

113TH CONGRESS
1ST SESSION

H. R. 1468

To improve information security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 10, 2013

Mrs. BLACKBURN introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Oversight and Government Reform, the Judiciary, Armed Services, Select Intelligence (Permanent Select), and Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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 2013” or “SECURE IT”.

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

Sec. 1. Short title; table of contents.

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

- Sec. 101. Definitions.
- Sec. 102. Authorization to share cyber threat information.
- Sec. 103. Information sharing by the Federal Government.
- Sec. 104. Construction.
- Sec. 105. Report on implementation.
- Sec. 106. Inspector General review.
- Sec. 107. Technical amendments.
- Sec. 108. 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.
- Sec. 205. Clarification of authorities.

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.
- Sec. 307. No new funding.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

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

TITLE V—DATA SECURITY AND BREACH NOTIFICATION

- Sec. 501. Requirements for information security.
- Sec. 502. Notification of information security breach.
- Sec. 503. Application and enforcement.
- Sec. 504. Definitions.

Sec. 505. Effect on other laws.

Sec. 506. Effective date.

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.

1 (4) CYBER THREAT INFORMATION.—The term
2 “cyber threat information” means information that
3 indicates or describes—

4 (A) a technical or operation vulnerability
5 or a cyber threat mitigation measure;

6 (B) an action or operation to mitigate a
7 cyber threat;

8 (C) malicious reconnaissance, including
9 anomalous patterns of network activity that ap-
10 pear to be transmitted for the purpose of gath-
11 ering technical information related to a cyberse-
12 curity threat;

13 (D) a method of defeating a technical con-
14 trol;

15 (E) a method of defeating an operational
16 control;

17 (F) network activity or protocols known to
18 be associated with a malicious cyber actor or
19 that signify malicious cyber intent;

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

1 (H) any other attribute of a cybersecurity
2 threat or cyber defense information that would
3 foster situational awareness of the United
4 States cybersecurity posture, if disclosure of
5 such attribute or information is not otherwise
6 prohibited by law;

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

11 (J) any combination of subparagraphs (A)
12 through (I).

13 (5) CYBERSECURITY CENTER.—The term “cy-
14 bersecurity center” means the Department of De-
15 fense Cyber Crime Center, the Intelligence Commu-
16 nity Incident Response Center, the United States
17 Cyber Command Joint Operations Center, the Na-
18 tional Cyber Investigative Joint Task Force, the Na-
19 tional Security Agency/Central Security Service
20 Threat Operations Center, the National Cybersecu-
21 rity and Communications Integration Center, and
22 any successor center.

23 (6) CYBERSECURITY SYSTEM.—The term “cy-
24 bersecurity system” means a system designed or em-
25 ployed to ensure the integrity, confidentiality, or

1 availability of, or to safeguard, a system or network,
2 including measures intended to protect a system or
3 network from—

4 (A) efforts to degrade, disrupt, or destroy
5 such system or network; or

6 (B) theft or misappropriations of private
7 or government information, intellectual prop-
8 erty, or personally identifiable information.

9 (7) ENTITY.—

10 (A) IN GENERAL.—The term “entity”
11 means any private entity, non-Federal Govern-
12 ment agency or department, or State, tribal, or
13 local government agency or department (includ-
14 ing an officer, employee, or agent thereof).

15 (B) INCLUSIONS.—The term “entity” in-
16 cludes a government agency or department (in-
17 cluding an officer, employee, or agent thereof)
18 of the District of Columbia, the Commonwealth
19 of Puerto Rico, the Virgin Islands, Guam,
20 American Samoa, the Northern Mariana Is-
21 lands, and any other territory or possession of
22 the United States.

23 (8) FEDERAL INFORMATION SYSTEM.—The
24 term “Federal information system” means an infor-
25 mation system of a Federal department or agency

1 used or operated by an executive agency, by a con-
2 tractor of an executive agency, or by another organi-
3 zation on behalf of an executive agency.

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

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

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

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

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

22 (11) LOCAL GOVERNMENT.—The term “local
23 government” means any borough, city, county, par-
24 ish, town, township, village, or other general purpose
25 political subdivision of a State.

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

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

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

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

20 (16) SIGNIFICANT CYBER INCIDENT.—The term
21 “significant cyber incident” means a cyber incident
22 resulting in, or an attempted cyber incident that, if
23 successful, would have resulted in—

1 (A) the exfiltration from a Federal infor-
2 mation system of data that is essential to the
3 operation of the Federal information system; or

4 (B) an incident in which an operational or
5 technical control essential to the security or op-
6 eration of a Federal information system was de-
7 feated.

8 (17) TECHNICAL CONTROL.—The term “tech-
9 nical control” means a hardware or software restric-
10 tion on, or audit of, access or use of an information
11 system or information that is stored on, processed
12 by, or transiting an information system that is in-
13 tended to ensure the confidentiality, integrity, or
14 availability of that system.

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

19 (19) TRIBAL.—The term “tribal” has the
20 meaning given the term “Indian tribe” in section 4
21 of the Indian Self-Determination and Education As-
22 sistance Act (25 U.S.C. 450b).

23 **SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT IN-**
24 **FORMATION.**

25 (a) VOLUNTARY DISCLOSURE.—

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

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

12 (A) a cybersecurity center; or

13 (B) any other entity in order to assist with
14 preventing, investigating, or otherwise miti-
15 gating threats to information security.

16 (3) INFORMATION SECURITY PROVIDERS.—If
17 the cyber threat information described in paragraph
18 (1) is obtained, identified, or otherwise possessed in
19 the course of providing information security prod-
20 ucts or services under contract to another entity,
21 that entity shall be given, at any time prior to dis-
22 closure of such information, a reasonable oppor-
23 tunity to authorize or prevent such disclosure, to re-
24 quest anonymization of such information, or to re-
25 quest that reasonable efforts be made to safeguard

1 such information that identifies specific persons
2 from unauthorized access or disclosure.

3 (b) SIGNIFICANT CYBER INCIDENTS INVOLVING
4 FEDERAL INFORMATION SYSTEMS.—

5 (1) IN GENERAL.—An entity providing elec-
6 tronic communication services, remote computing
7 services, or information security services to a Fed-
8 eral department or agency shall inform the Federal
9 department or agency of a significant cyber incident
10 involving the Federal information system of that
11 Federal department or agency that—

12 (A) is directly known to the entity as a re-
13 sult of providing such services;

14 (B) is directly related to the provision of
15 such services by the entity; and

16 (C) as determined by the entity, has im-
17 peded or will impede the performance of a crit-
18 ical mission of the Federal department or agen-
19 cy.

20 (2) ADVANCE COORDINATION.—A Federal de-
21 partment or agency receiving the services described
22 in paragraph (1) shall coordinate in advance with an
23 entity described in paragraph (1) to develop the pa-
24 rameters of any information that may be provided
25 under paragraph (1), including clarification of the

1 type of significant cyber incident that will impede
2 the performance of a critical mission of the Federal
3 department or agency.

4 (3) REPORT.—A Federal department or agency
5 shall report information provided under this sub-
6 section to a cybersecurity center.

7 (4) CONSTRUCTION.—Any information provided
8 to a cybersecurity center under paragraph (3) shall
9 be treated in the same manner as information pro-
10 vided to a cybersecurity center under subsection (a).

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

14 (1) may be disclosed to, retained by, and used
15 by, consistent with otherwise applicable Federal law,
16 any Federal agency or department, component, offi-
17 cer, employee, or agent of the Federal Government
18 for a cybersecurity purpose, a national security pur-
19 pose, or in order to prevent, investigate, or prosecute
20 any of the offenses listed in section 2516 of title 18,
21 United States Code, and such information shall not
22 be disclosed to, retained by, or used by any Federal
23 agency or department for any use not permitted
24 under this paragraph;

1 (2) may, with the prior written consent of the
2 entity submitting such information, be disclosed to
3 and used by a State, tribal, or local government or
4 government agency for the purpose of protecting in-
5 formation systems, or in furtherance of preventing,
6 investigating, or prosecuting a criminal act, except
7 that if the need for immediate disclosure prevents
8 obtaining written consent, such consent may be pro-
9 vided orally with subsequent documentation of such
10 consent;

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

22 (4) shall be deemed voluntarily shared informa-
23 tion and exempt from disclosure under section 552
24 of title 5, United States Code, and any State, tribal,

1 or local law requiring disclosure of information or
2 records;

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

7 (6) shall not be subject to the rules of any Fed-
8 eral agency or department or any judicial doctrine
9 regarding ex parte communications with a decision-
10 making official;

11 (7) shall not, if subsequently provided to a
12 State, tribal, or local government or government
13 agency, otherwise be disclosed or distributed to any
14 entity by such State, tribal, or local government or
15 government agency without the prior written consent
16 of the entity submitting such information, notwith-
17 standing any State, tribal, or local law requiring dis-
18 closure of information or records, except that if the
19 need for immediate disclosure prevents obtaining
20 written consent, such consent may be provided orally
21 with subsequent documentation of such consent; and

22 (8) shall not be directly used by any Federal,
23 State, tribal, or local department or agency to regu-
24 late the lawful activities of an entity, including ac-
25 tivities relating to obtaining, identifying, or other-

1 wise possessing cyber threat information, except that
2 the procedures required to be developed and imple-
3 mented under this title shall not be considered regu-
4 lations within the meaning of this paragraph.

