulatory entities, and nongovernmental
2 organizations in the course of the study.

3 (b) SCOPE.—The study shall include—

4 (1) an evaluation of the body of knowledge and
5 various skills that specific categories of personnel
6 working in information infrastructure should possess
7 in order to secure information systems;

8 (2) an assessment of whether existing govern-
9 ment, academic, and private-sector accreditation,
10 training, and certification programs provide the body
11 of knowledge and various skills described in para-
12 graph (1);

13 (3) an analysis of any barriers to the Federal
14 Government recruiting and hiring cybersecurity tal-
15 ent, including barriers relating to compensation, the
16 hiring process, job classification, and hiring flexi-
17 bility; and

18 (4) an analysis of the sources and availability of
19 cybersecurity talent, a comparison of the skills and
20 expertise sought by the Federal Government and the
21 private sector, and an examination of the current
22 and future capacity of United States institutions of
23 higher education, including community colleges, to
24 provide current and future cybersecurity profes-
25 sionals, through education and training activities,

1 with those skills sought by the Federal Government,
2 State and local entities, and the private sector.

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

7 (1) findings regarding the state of information
8 infrastructure accreditation, training, and certifi-
9 cation programs, including specific areas of defi-
10 ciency and demonstrable progress; and

11 (2) recommendations for the improvement of in-
12 formation infrastructure accreditation, training, and
13 certification programs.

14 **SEC. 410. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
15 **VELOPMENT PLAN.**

16 (a) IN GENERAL.—Not later than 12 months after
17 the date of enactment of this Act, the agencies designated
18 under subsection 101(a)(3)(B)(i) through (xi) of the
19 High-Performance Computing Act of 1991 (15 U.S.C.
20 5511(a)(3)(B)(i) through (xi)) (working through the Na-
21 tional Science and Technology Council) shall transmit to
22 Congress a strategic plan based on an assessment of
23 cybersecurity risk to guide the overall direction of Federal
24 cybersecurity and information assurance research and de-
25 velopment for information technology and networking sys-

1 tems. Once every 3 years after the initial strategic plan
2 is transmitted to Congress under this section, the agencies
3 shall prepare and transmit to Congress an update of the
4 strategic plan.

5 (b) CONTENTS OF PLAN.—The strategic plan under
6 subsection (a) shall—

7 (1) specify and prioritize—

8 (A) near-term, mid-term, and long-term re-
9 search objectives, including objectives associated
10 with the research areas identified in section
11 4(a)(1) of the Cyber Security Research and De-
12 velopment Act (15 U.S.C. 7403(a)(1)); and

13 (B) how the near-term objectives com-
14 plement research and development areas in
15 which the private sector is actively engaged;

16 (2) describe how the National Networking and
17 Information Technology Research and Development
18 Program will focus on innovative, transformational
19 technologies with the potential to enhance the secu-
20 rity, reliability, resilience, and trustworthiness of the
21 digital infrastructure, and to protect consumer pri-
22 vacy;

23 (3) describe how the Program will foster the
24 rapid transfer of research and development results
25 into new cybersecurity technologies and applications

1 for the timely benefit of society and the national in-
2 terest, including through the dissemination of best
3 practices and other outreach activities;

4 (4) describe how the Program will establish and
5 maintain a national research infrastructure for cre-
6 ating, testing, and evaluating the next generation of
7 secure networking and information technology sys-
8 tems;

9 (5) describe how the Program will facilitate ac-
10 cess by academic researchers to the infrastructure
11 described in paragraph (4), as well as to relevant
12 data, including event data; and

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

18 (c) DEVELOPMENT OF IMPLEMENTATION ROAD-
19 MAP.—The agencies described in subsection (a) shall de-
20 velop and annually update an implementation roadmap for
21 the strategic plan under this section. The implementation
22 roadmap shall—

23 (1) specify the role of each Federal agency in
24 carrying out or sponsoring research and development
25 to meet the research objectives of the strategic plan,

1 including a description of how progress toward the
2 research objectives will be evaluated;

3 (2) specify the funding allocated to each major
4 research objective of the strategic plan and the
5 source of funding by agency for the current fiscal
6 year; and

7 (3) estimate the funding required for each
8 major research objective of the strategic plan for the
9 following 3 fiscal years.

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

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

16 (2) a wide range of stakeholders, including in-
17 dustry, academia (including representatives of mi-
18 nority serving institutions and community colleges),
19 National Laboratories, and other relevant organiza-
20 tions and institutions.

21 (e) REPORT APPENDIX.—The implementation road-
22 map under subsection (c), and its annual updates, shall
23 be appended to the report under section 101(a)(2)(D) of
24 the High-Performance Computing Act of 1991 (15 U.S.C.
25 5511(a)(2)(D)).