5 (d) PROCEDURES RELATING TO INFORMATION SHAR-
6 ING WITH A CYBERSECURITY CENTER.—Not later than
7 60 days after the date of enactment of this Act, the heads
8 of each department or agency containing a cybersecurity
9 center shall jointly develop, promulgate, and submit to
10 Congress procedures to ensure that cyber threat informa-
11 tion shared with or provided to—

12 (1) a cybersecurity center under this section—

13 (A) may be submitted to a cybersecurity
14 center by an entity, to the greatest extent pos-
15 sible, through a uniform, publicly available
16 process or format that is easily accessible on
17 the website of such cybersecurity center, and
18 that includes the ability to provide relevant de-
19 tails about the cyber threat information and
20 written consent to any subsequent disclosures
21 authorized by this paragraph;

22 (B) shall immediately be further shared
23 with each cybersecurity center in order to pre-
24 vent, investigate, or otherwise mitigate threats

1 to information security across the Federal Gov-
2 ernment;

3 (C) is handled by the Federal Government
4 in a reasonable manner, including consideration
5 of the need to protect the privacy and civil lib-
6 erties of individuals through anonymization or
7 other appropriate methods, while fully accom-
8 plishing the objectives of this title, and the Fed-
9 eral Government may undertake efforts con-
10 sistent with this subparagraph to limit the im-
11 pact on privacy and civil liberties of the sharing
12 of cyber threat information with the Federal
13 Government; and

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

17 (2) a Federal agency or department under sub-
18 section (b) is provided immediately to a cybersecu-
19 rity center in order to prevent, investigate, or other-
20 wise mitigate threats to information security across
21 the Federal Government.

22 (e) INFORMATION SHARED BETWEEN ENTITIES.—

23 (1) IN GENERAL.—An entity sharing cyber
24 threat information with another entity under this

1 title may restrict the use or sharing of such informa-
2 tion by such other entity.

3 (2) FURTHER SHARING.—Cyber threat informa-
4 tion shared by any entity with another entity under
5 this title—

6 (A) shall only be further shared in accord-
7 ance with any restrictions placed on the sharing
8 of such information by the entity authorizing
9 such sharing, such as appropriate
10 anonymization of such information; and

11 (B) may not be used by any entity to gain
12 an unfair competitive advantage to the det-
13 riment of the entity authorizing the sharing of
14 such information, except that the conduct de-
15 scribed in paragraph (3) shall not constitute
16 unfair competitive conduct.

17 (3) INFORMATION SHARED WITH STATE, TRIB-
18 AL, OR LOCAL GOVERNMENT OR GOVERNMENT
19 AGENCY.—Cyber threat information shared with a
20 State, tribal, or local government or government
21 agency under this title—

22 (A) may, with the prior written consent of
23 the entity sharing such information, be dis-
24 closed to and used by a State, tribal, or local
25 government or government agency for the pur-

1 pose of protecting information systems, or in
2 furtherance of preventing, investigating, or
3 prosecuting a criminal act, except if the need
4 for immediate disclosure prevents obtaining
5 written consent, consent may be provided orally
6 with subsequent documentation of the consent;

7 (B) shall be deemed voluntarily shared in-
8 formation and exempt from disclosure under
9 any State, tribal, or local law requiring disclo-
10 sure of information or records;

11 (C) shall not be disclosed or distributed to
12 any entity by the State, tribal, or local govern-
13 ment or government agency without the prior
14 written consent of the entity submitting such
15 information, notwithstanding any State, tribal,
16 or local law requiring disclosure of information
17 or records, except if the need for immediate dis-
18 closure prevents obtaining written consent, con-
19 sent may be provided orally with subsequent
20 documentation of the consent; and

21 (D) shall not be directly used by any State,
22 tribal, or local department or agency to regulate
23 the lawful activities of an entity, including ac-
24 tivities relating to obtaining, identifying, or oth-
25 erwise possessing cyber threat information, ex-

1 cept that the procedures required to be devel-
2 oped and implemented under this title shall not
3 be considered regulations within the meaning of
4 this subparagraph.

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

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

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

18 (5) NO RIGHT OR BENEFIT.—The provision of
19 cyber threat information to an entity under this sec-
20 tion shall not create a right or a benefit to similar
21 information by such entity or any other entity.

22 (f) FEDERAL PREEMPTION.—

23 (1) IN GENERAL.—This section supersedes any
24 statute or other law of a State or political subdivi-

1 sion of a State that restricts or otherwise expressly
2 regulates an activity authorized under this section.

3 (2) STATE LAW ENFORCEMENT.—Nothing in
4 this section shall be construed to supersede any stat-
5 ute or other law of a State or political subdivision
6 of a State concerning the use of authorized law en-
7 forcement techniques.

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

14 (g) CIVIL AND CRIMINAL LIABILITY.—

15 (1) GENERAL PROTECTIONS.—

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

19 (i) the use of countermeasures and cy-
20 bersecurity systems as authorized by this
21 title;

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

1 (iii) the subsequent actions or inac-
2 tions of any lawful recipient of cyber threat
3 information provided by such private enti-
4 ty.

5 (B) ENTITIES.—No cause of action shall
6 lie or be maintained in any court against any
7 entity for—

8 (i) the use, receipt, or disclosure of
9 any cyber threat information as authorized
10 by this title; or

11 (ii) the subsequent actions or inac-
12 tions of any lawful recipient of cyber threat
13 information provided by such entity.

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

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

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

5 (j) RELATIONSHIP TO OTHER LAWS.—The submis-
6 sion of cyber threat information under this section to a
7 cybersecurity center shall not affect any requirement
8 under any other provision of law for an entity to provide
9 information to the Federal Government.

10 **SEC. 103. INFORMATION SHARING BY THE FEDERAL GOV-**
11 **ERNMENT.**

12 (a) CLASSIFIED INFORMATION.—

13 (1) PROCEDURES.—Consistent with the protec-
14 tion of intelligence sources and methods, and as oth-
15 erwise determined appropriate, the Director of Na-
16 tional Intelligence and the Secretary of Defense, in
17 consultation with the heads of the appropriate Fed-
18 eral departments or agencies, shall develop and pro-
19 mulgate procedures to facilitate and promote—

20 (A) the immediate sharing, through the cy-
21 bersecurity centers, of classified cyber threat in-
22 formation in the possession of the Federal Gov-
23 ernment with appropriately cleared representa-
24 tives of any appropriate entity; and

1 (B) the declassification and immediate
2 sharing, through the cybersecurity centers, with
3 any entity or, if appropriate, public availability
4 of cyber threat information in the possession of
5 the Federal Government.

6 (2) HANDLING OF CLASSIFIED INFORMATION.—

7 The procedures developed under paragraph (1) shall
8 ensure that each entity receiving classified cyber
9 threat information pursuant to this section has ac-
10 knowledged in writing the ongoing obligation to com-
11 ply with all laws, Executive orders, and procedures
12 concerning the appropriate handling, disclosure, or
13 use of classified information.

14 (b) UNCLASSIFIED CYBER THREAT INFORMATION.—

15 The heads of each department or agency containing a cy-
16 bersecurity center shall jointly develop and promulgate
17 procedures that ensure that, consistent with the provisions
18 of this section, unclassified, including controlled unclassi-
19 fied, cyber threat information in the possession of the Fed-
20 eral Government—

21 (1) is shared, through the cybersecurity centers,
22 in an immediate and adequate manner with appro-
23 priate entities; and

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

25 (c) DEVELOPMENT OF PROCEDURES.—

1 (1) IN GENERAL.—The procedures developed
2 under this section shall incorporate, to the greatest
3 extent possible, existing processes utilized by sector
4 specific information sharing and analysis centers.

5 (2) COORDINATION WITH ENTITIES.—In devel-
6 oping the procedures required under this section, the
7 Director of National Intelligence and the heads of
8 each department or agency containing a cybersecu-
9 rity center shall coordinate with appropriate entities
10 to ensure that protocols are implemented that will
11 facilitate and promote the sharing of cyber threat in-
12 formation by the Federal Government.

13 (d) ADDITIONAL RESPONSIBILITIES OF CYBERSECU-
14 RITY CENTERS.—Consistent with section 102, a cyberse-
15 curity center shall—

16 (1) facilitate information sharing, interaction,
17 and collaboration among and between cybersecurity
18 centers and—

19 (A) other Federal entities;

20 (B) any entity; and

21 (C) international partners, in consultation
22 with the Secretary of State;

23 (2) disseminate timely and actionable cyberse-
24 curity threat, vulnerability, mitigation, and warning
25 information, including alerts, advisories, indicators,

1 signatures, and mitigation and response measures,
2 to improve the security and protection of informa-
3 tion systems; and

4 (3) coordinate with other Federal entities, as
5 appropriate, to integrate information from across
6 the Federal Government to provide situational
7 awareness of the cybersecurity posture of the United
8 States.

9 (e) SHARING WITHIN THE FEDERAL GOVERN-
10 MENT.—The heads of appropriate Federal departments
11 and agencies shall ensure that cyber threat information
12 in the possession of such Federal departments or agencies
13 that relates to the prevention, investigation, or mitigation
14 of threats to information security across the Federal Gov-
15 ernment is shared effectively with the cybersecurity cen-
16 ters.

17 (f) SUBMISSION TO CONGRESS.—Not later than 60
18 days after the date of enactment of this Act, the Director
19 of National Intelligence, in coordination with the appro-
20 priate head of a department or an agency containing a
21 cybersecurity center, shall submit the procedures required
22 by this section to Congress.

23 **SEC. 104. CONSTRUCTION.**

24 (a) INFORMATION SHARING RELATIONSHIPS.—Noth-
25 ing in this title shall be construed—

1 (1) to limit or modify an existing information
2 sharing relationship;

3 (2) to prohibit a new information sharing rela-
4 tionship;

5 (3) to require a new information sharing rela-
6 tionship between any entity and the Federal Govern-
7 ment, except as specified under section 102(b); or

8 (4) to modify the authority of a department or
9 agency of the Federal Government to protect sources
10 and methods and the national security of the United
11 States.

12 (b) ANTI-TASKING RESTRICTION.—Nothing in this
13 title shall be construed to permit the Federal Govern-
14 ment—

15 (1) to require an entity to share information
16 with the Federal Government, except as expressly
17 provided under section 102(b); or

18 (2) to condition the sharing of cyber threat in-
19 formation with an entity on such entity’s provision
20 of cyber threat information to the Federal Govern-
21 ment.

22 (c) NO LIABILITY FOR NON-PARTICIPATION.—Noth-
23 ing in this title shall be construed to subject any entity
24 to liability for choosing not to engage in the voluntary ac-
25 tivities authorized under this title.

1 (d) USE AND RETENTION OF INFORMATION.—Noth-
2 ing in this title shall be construed to authorize, or to mod-
3 ify any existing authority of, a department or agency of
4 the Federal Government to retain or use any information
5 shared under section 102 for any use other than a use
6 permitted under subsection 102(c)(1).

7 (e) NO NEW FUNDING.—An applicable Federal agen-
8 cy shall carry out the provisions of this title with existing
9 facilities and funds otherwise available, through such
10 means as the head of the agency considers appropriate.

11 **SEC. 105. REPORT ON IMPLEMENTATION.**

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

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

1 (2) an assessment of whether information has
2 been appropriately classified and an accounting of
3 the number of security clearances authorized by the
4 Federal Government for purposes of this title;

5 (3) a review of the type of cyber threat infor-
6 mation shared with a cybersecurity center under sec-
7 tion 102 of this Act, including whether such infor-
8 mation meets the definition of cyber threat informa-
9 tion under section 101, the degree to which such in-
10 formation may impact the privacy and civil liberties
11 of individuals, any appropriate metrics to determine
12 any impact of the sharing of such information with
13 the Federal Government on privacy and civil lib-
14 erties, and the adequacy of any steps taken to re-
15 duce such impact;

16 (4) a review of actions taken by the Federal
17 Government based on information provided to a cy-
18 bersecurity center under section 102 of this Act, in-
19 cluding the appropriateness of any subsequent use
20 under section 102(c)(1) of this Act and whether
21 there was inappropriate stovepiping within the Fed-
22 eral Government of any such information;

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

1 (6) 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 (7) a summary of any breach of information se-
7 curity, if known, attributable to a specific failure by
8 any entity or the Federal Government to act on
9 cyber threat information in the possession of such
10 entity or the Federal Government that resulted in
11 substantial economic harm or injury to a specific en-
12 tity or the Federal Government; and

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

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

18 **SEC. 106. INSPECTOR GENERAL REVIEW.**

19 (a) IN GENERAL.—The Council of the Inspectors
20 General on Integrity and Efficiency are authorized to re-
21 view compliance by the cybersecurity centers, and by any
22 Federal department or agency receiving cyber threat infor-
23 mation from such cybersecurity centers, with the proce-
24 dures required under section 102 of this Act.

1 (b) SCOPE OF REVIEW.—The review under sub-
2 section (a) shall consider whether the Federal Government
3 has handled such cyber threat information in a reasonable
4 manner, including consideration of the need to protect the
5 privacy and civil liberties of individuals through
6 anonymization or other appropriate methods, while fully
7 accomplishing the objectives of this title.

8 (c) REPORT TO CONGRESS.—Each review conducted
9 under this section shall be provided to Congress not later
10 than 30 days after the date of completion of the review.

11 **SEC. 107. TECHNICAL AMENDMENTS.**

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

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

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

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

18 “(10) information shared with or provided to a
19 cybersecurity center under section 102 of title I of
20 the Strengthening and Enhancing Cybersecurity by
21 Using Research, Education, Information, and Tech-
22 nology Act of 2013.”.

23 **SEC. 108. ACCESS TO CLASSIFIED INFORMATION.**

24 (a) AUTHORIZATION REQUIRED.—No person shall be
25 provided with access to classified information (as defined

1 in section 6.1 of Executive Order 13526 (50 U.S.C. 435
2 note; relating to classified national security information))
3 relating to cyber security threats or cyber security
4 vulnerabilities under this title without the appropriate se-
5 curity clearances.

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

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

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

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

23 “SUBCHAPTER II—INFORMATION SECURITY

24 “§ 3551. Purposes

25 “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 ‘cy-
13 bersecurity 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 Cybersecu-
20 rity and Communications Integration Center, and
21 any successor center.

22 “(4) CYBER THREAT INFORMATION.—The term
23 ‘cyber threat information’ means information that
24 indicates 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 cyberse-
9 curity 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 signify malicious cyber 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 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 of subparagraphs
9 (A) through (I).

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

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

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

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

1 “(A) actually or imminently jeopardizes
2 the integrity, confidentiality, or availability of
3 an information system or the information that
4 system controls, processes, stores, or transmits;
5 or

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

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

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

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

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

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

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

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

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

16 “(14) NATIONAL SECURITY SYSTEM.—

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

23 “(i) the function, operation, or use of
24 which—

1 “(I) involves intelligence activi-
2 ties;

3 “(II) involves cryptologic activi-
4 ties related to national security;

5 “(III) involves command and
6 control of military forces;

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

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

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

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

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

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

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

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

16 “(19) SIGNIFICANT CYBER INCIDENT.—The
17 term ‘significant cyber incident’ means a cyber inci-
18 dent resulting in, or an attempted cyber incident
19 that, if successful, would have resulted in—

20 “(A) the exfiltration from a Federal infor-
21 mation system of data that is essential to the
22 operation of the Federal information system; or

23 “(B) an incident in which an operational
24 or technical control essential to the security or

1 operation of a Federal information system was
2 defeated.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 **“§ 3554. Agency responsibilities**

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

3 “(1) be responsible for—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 information security classifications and related re-
2 quirements;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 “(A) relevant security risk assessments, in-
5 cluding technical assessments and others re-
6 lated to the acquisition process;

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

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

11 “(D) risk-based continuous monitoring and
12 threat assessment of the operational status and
13 security of agency information systems to en-
14 able evaluation of the effectiveness of and com-
15 pliance with information security policies, proce-
16 dures, and practices, including a relevant and
17 appropriate selection of security controls of in-
18 formation systems identified in the inventory
19 under section 3505(c);

20 “(E) operation of appropriate technical ca-
21 pabilities in order to detect, mitigate, report,
22 and respond to information security incidents,
23 cyber threat information, and deterioration of
24 security controls in a manner that is consistent

1 with the policies and directives under section
2 3553, including—

3 “(i) mitigating risks associated with
4 such information security incidents;

5 “(ii) notifying and consulting with the
6 entity designated under section 3555; and

7 “(iii) notifying and consulting with, as
8 appropriate—

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

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

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

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

23 “(2) RISK MANAGEMENT STRATEGIES.—Each
24 agencywide information security program under sub-
25 section (b)(2) shall include the development and

1 maintenance of a risk management strategy for in-
2 formation security. The risk management strategy
3 shall include—

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

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

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

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

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

23 “(C) ensure that cost-effective and ade-
24 quate information security is addressed as part

1 of the acquisition and ongoing management of
2 each agency information system; and

3 “(D) ensure compliance with—

4 “(i) this subchapter; and

5 “(ii) any other applicable require-
6 ments.

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

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

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

23 “(d) ANNUAL REPORT.—Each agency shall submit a
24 report annually to the Secretary of Homeland Security on

1 its agencywide information security program and informa-
2 tion systems.

3 **“§ 3555. Multiagency ongoing threat assessment**

4 “(a) IMPLEMENTATION.—The Director of the Office
5 of Management and Budget, in coordination with the Sec-
6 retary of Homeland Security, shall designate an entity to
7 implement ongoing security analysis concerning agency in-
8 formation systems—

9 “(1) based on cyber threat information;

10 “(2) based on agency information system and
11 environment of operation changes, including—

12 “(A) an ongoing evaluation of the informa-
13 tion system security controls; and

14 “(B) the security state, risk level, and en-
15 vironment of operation of an agency informa-
16 tion system, including—

17 “(i) a change in risk level due to a
18 new cyber threat;

19 “(ii) a change resulting from a new
20 technology;

21 “(iii) a change resulting from the
22 agency’s mission; and

23 “(iv) a change resulting from the
24 business practice; and

1 “(3) using automated processes to the max-
2 imum extent possible—

3 “(A) to increase information system secu-
4 rity;

5 “(B) to reduce paper-based reporting re-
6 quirements; and

7 “(C) to maintain timely and actionable
8 knowledge of the state of the information sys-
9 tem security.