1 (f) AUTHORIZATION OF APPROPRIATIONS.—From
2 amounts made available under section 503 of the America
3 COMPETES Reauthorization Act of 2010 (124 Stat.
4 4005), the Secretary may use funds to carry out the re-
5 quirements of this section for fiscal years 2012 through
6 2013.

7 **SEC. 411. INTERNATIONAL CYBERSECURITY TECHNICAL**
8 **STANDARDS.**

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

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

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

20 (b) CONSULTATION WITH THE PRIVATE SECTOR.—
21 In carrying out the activities under subsection (a)(1), the
22 Director shall ensure consultation with appropriate private
23 sector stakeholders.

1 **SEC. 412. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
2 **OPMENT.**

3 The Director of the National Institute of Standards
4 and Technology shall continue a program to support the
5 development of technical standards, metrology, testbeds,
6 and conformance criteria, taking into account appropriate
7 user concerns—

8 (1) to improve interoperability among identity
9 management technologies;

10 (2) to strengthen authentication methods of
11 identity management systems;

12 (3) to improve privacy protection in identity
13 management systems, including health information
14 technology systems, through authentication and se-
15 curity protocols; and

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

18 **SEC. 413. FEDERAL CYBERSECURITY RESEARCH AND DE-**
19 **VELOPMENT PROGRAMS.**

20 (a) COMPUTER AND NETWORK SECURITY RESEARCH
21 AREAS.—Section 4(a)(1) of the Cyber Security Research
22 and Development Act (15 U.S.C. 7403(a)(1)) is amend-
23 ed—

24 (1) in subparagraph (A) by inserting “identity
25 management,” after “cryptography,”; and

1 (3) in subparagraph (I), by inserting “, crimes
2 against children, and organized crime” after “intel-
3 lectual property”.

4 (b) COMPUTER AND NETWORK SECURITY RESEARCH
5 GRANTS.—Section 4(a)(3) of such Act (15 U.S.C.
6 7403(a)(3)) is amended by striking subparagraphs (A)
7 through (E) and inserting the following new subpara-
8 graphs:

9 “(A) \$90,000,000 for fiscal year 2012;

10 “(B) \$90,000,000 for fiscal year 2013; and

11 “(C) \$90,000,000 for fiscal year 2014.”.

12 (c) COMPUTER AND NETWORK SECURITY RESEARCH
13 CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b))
14 is amended—

15 (1) in paragraph (4)—

16 (A) in subparagraph (C), by striking
17 “and” after the semicolon;

18 (B) in subparagraph (D), by striking the
19 period and inserting “; and”; and

20 (C) by adding at the end the following new
21 subparagraph:

22 “(E) how the center will partner with gov-
23 ernment laboratories, for-profit entities, other
24 institutions of higher education, or nonprofit re-
25 search institutions.”; and

1 (2) in paragraph (7) by striking subparagraphs
2 (A) through (E) and inserting the following new
3 subparagraphs:

4 “(A) \$4,500,000 for fiscal year 2012;

5 “(B) \$4,500,000 for fiscal year 2013; and

6 “(C) \$4,500,000 for fiscal year 2014.”.

7 (d) COMPUTER AND NETWORK SECURITY CAPACITY
8 BUILDING GRANTS.—Section 5(a)(6) of such Act (15
9 U.S.C. 7404(a)(6)) is amended by striking subparagraphs
10 (A) through (E) and inserting the following new subpara-
11 graphs:

12 “(A) \$19,000,000 for fiscal year 2012;

13 “(B) \$19,000,000 for fiscal year 2013; and

14 “(C) \$19,000,000 for fiscal year 2014.”.

15 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
16 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
17 7404(b)(2)) is amended by striking subparagraphs (A)
18 through (E) and inserting the following new subpara-
19 graphs:

20 “(A) \$2,500,000 for fiscal year 2012;

21 “(B) \$2,500,000 for fiscal year 2013; and

22 “(C) \$2,500,000 for fiscal year 2014.”.

23 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
24 NETWORK SECURITY.—Section 5(c)(7) of such Act (15
25 U.S.C. 7404(c)(7)) is amended by striking subparagraphs

1 (A) through (E) and inserting the following new subpara-
2 graphs:

3 “(A) \$24,000,000 for fiscal year 2012;

4 “(B) \$24,000,000 for fiscal year 2013; and

5 “(C) \$24,000,000 for fiscal year 2014.”.