10 “(b) STANDARDS.—The National Institute of Stand-
11 ards and Technology may promulgate standards, in co-
12 ordination with the Secretary of Homeland Security, to
13 assist an agency with its duties under this section.

14 “(c) COMPLIANCE.—The head of each appropriate
15 department and agency shall be responsible for ensuring
16 compliance and implementing necessary procedures to
17 comply with this section. The head of each appropriate
18 department and agency, in consultation with the Director
19 of the Office of Management and Budget and the Sec-
20 retary of Homeland Security, shall—

21 “(1) monitor compliance under this section;

22 “(2) develop a timeline and implement for the
23 department or agency—

24 “(A) adoption of any technology, system,
25 or method that facilitates continuous moni-

1 toring and threat assessments of an agency in-
2 formation system;

3 “(B) adoption or updating of any tech-
4 nology, system, or method that prevents, de-
5 tects, or remediates a significant cyber incident
6 to a Federal information system of the depart-
7 ment or agency that has impeded, or is reason-
8 ably likely to impede, the performance of a crit-
9 ical mission of the department or agency; and

10 “(C) adoption of any technology, system,
11 or method that satisfies a requirement under
12 this section.

13 “(d) LIMITATION OF AUTHORITY.—The authorities
14 of the Director of the Office of Management and Budget
15 and of the Secretary of Homeland Security under this sec-
16 tion shall not apply to national security systems.

17 “(e) REPORT.—Not later than 6 months after the
18 date of enactment of the Strengthening and Enhancing
19 Cybersecurity by Using Research, Education, Information,
20 and Technology Act of 2013, the Government Account-
21 ability Office shall issue a report evaluating each agency’s
22 status toward implementing this section.

23 **“§ 3556. Independent evaluations**

24 “(a) IN GENERAL.—The Council of the Inspectors
25 General on Integrity and Efficiency, in consultation with

1 the Director and the Secretary of Homeland Security, the
2 Secretary of Commerce, and the Secretary of Defense,
3 shall issue and maintain criteria for the timely, cost-effec-
4 tive, risk-based, and independent evaluation of each agen-
5 cywide information security program (and practices) to de-
6 termine the effectiveness of the agencywide information
7 security program (and practices). The criteria shall in-
8 clude measures to assess any conflicts of interest in the
9 performance of the evaluation and whether the agencywide
10 information security program includes appropriate safe-
11 guards against disclosure of information where such dis-
12 closure may adversely affect information security.

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

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

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

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

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

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

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

14 (b) SAVINGS PROVISIONS.—

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

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

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

8 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

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

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

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

16 (C) by inserting the following:

“3551. Purposes.

“3552. Definitions.

“3553. Federal information security authority and coordination.

“3554. Agency responsibilities.

“3555. Multiagency ongoing threat assessment.

“3556. Independent evaluations.

“3557. National security systems.”.

17 (2) OTHER REFERENCES.—

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

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

4 (C) Section 2223(c)(3) of title 10, United
5 States Code, is amended, by striking “section
6 3542(b)(2)” and inserting “section 3552”.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21 “(a) STANDARDS AND GUIDELINES.—

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

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

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

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

14 “(b) MANDATORY STANDARDS AND GUIDELINES.—

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

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

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

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

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

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

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

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

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

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

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

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

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

1 “(g) DEFINITIONS.—In this section:

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

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

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

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

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

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

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

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

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

1 **SEC. 205. CLARIFICATION OF AUTHORITIES.**

2 Nothing in this title shall be construed to convey any
3 new regulatory authority to any government entity imple-
4 menting or complying with any provision of this title.

5 **TITLE III—CRIMINAL PENALTIES**

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

7 **IN CONNECTION WITH COMPUTERS.**

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

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

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

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

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

23 “(i) the offense was committed for
24 purposes of commercial advantage or pri-
25 vate financial gain;

1 “(ii) the offense was committed in the
2 furtherance of any criminal or tortious act
3 in violation of the Constitution or laws of
4 the United States, or of any State; or

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

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

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

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

19 “(i) loss to 1 or more persons during
20 any 1-year period (and, for purposes of an
21 investigation, prosecution, or other pro-
22 ceeding brought by the United States only,
23 loss resulting from a related course of con-
24 duct affecting 1 or more other protected

1 computers) aggregating at least \$5,000 in
2 value;

3 “(ii) the modification or impairment,
4 or potential modification or impairment, of
5 the medical examination, diagnosis, treat-
6 ment, or care of 1 or more individuals;

7 “(iii) physical injury to any person;

8 “(iv) a threat to public health or safe-
9 ty;

10 “(v) damage affecting a computer
11 used by, or on behalf of, an entity of the
12 United States Government in furtherance
13 of the administration of justice, national
14 defense, or national security; or

15 “(vi) damage affecting 10 or more
16 protected computers during any 1-year pe-
17 riod;

18 “(B) a fine under this title, imprisonment
19 for not more than 20 years, or both, in the case
20 of an offense under subsection (a)(5)(B), if the
21 offense caused a harm provided in clause (i)
22 through (vi) of subparagraph (A) of this sub-
23 section;

24 “(C) if the offender attempts to cause or
25 knowingly or recklessly causes death from con-

1 duct in violation of subsection (a)(5)(A), a fine
2 under this title, imprisonment for any term of
3 years or for life, or both;

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

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

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

15 **SEC. 302. TRAFFICKING IN PASSWORDS.**

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

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

1 **SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER**
2 **FRAUD OFFENSES.**

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

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

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

12 “(i) **CRIMINAL FORFEITURE.**—

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

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

23 “(B) any property, real or personal, consti-
24 tuting or derived from any gross proceeds, or
25 any property traceable to such property, that

1 such person obtained, directly or indirectly, as
2 a result of such violation.

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

10 “(j) CIVIL FORFEITURE.—

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

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

18 “(B) Any property, real or personal, con-
19 stituting or derived from any gross proceeds ob-
20 tained directly or indirectly, or any property
21 traceable to such property, as a result of the
22 commission of any violation of this section, or
23 a conspiracy to violate this section.

24 “(2) Seizures and forfeitures under this sub-
25 section shall be governed by the provisions in chap-

1 ter 46 relating to civil forfeitures, except that such
2 duties as are imposed on the Secretary of the Treas-
3 ury under the customs laws described in section
4 981(d) shall be performed by such officers, agents
5 and other persons as may be designated for that
6 purpose by the Secretary of Homeland Security or
7 the Attorney General.”.

8 **SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COM-**
9 **PUTERS.**

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

13 **“§ 1030A. Aggravated damage to a critical infrastruc-**
14 **ture computer**

15 “(a) DEFINITIONS.—In this section—

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

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

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

1 “(B) water supply systems;

2 “(C) telecommunication networks;

3 “(D) electrical power generation and deliv-
4 ery systems;

5 “(E) finance and banking systems;

6 “(F) emergency services;

7 “(G) transportation systems and services;

8 and

9 “(H) government operations that provide
10 essential services to the public; and

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

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

19 “(1) of the operation of the critical infrastruc-
20 ture computer; or

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

23 “(c) PENALTY.—Any person who violates subsection
24 (b) shall be—

25 “(1) fined under this title;

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

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

4 “(d) CONSECUTIVE SENTENCE.—Notwithstanding
5 any other provision of law—

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

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

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

22 “(4) a term of imprisonment imposed on a per-
23 son for a violation of this section may, in the discre-
24 tion of the court, run concurrently, in whole or in
25 part, only with another term of imprisonment that

1 is imposed by the court at the same time on that
2 person for an additional violation of this section,
3 provided that such discretion shall be exercised in
4 accordance with any applicable guidelines and policy
5 statements issued by the United States Sentencing
6 Commission pursuant to section 994 of title 28.”.

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

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

11 **SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHOR-**
12 **IZED USE.**

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

21 **SEC. 307. NO NEW FUNDING.**

22 An applicable Federal agency shall carry out the pro-
23 visions of this title with existing facilities and funds other-
24 wise available, through such means as the head of the
25 agency considers appropriate.

1 **TITLE IV—CYBERSECURITY**
2 **RESEARCH AND DEVELOPMENT**

3 **SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING**
4 **PROGRAM PLANNING AND COORDINATION.**

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

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

12 “(1) encouraging and supporting mechanisms
13 for interdisciplinary research and development in
14 networking and information technology, including—

15 “(A) through collaborations across agen-
16 cies;

17 “(B) through collaborations across Pro-
18 gram Component Areas;

19 “(C) through collaborations with industry;

20 “(D) through collaborations with institu-
21 tions of higher education;

22 “(E) through collaborations with Federal
23 laboratories (as defined in section 4 of the Ste-
24 venson-Wydler Technology Innovation Act of
25 1980 (15 U.S.C. 3703)); and

1 “(F) through collaborations with inter-
2 national organizations;

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

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

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

12 “(e) STRATEGIC PLAN.—

13 “(1) IN GENERAL.—Not later than 1 year after
14 the date of enactment of the Strengthening and En-
15 hancing Cybersecurity by Using Research, Edu-
16 cation, Information, and Technology Act of 2013,
17 the agencies under subsection (a)(3)(B), working
18 through the National Science and Technology Coun-
19 cil and with the assistance of the Office of Science
20 and Technology Policy shall develop a 5-year stra-
21 tegic plan to guide the activities under subsection
22 (a)(1).

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

1 “(A) the near-term objectives for the Pro-
2 gram;

3 “(B) the long-term objectives for the Pro-
4 gram;

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

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

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

13 “(3) IMPLEMENTATION ROADMAP.—

14 “(A) IN GENERAL.—The agencies under
15 subsection (a)(3)(B) shall develop and annually
16 update an implementation roadmap for the
17 strategic plan.

18 “(B) REQUIREMENTS.—The information in
19 the implementation roadmap shall be coordi-
20 nated with the database under section 102(c)
21 and the annual report under section 101(a)(3).

22 The implementation roadmap shall—

23 “(i) specify the role of each Federal
24 agency in carrying out or sponsoring re-
25 search and development to meet the re-

1 search objectives of the strategic plan, in-
2 cluding a description of how progress to-
3 ward the research objectives will be evalu-
4 ated, with consideration of any relevant
5 recommendations of the advisory com-
6 mittee;

7 “(ii) specify the funding allocated to
8 each major research objective of the stra-
9 tegic plan and the source of funding by
10 agency for the current fiscal year; and

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

14 “(4) RECOMMENDATIONS.—The agencies under
15 subsection (a)(3)(B) shall take into consideration
16 when developing the strategic plan under paragraph
17 (1) the recommendations of—

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

20 “(B) the stakeholders under section
21 102(a)(3).

22 “(5) REPORT TO CONGRESS.—The Director of
23 the Office of Science and Technology Policy shall
24 transmit the strategic plan under this subsection, in-

1 including the implementation roadmap and any up-
2 dates under paragraph (3), to—

3 “(A) the advisory committee under sub-
4 section (b);

5 “(B) the Committee on Commerce,
6 Science, and Transportation of the Senate; and

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

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

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

14 “(1) periodically assess the contents and fund-
15 ing levels of the Program Component Areas and re-
16 structure the Program when warranted, taking into
17 consideration any relevant recommendations of the
18 advisory committee under subsection (b); and

19 “(2) ensure that the Program includes national,
20 multi-agency, multi-faceted research and develop-
21 ment activities, including activities described in sec-
22 tion 104.”.

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

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

3 (2) by inserting after subparagraph (D) the fol-
4 lowing:

5 “(E) encourage and monitor the efforts of
6 the agencies participating in the Program to al-
7 locate the level of resources and management
8 attention necessary—

9 “(i) to ensure that the strategic plan
10 under subsection (e) is developed and exe-
11 cuted effectively; and

12 “(ii) to ensure that the objectives of
13 the Program are met;

14 “(F) working with the Office of Manage-
15 ment and Budget and in coordination with the
16 creation of the database under section 102(c),
17 direct the Office of Science and Technology Pol-
18 icy and the agencies participating in the Pro-
19 gram to establish a mechanism (consistent with
20 existing law) to track all ongoing and completed
21 research and development projects and associ-
22 ated funding;”.

23 (e) ADVISORY COMMITTEE.—Section 101(b) of the
24 High-Performance Computing Act of 1991 (15 U.S.C.
25 5511(b)) is amended—

1 (1) in paragraph (1)—

2 (A) by inserting after the first sentence the
3 following: “The co-chairs of the advisory com-
4 mittee shall meet the qualifications of com-
5 mittee members and may be members of the
6 Presidents Council of Advisors on Science and
7 Technology.”; and

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

10 (2) by amending paragraph (2) to read as fol-
11 lows:

12 “(2) In addition to the duties under paragraph
13 (1), the advisory committee shall conduct periodic
14 evaluations of the funding, management, coordina-
15 tion, implementation, and activities of the Program.
16 The advisory committee shall report its findings and
17 recommendations not less frequently than once every
18 3 fiscal years to the Committee on Commerce,
19 Science, and Transportation of the Senate and the
20 Committee on Science and Technology of the House
21 of Representatives. The report shall be submitted in
22 conjunction with the update of the strategic plan.”.

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

1 (1) in subparagraph (C)—

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

5 (B) by striking “each Program Component
6 Area” and inserting “each Program Component
7 Area and each research area supported in ac-
8 cordance with section 104”;

9 (2) in subparagraph (D)—

10 (A) by striking “each Program Component
11 Area,” and inserting “each Program Compo-
12 nent Area and each research area supported in
13 accordance with section 104,”;

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

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

18 (3) by redesignating subparagraph (E) as sub-
19 paragraph (G); and

20 (4) by inserting after subparagraph (D) the fol-
21 lowing:

22 “(E) include a description of how the ob-
23 jectives for each Program Component Area, and
24 the objectives for activities that involve multiple
25 Program Component Areas, relate to the objec-

1 tives of the Program identified in the strategic
2 plan under subsection (e);

3 “(F) include—

4 “(i) a description of the funding re-
5 quired by the Office of Science and Tech-
6 nology Policy to perform the functions
7 under subsections (a) and (c) of section
8 102 for the next fiscal year by category of
9 activity;

10 “(ii) a description of the funding re-
11 quired by the Office of Science and Tech-
12 nology Policy to perform the functions
13 under subsections (a) and (c) of section
14 102 for the current fiscal year by category
15 of activity; and

16 “(iii) the amount of funding provided
17 for the Office of Science and Technology
18 Policy for the current fiscal year by each
19 agency participating in the Program; and”.

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

23 (1) by redesignating paragraphs (1) and (2) as
24 paragraphs (2) and (3), respectively;

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

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

5 (4) by inserting before paragraph (2), as redesi-
6 gnated, the following:

7 “(1) ‘cyber-physical systems’ means physical or
8 engineered systems whose networking and informa-
9 tion technology functions and physical elements are
10 deeply integrated and are actively connected to the
11 physical world through sensors, actuators, or other
12 means to perform monitoring and control func-
13 tions;”;

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

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

18 (A) by striking “high-performance com-
19 puting” and inserting “networking and infor-
20 mation technology”; and

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

23 (7) in paragraph (5), by striking “network re-
24 ferred to as” and all that follows through the semi-
25 colon and inserting “network, including advanced

1 computer networks of Federal agencies and depart-
2 ments”; and

3 (8) in paragraph (7), as redesignated, by strik-
4 ing “National High-Performance Computing Pro-
5 gram” and inserting “networking and information
6 technology research and development program”.

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

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

12 **“SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPOR-
13 TANCE.**

14 “(a) IN GENERAL.—The Program shall encourage
15 agencies under section 101(a)(3)(B) to support, maintain,
16 and improve national, multi-agency, multi-faceted, re-
17 search and development activities in networking and infor-
18 mation technology directed toward application areas that
19 have the potential for significant contributions to national
20 economic competitiveness and for other significant societal
21 benefits.

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

1 “(1) cybersecurity;

2 “(2) health care;

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

5 “(4) transportation, including surface and air
6 transportation;

7 “(5) cyber-physical systems;

8 “(6) large-scale data analysis and modeling of
9 physical phenomena;

10 “(7) large scale data analysis and modeling of
11 behavioral phenomena;

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

13 “(9) privacy protection and protected disclosure
14 of confidential data.

15 “(c) RECOMMENDATIONS.—The advisory committee
16 under section 101(b) shall make recommendations to the
17 Program for candidate research and development areas for
18 support under this section.

19 “(d) CHARACTERISTICS.—

20 “(1) IN GENERAL.—Research and development
21 activities under this section—

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

1 “(B) shall leverage, when possible, Federal
2 investments through collaboration with related
3 State initiatives;

4 “(C) shall include a plan for fostering the
5 transfer of research discoveries and the results
6 of technology demonstration activities, including
7 from institutions of higher education and Fed-
8 eral laboratories, to industry for commercial de-
9 velopment;

10 “(D) shall involve collaborations among re-
11 searchers in institutions of higher education
12 and industry; and

13 “(E) may involve collaborations among
14 nonprofit research institutions and Federal lab-
15 oratories, as appropriate.

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

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

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

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

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

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

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

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

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

23 (c) TASK FORCE.—Title I of the High-Performance
24 Computing Act of 1991 (15 U.S.C. 5511 et seq.), as

1 amended by section 402(a) of this Act, is amended by add-
2 ing at the end the following:

3 **“SEC. 105. TASK FORCE.**

4 “(a) ESTABLISHMENT.—Not later than 180 days
5 after the date of enactment the Strengthening and En-
6 hancing Cybersecurity by Using Research, Education, In-
7 formation, and Technology Act of 2013, the Director of
8 the Office of Science and Technology Policy under section
9 102 shall convene a task force to explore mechanisms for
10 carrying out collaborative research and development activi-
11 ties for cyber-physical systems (including the related tech-
12 nologies required to enable these systems) through a con-
13 sortium or other appropriate entity with participants from
14 institutions of higher education, Federal laboratories, and
15 industry.