6 (g) CYBER SECURITY FACULTY DEVELOPMENT
7 TRAINEESHIP PROGRAM.—Section 5(e) of such Act (15
8 U.S.C. 7404(e)) is repealed.

9 **SEC. 414. CYBERSECURITY AUTOMATION AND CHECKLISTS**
10 **FOR GOVERNMENT SYSTEMS.**

11 Section 8(c) of the Cyber Security Research and De-
12 velopment Act (15 U.S.C. 7406(c)) is amended to read
13 as follows:

14 “(c) SECURITY AUTOMATION AND CHECKLISTS FOR
15 GOVERNMENT SYSTEMS.—

16 “(1) IN GENERAL.—The Director of the Na-
17 tional Institute of Standards and Technology shall
18 develop, and revise as necessary, security automation
19 standards, associated reference materials (including
20 protocols), and checklists providing settings and op-
21 tion selections that minimize the security risks asso-
22 ciated with each information technology hardware or
23 software system and security tool that is, or is likely
24 to become, widely used within the Federal Govern-
25 ment in order to enable standardized and interoper-

1 able technologies, architectures, and frameworks for
2 continuous monitoring of information security within
3 the Federal Government.

4 “(2) PRIORITIES FOR DEVELOPMENT.—The Di-
5 rector of the National Institute of Standards and
6 Technology shall establish priorities for the develop-
7 ment of standards, reference materials, and check-
8 lists under this subsection on the basis of—

9 “(A) the security risks associated with the
10 use of the system;

11 “(B) the number of agencies that use a
12 particular system or security tool;

13 “(C) the usefulness of the standards, ref-
14 erence materials, or checklists to Federal agen-
15 cies that are users or potential users of the sys-
16 tem;

17 “(D) the effectiveness of the associated
18 standard, reference material, or checklist in cre-
19 ating or enabling continuous monitoring of in-
20 formation security; or

21 “(E) such other factors as the Director of
22 the National Institute of Standards and Tech-
23 nology determines to be appropriate.

24 “(3) EXCLUDED SYSTEMS.—The Director of
25 the National Institute of Standards and Technology

1 may exclude from the application of paragraph (1)
2 any information technology hardware or software
3 system or security tool for which such Director de-
4 termines that the development of a standard, ref-
5 erence material, or checklist is inappropriate because
6 of the infrequency of use of the system, the obsoles-
7 cence of the system, or the inutility or imprac-
8 ticability of developing a standard, reference mate-
9 rial, or checklist for the system.

10 “(4) DISSEMINATION OF STANDARDS AND RE-
11 LATED MATERIALS.—The Director of the National
12 Institute of Standards and Technology shall ensure
13 that Federal agencies are informed of the avail-
14 ability of any standard, reference material, checklist,
15 or other item developed under this subsection.

16 “(5) AGENCY USE REQUIREMENTS.—The devel-
17 opment of standards, reference materials, and check-
18 lists under paragraph (1) for an information tech-
19 nology hardware or software system or tool does
20 not—

21 “(A) require any Federal agency to select
22 the specific settings or options recommended by
23 the standard, reference material, or checklist
24 for the system;

1 “(B) establish conditions or prerequisites
2 for Federal agency procurement or deployment
3 of any such system;

4 “(C) imply an endorsement of any such
5 system by the Director of the National Institute
6 of Standards and Technology; or

7 “(D) preclude any Federal agency from
8 procuring or deploying other information tech-
9 nology hardware or software systems for which
10 no such standard, reference material, or check-
11 list has been developed or identified under para-
12 graph (1).”.

13 **SEC. 415. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
14 **NOLOGY CYBERSECURITY RESEARCH AND**
15 **DEVELOPMENT.**

16 Section 20 of the National Institute of Standards and
17 Technology Act (15 U.S.C. 278g-3) is amended—

18 (1) by redesignating subsection (e) as sub-
19 section (f); and

20 (2) by inserting after subsection (d) the fol-
21 lowing:

22 “(e) INTRAMURAL SECURITY RESEARCH.—As part of
23 the research activities conducted in accordance with sub-
24 section (d)(3), the Institute shall—

1 “(1) conduct a research program to develop a
2 unifying and standardized identity, privilege, and ac-
3 cess control management framework for the execu-
4 tion of a wide variety of resource protection policies
5 and that is amenable to implementation within a
6 wide variety of existing and emerging computing en-
7 vironments;

8 “(2) carry out research associated with improv-
9 ing the security of information systems and net-
10 works;

11 “(3) carry out research associated with improv-
12 ing the testing, measurement, usability, and assur-
13 ance of information systems and networks; and

14 “(4) carry out research associated with improv-
15 ing security of industrial control systems.”.