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

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

24 “(2) propose a process for developing a re-
25 search and development agenda for such entity, in-

1 including guidelines to ensure an appropriate scope of
2 work focused on nationally significant challenges and
3 requiring collaboration and to ensure the develop-
4 ment of related scientific and technological mile-
5 stones;

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

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

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

15 “(c) COMPOSITION.—In establishing the task force
16 under subsection (a), the Director of the Office of Science
17 and Technology Policy shall appoint an equal number of
18 individuals from institutions of higher education and from
19 industry with knowledge and expertise in cyber-physical
20 systems, and may appoint not more than 2 individuals
21 from Federal laboratories.

22 “(d) REPORT.—Not later than 1 year after the date
23 of enactment of the Strengthening and Enhancing Cyber-
24 security by Using Research, Education, Information, and
25 Technology Act of 2013, the Director of the Office of

1 Science and Technology Policy shall transmit to the Com-
2 mittee on Commerce, Science, and Transportation of the
3 Senate and the Committee on Science and Technology of
4 the House of Representatives a report describing the find-
5 ings and recommendations of the task force.

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

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

11 **SEC. 403. PROGRAM IMPROVEMENTS.**

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

14 **“SEC. 102. PROGRAM IMPROVEMENTS.**

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

17 “(1) to provide technical and administrative
18 support to—

19 “(A) the agencies participating in planning
20 and implementing the Program, including sup-
21 port needed to develop the strategic plan under
22 section 101(e); and

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

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

8 “(3) to solicit input and recommendations from
9 a wide range of stakeholders during the development
10 of each strategic plan under section 101(e) by con-
11 vening at least 1 workshop with invitees from aca-
12 demia, industry, Federal laboratories, and other rel-
13 evant organizations and institutions;

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

17 “(5) to promote access to and early application
18 of the technologies, innovations, and expertise de-
19 rived from Program activities to agency missions
20 and systems across the Federal Government and to
21 United States industry;

22 “(6) to ensure accurate and detailed budget re-
23 porting of networking and information technology
24 research and development investment; and

1 “(7) to encourage agencies participating in the
2 Program to use existing programs and resources to
3 strengthen networking and information technology
4 education and training, and increase participation in
5 such fields, including by women and underrep-
6 resented minorities.

7 “(b) SOURCE OF FUNDING.—

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

11 “(2) SPECIFICATIONS.—The portion of the total
12 budget of the Office of Science and Technology Pol-
13 icy that is provided by each agency participating in
14 the Program for each fiscal year shall be in the
15 same proportion as each agency’s share of the total
16 budget for the Program for the previous fiscal year,
17 as specified in the database under section 102(c).

18 “(c) DATABASE.—

19 “(1) IN GENERAL.—The Director of the Office
20 of Science and Technology Policy shall develop and
21 maintain a database of projects funded by each
22 agency for the fiscal year for each Program Compo-
23 nent Area.

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

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

6 “(A) a description of the project;

7 “(B) each agency, industry, institution of
8 higher education, Federal laboratory, or inter-
9 national institution involved in the project;

10 “(C) the source funding of the project (set
11 forth by agency);

12 “(D) the funding history of the project;
13 and

14 “(E) whether the project has been com-
15 pleted.”.

16 **SEC. 404. IMPROVING EDUCATION OF NETWORKING AND**
17 **INFORMATION TECHNOLOGY, INCLUDING**
18 **HIGH PERFORMANCE COMPUTING.**

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

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

23 (2) by inserting after paragraph (1) the fol-
24 lowing:

1 “(2) the National Science Foundation shall use
2 its existing programs, in collaboration with other
3 agencies, as appropriate, to improve the teaching
4 and learning of networking and information tech-
5 nology at all levels of education and to increase par-
6 ticipation in networking and information technology
7 fields;”.

8 **SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO**
9 **THE HIGH-PERFORMANCE COMPUTING ACT**
10 **OF 1991.**

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

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

16 (2) in paragraph (1)—

17 (A) in the matter preceding subparagraph
18 (A), by striking “high-performance computing”
19 and inserting “networking and information
20 technology”;

21 (B) in subparagraphs (A), (F), and (G), by
22 striking “high-performance computing” each
23 place it appears and inserting “networking and
24 information technology”; and

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

5 (A) by striking “high-performance com-
6 puting and” and inserting “networking and in-
7 formation technology, and”; and

8 (B) by striking “high-performance com-
9 puting network” and inserting “networking and
10 information technology”.

11 (b) TITLE HEADING.—The heading of title I of the
12 High-Performance Computing Act of 1991 (105 Stat.
13 1595) is amended by striking “**HIGH-PERFORM-**
14 **ANCE COMPUTING**” and inserting “**NET-**
15 **WORKING AND INFORMATION TECH-**
16 **NOLOGY**”.

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

20 (1) in the section heading, by striking “**HIGH-**
21 **PERFORMANCE COMPUTING**” and inserting
22 “**NETWORKING AND INFORMATION TECH-**
23 **NOLOGY RESEARCH AND DEVELOPMENT**”;

24 (2) in subsection (a)—

1 (A) in the subsection heading, by striking
2 “NATIONAL HIGH-PERFORMANCE COMPUTING”
3 and inserting “NETWORKING AND INFORMA-
4 TION TECHNOLOGY RESEARCH AND DEVELOP-
5 MENT”;

6 (B) in paragraph (1)—

7 (i) by striking “National High-Per-
8 formance Computing Program” and insert-
9 ing “networking and information tech-
10 nology research and development pro-
11 gram”;

12 (ii) in subparagraph (A), by striking
13 “high-performance computing, including
14 networking” and inserting “networking
15 and information technology”;

16 (iii) in subparagraphs (B) and (G), by
17 striking “high-performance” each place it
18 appears and inserting “high-end”; and

19 (iv) in subparagraph (C), by striking
20 “high-performance computing and net-
21 working” and inserting “high-end com-
22 puting, distributed, and networking”; and

23 (C) in paragraph (2)—

24 (i) in subparagraphs (A) and (C)—

1 (I) by striking “high-performance
2 computing” each place it appears and
3 inserting “networking and information
4 technology”; and

5 (II) by striking “development,
6 networking,” each place it appears
7 and inserting “development,”; and

8 (ii) in subparagraphs (G) and (H), as
9 redesignated by section 401(d) of this Act,
10 by striking “high-performance” each place
11 it appears and inserting “high-end”;

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

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

19 (d) SECTION 201.—Section 201(a)(1) of the High-
20 Performance Computing Act of 1991 (15 U.S.C.
21 5521(a)(1)) is amended by striking “high-performance
22 computing and advanced high-speed computer net-
23 working” and inserting “networking and information tech-
24 nology research and development”.

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

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

8 (1) in paragraph (1), by striking “high-per-
9 formance computing and networking” and inserting
10 “networking and information technology”; and

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

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

16 (1) in subsection (a)(1)—

17 (A) in subparagraph (A), by striking
18 “high-performance computing systems and net-
19 works” and inserting “networking and informa-
20 tion technology systems and capabilities”;

21 (B) in subparagraph (B), by striking
22 “interoperability of high-performance com-
23 puting systems in networks and for common
24 user interfaces to systems” and inserting

1 “interoperability and usability of networking
2 and information technology systems”; and

3 (C) in subparagraph (C), by striking
4 “high-performance computing” and inserting
5 “networking and information technology”; and
6 (2) in subsection (b)—

7 (A) by striking “HIGH-PERFORMANCE
8 COMPUTING AND NETWORK” in the heading
9 and inserting “NETWORKING AND INFORMA-
10 TION TECHNOLOGY”; and

11 (B) by striking “sensitive”.

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

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

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

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

4 (1) in the section heading, by striking “**HIGH-**
5 **PERFORMANCE COMPUTING**” and inserting
6 “**NETWORKING AND INFORMATION TECH-**
7 **NOLOGY**”; and

8 (2) in subsection (a)—

9 (A) in paragraph (1), by striking “High-
10 performance computing and associated” and in-
11 serting “Networking and information”;

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

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

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

20 (E) in paragraph (5), by striking “high-
21 performance computing and associated” and in-
22 serting “networking and information”.

1 **SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
2 **PROGRAM.**

3 (a) IN GENERAL.—The Director of the National
4 Science Foundation, in coordination with the Secretary of
5 Homeland Security, shall carry out a Federal cyber schol-
6 arship-for-service program to recruit and train the next
7 generation of information technology professionals and se-
8 curity managers to meet the needs of the cybersecurity
9 mission for the Federal Government.

10 (b) PROGRAM DESCRIPTION AND COMPONENTS.—
11 The program shall—

12 (1) annually assess the workforce needs of the
13 Federal Government for cybersecurity professionals,
14 including network engineers, software engineers, and
15 other experts in order to determine how many schol-
16 arships should be awarded annually to ensure that
17 the workforce needs following graduation match the
18 number of scholarships awarded;

19 (2) provide scholarships for up to 1,000 stu-
20 dents per year in their pursuit of undergraduate or
21 graduate degrees in the cybersecurity field, in an
22 amount that may include coverage for full tuition,
23 fees, and a stipend;

24 (3) require each scholarship recipient, as a con-
25 dition of receiving a scholarship under the program,
26 to serve in a Federal information technology work-

1 force for a period equal to one and one-half times
2 each year, or partial year, of scholarship received, in
3 addition to an internship in the cybersecurity field,
4 if applicable, following graduation;

5 (4) provide a procedure for the National
6 Science Foundation or a Federal agency, consistent
7 with regulations of the Office of Personnel Manage-
8 ment, to request and fund a security clearance for
9 a scholarship recipient, including providing for clear-
10 ance during a summer internship and upon gradua-
11 tion; 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 student's studies, a student re-
21 ceiving a 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.—The eligibility requirements for a
7 scholarship under this section shall include that a scholar-
8 ship applicant—

9 (1) be a citizen of the United States;

10 (2) be eligible to be granted a security clear-
11 ance;

12 (3) maintain a grade point average of 3.2 or
13 above on a 4.0 scale for undergraduate study or a
14 3.5 or above on a 4.0 scale for postgraduate study;

15 (4) demonstrate a commitment to a career in
16 improving the security of the information infrastruc-
17 ture; and

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

20 (e) FAILURE TO COMPLETE SERVICE OBLIGA-
21 TION.—

22 (1) IN GENERAL.—A scholarship recipient
23 under this section shall be liable to the United
24 States under paragraph (2) if the scholarship recipi-
25 ent—

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

5 (B) is dismissed from such educational in-
6 stitution for disciplinary reasons;

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

10 (D) declares that the individual does not
11 intend to fulfill the service obligation under this
12 section;

13 (E) fails to fulfill the service obligation of
14 the individual under this section; or

15 (F) loses a security clearance or becomes
16 ineligible for a security clearance.

17 (2) REPAYMENT AMOUNTS.—

18 (A) LESS THAN 1 YEAR OF SERVICE.—If a
19 circumstance under paragraph (1) occurs before
20 the completion of 1 year of a service obligation
21 under this section, the total amount of awards
22 received by the individual under this section
23 shall be repaid.

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

1 (D) or (E) of paragraph (1) occurs after the
2 completion of 1 year of a service obligation
3 under this section, the total amount of scholar-
4 ship awards received by the individual under
5 this section, reduced by the ratio of the number
6 of years of service completed divided by the
7 number of years of service required, shall be re-
8 paid.

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

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

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

19 (g) AUTHORIZATION OF APPROPRIATIONS.—From
20 amounts made available under section 503 of the America
21 COMPETES Reauthorization Act of 2010 (124 Stat.
22 4005), the Secretary may use funds to carry out the re-
23 quirements of this section for fiscal years 2014 through
24 2015.

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

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

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

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

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

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

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

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

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

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

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

1 **SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL**
2 **STANDARDS.**

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

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

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

14 (b) CONSULTATION WITH THE PRIVATE SECTOR.—
15 In carrying out the activities under subsection (a)(1), the
16 Director shall ensure consultation with appropriate private
17 sector stakeholders.

18 **SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
19 **OPMENT.**

20 The Director of the National Institute of Standards
21 and Technology shall continue a program to support the
22 development of technical standards, metrology, testbeds,
23 and conformance criteria, taking into account appropriate
24 user concerns—

25 (1) to improve interoperability among identity
26 management technologies;

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

3 (3) to improve privacy protection in identity
4 management systems, including health information
5 technology systems, through authentication and se-
6 curity protocols; and

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

9 **SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DE-**
10 **VELOPMENT.**

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

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

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

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

20 “(J) secure fundamental protocols that are
21 at the heart of inter-network communications
22 and data exchange;

23 “(K) system security that addresses the
24 building of secure systems from trusted and
25 untrusted components;

1 “(L) monitoring and detection; and

2 “(M) resiliency and rapid recovery meth-
3 ods.”.

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

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

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

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

12 “(F) such funds from amounts made avail-
13 able under section 503 of the America COM-
14 PETES Reauthorization Act of 2010 (124
15 Stat. 4005), as the Secretary finds necessary to
16 carry out the requirements of this subsection
17 for fiscal years 2014 through 2015.”.

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

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

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

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

1 “(F) such funds from amounts made avail-
2 able under section 503 of the America COM-
3 PETES Reauthorization Act of 2010 (124
4 Stat. 4005), as the Secretary finds necessary to
5 carry out the requirements of this subsection
6 for fiscal years 2014 through 2015.”.

7 (d) COMPUTER AND NETWORK SECURITY CAPACITY
8 BUILDING GRANTS.—Section 5(a)(6) of the Cyber Secu-
9 rity Research and Development Act (15 U.S.C.
10 7404(a)(6)) is amended—

- 11 (1) in subparagraph (D), by striking “and”;
12 (2) in subparagraph (E), by striking “2007.”
13 and inserting “2007;”; and
14 (3) by adding at the end the following:

15 “(F) such funds from amounts made avail-
16 able under section 503 of the America COM-
17 PETES Reauthorization Act of 2010 (124
18 Stat. 4005), as the Secretary finds necessary to
19 carry out the requirements of this subsection
20 for fiscal years 2014 through 2015.”.

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

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

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

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

4 “(F) such funds from amounts made avail-
5 able under section 503 of the America COM-
6 PETES Reauthorization Act of 2010 (124
7 Stat. 4005), as the Secretary finds necessary to
8 carry out the requirements of this subsection
9 for fiscal years 2014 through 2015.”.

10 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
11 NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the
12 Cyber Security Research and Development Act (15 U.S.C.
13 7404(c)(7)) is amended—

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

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

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

18 “(F) such funds from amounts made avail-
19 able under section 503 of the America COM-
20 PETES Reauthorization Act of 2010 (124
21 Stat. 4005), as the Secretary finds necessary to
22 carry out the requirements of this subsection
23 for fiscal years 2014 through 2015.”.

1 **TITLE V—DATA SECURITY AND**
2 **BREACH NOTIFICATION**

3 **SEC. 501. REQUIREMENTS FOR INFORMATION SECURITY.**

4 Each covered entity shall take reasonable measures
5 to protect and secure data in electronic form containing
6 personal information.

7 **SEC. 502. NOTIFICATION OF INFORMATION SECURITY**
8 **BREACH.**

9 (a) NOTIFICATION.—

10 (1) IN GENERAL.—A covered entity that owns
11 or licenses data in electronic form containing per-
12 sonal information shall give notice of any breach of
13 the security of the system following discovery by the
14 covered entity of the breach of the security of the
15 system to each individual who is a citizen or resident
16 of the United States whose personal information was
17 or that the covered entity reasonably believes to have
18 been accessed and acquired by an unauthorized per-
19 son and that the covered entity reasonably believes
20 has caused or will cause, identity theft or other fi-
21 nancial harm.

22 (2) LAW ENFORCEMENT.—A covered entity
23 shall notify the Secret Service or the Federal Bureau
24 of Investigation of the fact that a breach of security
25 has occurred if the number of individuals whose per-

1 sonal information the covered entity reasonably be-
2 lieves to have been accessed and acquired by an un-
3 authorized person exceeds 10,000.

4 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

5 (1) THIRD-PARTY AGENTS.—

6 (A) IN GENERAL.—In the event of a
7 breach of security of a system maintained by a
8 third-party entity that has been contracted to
9 maintain, store, or process data in electronic
10 form containing personal information on behalf
11 of a covered entity who owns or possesses such
12 data, such third-party entity shall notify such
13 covered entity of the breach of security.

14 (B) COVERED ENTITIES WHO RECEIVE NO-
15 TICE FROM THIRD PARTIES.—Upon receiving
16 notification from a third party under subpara-
17 graph (A), a covered entity shall provide notifi-
18 cation as required under subsection (a).

19 (C) EXCEPTION FOR SERVICE PRO-
20 VIDERS.—A service provider shall not be consid-
21 ered a third-party agent for purposes of this
22 paragraph.

23 (2) SERVICE PROVIDERS.—

24 (A) IN GENERAL.—If a service provider be-
25 comes aware of a breach of security involving

1 data in electronic form containing personal in-
2 formation that is owned or possessed by a cov-
3 ered entity that connects to or uses a system or
4 network provided by the service provider for the
5 purpose of transmitting, routing, or providing
6 intermediate or transient storage of such data,
7 such service provider shall notify the covered
8 entity who initiated such connection, trans-
9 mission, routing, or storage if such covered en-
10 tity can be reasonably identified.

11 (B) COVERED ENTITIES WHO RECEIVE NO-
12 TICE FROM SERVICE PROVIDERS.—Upon receiv-
13 ing notification from a service provider under
14 subparagraph (A), a covered entity shall provide
15 notification as required under subsection (a).

16 (c) TIMELINESS OF NOTIFICATION.—

17 (1) IN GENERAL.—Unless subject to a delay au-
18 thorized under paragraph (2), a notification required
19 under subsection (a) with respect to a security
20 breach shall be made as expeditiously as practicable
21 and without unreasonable delay, consistent with any
22 measures necessary to determine the scope of the se-
23 curity breach and restore the reasonable integrity of
24 the data system that was breached.

1 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
2 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
3 POSES.—

4 (A) LAW ENFORCEMENT.—If a Federal
5 law enforcement agency determines that the no-
6 tification required under subsection (a) would
7 impede a civil or criminal investigation, such
8 notification shall be delayed upon the written
9 request of the law enforcement agency for any
10 period which the law enforcement agency deter-
11 mines is reasonably necessary. A law enforce-
12 ment agency may, by a subsequent written re-
13 quest, revoke such delay or extend the period
14 set forth in the original request made under
15 this subparagraph by a subsequent request if
16 further delay is necessary.

17 (B) NATIONAL SECURITY.—If a Federal
18 national security agency or homeland security
19 agency determines that the notification required
20 under this section would threaten national or
21 homeland security, such notification may be de-
22 layed upon the written request of the national
23 security agency or homeland security agency for
24 any period which the national security agency
25 or homeland security agency determines is rea-

1 sonably necessary. A Federal national security
2 agency or homeland security agency may revoke
3 such delay or extend the period set forth in the
4 original request made under this subparagraph
5 by a subsequent written request if further delay
6 is necessary.

7 (d) METHOD AND CONTENT OF NOTIFICATION.—

8 (1) DIRECT NOTIFICATION.—

9 (A) METHOD OF NOTIFICATION.—A cov-
10 ered entity required to provide notification to
11 an individual under subsection (a) shall be in
12 compliance with such requirement if the covered
13 entity provides such notice by one of the fol-
14 lowing methods:

15 (i) Written notification, sent to the
16 postal address of the individual in the
17 records of the covered entity.

18 (ii) Telephone.

19 (iii) Email or other electronic means.

20 (B) CONTENT OF NOTIFICATION.—Regard-
21 less of the method by which notification is pro-
22 vided to an individual under subparagraph (A)
23 with respect to a security breach, such notifica-
24 tion, to the extent practicable, shall include—

1 (i) the date, estimated date, or esti-
2 mated date range of the breach of security;

3 (ii) a description of the personal infor-
4 mation that was accessed and acquired, or
5 reasonably believed to have been accessed
6 and acquired, by an unauthorized person
7 as a part of the security breach; and

8 (iii) information that the individual
9 can use to contact the covered entity to in-
10 quire about—

11 (I) the breach of security; or

12 (II) the information the covered
13 entity maintained about that indi-
14 vidual.

15 (2) SUBSTITUTE NOTIFICATION.—

16 (A) CIRCUMSTANCES GIVING RISE TO SUB-
17 STITUTE NOTIFICATION.—A covered entity re-
18 quired to provide notification to an individual
19 under subsection (a) may provide substitute no-
20 tification in lieu of the direct notification re-
21 quired by paragraph (1) if such direct notifica-
22 tion is not feasible due to—

23 (i) excessive cost to the covered entity
24 required to provide such notification rel-

1 ative to the resources of such covered enti-
2 ty; or

3 (ii) lack of sufficient contact informa-
4 tion for the individual required to be noti-
5 fied.

6 (B) FORM OF SUBSTITUTE NOTIFICA-
7 TION.—Such substitute notification shall in-
8 clude at least one of the following:

9 (i) A conspicuous notice on the Inter-
10 net website of the covered entity (if such
11 covered entity maintains such a website).

12 (ii) Notification in print and to broad-
13 cast media, including major media in met-
14 ropolitan and rural areas where the indi-
15 viduals whose personal information was ac-
16 quired reside.

17 (e) TREATMENT OF PERSONS GOVERNED BY OTHER
18 FEDERAL LAW.—Except as provided in section 503(b), a
19 covered entity who is in compliance with any other Federal
20 law that requires such covered entity to provide notifica-
21 tion to individuals following a breach of security shall be
22 deemed to be in compliance with this section.

23 **SEC. 503. APPLICATION AND ENFORCEMENT.**

24 (a) GENERAL APPLICATION.—The requirements of
25 sections 501 and 502 apply to—

1 (1) those persons, partnerships, or corporations
2 over which the Commission has authority pursuant
3 to section 5(a)(2) of the Federal Trade Commission
4 Act (15 U.S.C. 45(a)(2)); and

5 (2) notwithstanding section 5(a)(2) of the Fed-
6 eral Trade Commission Act (15 U.S.C. 45(a)(2)),
7 common carriers subject to the Communications Act
8 of 1934 (47 U.S.C. 151 et seq.).

9 (b) APPLICATION TO CABLE OPERATORS, SATELLITE
10 OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—
11 Sections 222, 338, and 631 of the Communications Act
12 of 1934 (47 U.S.C. 222, 338, and 551), and any regula-
13 tions promulgated thereunder, shall not apply with respect
14 to the information security practices, including practices
15 relating to the notification of unauthorized access to data
16 in electronic form, of any covered entity otherwise subject
17 to those sections.

18 (c) ENFORCEMENT BY FEDERAL TRADE COMMIS-
19 SION.—

20 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
21 TICES.—A violation of section 501 or 502 shall be
22 treated as an unfair or deceptive act or practice in
23 violation of a regulation under section 18(a)(1)(B)
24 of the Federal Trade Commission Act (15 U.S.C.

1 57a(a)(1)(B)) regarding unfair or deceptive acts or
2 practices.

3 (2) POWERS OF COMMISSION.—

4 (A) IN GENERAL.—Except as provided in
5 subsection (a), the Commission shall enforce
6 this title in the same manner, by the same
7 means, and with the same jurisdiction, powers,
8 and duties as though all applicable terms and
9 provisions of the Federal Trade Commission
10 Act (15 U.S.C. 41 et seq.) were incorporated
11 into and made a part of this title.

12 (B) PRIVILEGES AND IMMUNITIES.—Any
13 person who violates section 502 or 503 shall be
14 subject to the penalties and entitled to the
15 privileges and immunities provided in such Act.

16 (3) MAXIMUM TOTAL LIABILITY.—Notwith-
17 standing the number of actions which may be
18 brought against a covered entity under this sub-
19 section, the maximum civil penalty for which any
20 covered entity may be liable under this subsection
21 for all actions shall not exceed—

22 (A) \$500,000 for all violations of section
23 501 resulting from the same related act or
24 omission; and

1 (B) \$500,000 for all violations of section
2 502 resulting from a single breach of security.

3 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
4 this title shall be construed to establish a private cause
5 of action against a person for a violation of this title.

6 **SEC. 504. DEFINITIONS.**

7 In this title:

8 (1) BREACH OF SECURITY.—The term “breach
9 of security” means unauthorized access and acquisi-
10 tion of data in electronic form containing personal
11 information.

12 (2) COMMISSION.—The term “Commission”
13 means the Federal Trade Commission.

14 (3) COVERED ENTITY.—

15 (A) IN GENERAL.—The term “covered en-
16 tity” means a sole proprietorship, partnership,
17 corporation, trust, estate, cooperative, associa-
18 tion, or other commercial entity that acquires,
19 maintains, stores, or utilizes personal informa-
20 tion.

21 (B) EXEMPTIONS.—The term “covered en-
22 tity” does not include the following:

23 (i) Financial institutions subject to
24 title V of the Gramm-Leach-Bliley Act (15
25 U.S.C. 6801 et seq.).

1 (ii) An entity covered by the regula-
2 tions issued under section 264(c) of the
3 Health Insurance Portability and Account-
4 ability Act of 1996 (Public Law 104–191)
5 to the extent that such entity is subject to
6 the requirements of such regulations with
7 respect to protected health information.

8 (4) DATA IN ELECTRONIC FORM.—The term
9 “data in electronic form” means any data stored
10 electronically or digitally on any computer system or
11 other database and includes recordable tapes and
12 other mass storage devices.

13 (5) PERSONAL INFORMATION.—

14 (A) IN GENERAL.—The term “personal in-
15 formation” means an individual’s first name or
16 first initial and last name in combination with
17 any 1 or more of the following data elements
18 for that individual:

19 (i) Social Security number.

20 (ii) Driver’s license number, passport
21 number, military identification number, or
22 other similar number issued on a govern-
23 ment document used to verify identity.

24 (iii) Financial account number, or
25 credit or debit card number, and any re-

1 required security code, access code, or pass-
2 word that is necessary to permit access to
3 an individual's financial account.

4 (B) EXCLUSIONS.—

5 (i) PUBLIC RECORD INFORMATION.—

6 Personal information does not include in-
7 formation obtained about an individual
8 which has been lawfully made publicly
9 available by a Federal, State, or local gov-
10 ernment entity or widely distributed by
11 media.

12 (ii) ENCRYPTED, REDACTED, OR SE-
13 CURED DATA.—

14 Personal information does
15 not include information that is encrypted,
16 redacted, or secured by any other method
17 or technology that renders the data ele-
18 ments unusable.

19 (6) SERVICE PROVIDER.—

20 The term “service
21 provider” means an entity that provides electronic
22 data transmission, routing, intermediate, and tran-
23 sient storage, or connections to its system or net-
24 work, where such entity providing such services does
25 not select or modify the content of the electronic
26 data, is not the sender or the intended recipient of
27 the data, and does not differentiate personal infor-

1 mation from other information that such entity
2 transmits, routes, stores, or for which such entity
3 provides connections. Any such entity shall be treat-
4 ed as a service provider under this title only to the
5 extent that it is engaged in the provision of such
6 transmission, routing, intermediate and transient
7 storage, or connections.

8 **SEC. 505. EFFECT ON OTHER LAWS.**

9 This title preempts any law, rule, regulation, require-
10 ment, standard, or other provision having the force and
11 effect of law of any State, or political subdivision of a
12 State, relating to the protection or security of data in elec-
13 tronic form containing personal information or the notifi-
14 cation of a breach of security.

15 **SEC. 506. EFFECTIVE DATE.**

16 This title shall take effect on the date that is 1 year
17 after the date of enactment of this Act.

○