

113TH CONGRESS
1ST SESSION

H. R. 756

To advance cybersecurity research, development, and technical standards,
and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 15, 2013

Mr. MCCAUL (for himself, Mr. LIPINSKI, Mr. SMITH of Texas, Mr. LANGEVIN, Mr. MEEHAN, Ms. MATSUI, Mr. HALL, and Mr. BEN RAY LUJÁN of New Mexico) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

A BILL

To advance cybersecurity research, development, and
technical standards, 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.**

4 This Act may be cited as the “Cybersecurity En-
5 hancement Act of 2013”.

6 **TITLE I—RESEARCH AND**
7 **DEVELOPMENT**

8 **SEC. 101. DEFINITIONS.**

9 In this title:

1 (1) NATIONAL COORDINATION OFFICE.—The
2 term National Coordination Office means the Na-
3 tional Coordination Office for the Networking and
4 Information Technology Research and Development
5 program.

6 (2) PROGRAM.—The term Program means the
7 Networking and Information Technology Research
8 and Development program which has been estab-
9 lished under section 101 of the High-Performance
10 Computing Act of 1991 (15 U.S.C. 5511).

11 **SEC. 102. FINDINGS.**

12 Section 2 of the Cyber Security Research and Devel-
13 opment Act (15 U.S.C. 7401) is amended—

14 (1) by amending paragraph (1) to read as fol-
15 lows:

16 “(1) Advancements in information and commu-
17 nications technology have resulted in a globally
18 interconnected network of government, commercial,
19 scientific, and education infrastructures, including
20 critical infrastructures for electric power, natural
21 gas and petroleum production and distribution, tele-
22 communications, transportation, water supply, bank-
23 ing and finance, and emergency and government
24 services.”;

1 (2) in paragraph (2), by striking “Exponential
2 increases in interconnectivity have facilitated en-
3 hanced communications, economic growth,” and in-
4 serting “These advancements have significantly con-
5 tributed to the growth of the United States econ-
6 omy.”;

7 (3) by amending paragraph (3) to read as fol-
8 lows:

9 “(3) The Cyberspace Policy Review published
10 by the President in May, 2009, concluded that our
11 information technology and communications infra-
12 structure is vulnerable and has ‘suffered intrusions
13 that have allowed criminals to steal hundreds of mil-
14 lions of dollars and nation-states and other entities
15 to steal intellectual property and sensitive military
16 information’.”; and

17 (4) by amending paragraph (6) to read as fol-
18 lows:

19 “(6) While African-Americans, Hispanics, and
20 Native Americans constitute 33 percent of the col-
21 lege-age population, members of these minorities
22 comprise less than 20 percent of bachelor degree re-
23 cipients in the field of computer sciences.”.

1 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
2 **VELOPMENT PLAN.**

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

19 (b) CONTENTS OF PLAN.—The strategic plan re-
20 quired under subsection (a) shall—

21 (1) specify and prioritize near-term, mid-term
22 and long-term research objectives, including objec-
23 tives associated with the research areas identified in
24 section 4(a)(1) of the Cyber Security Research and
25 Development Act (15 U.S.C. 7403(a)(1)) and how
26 the near-term objectives complement research and

1 development areas in which the private sector is ac-
2 tively engaged;

3 (2) describe how the Program will focus on in-
4 novative, transformational technologies with the po-
5 tential to enhance the security, reliability, resilience,
6 and trustworthiness of the digital infrastructure, and
7 to protect consumer privacy;

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

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

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

23 (6) describe how the Program will engage fe-
24 males and individuals identified in section 33 or 34
25 of the Science and Engineering Equal Opportunities

1 Act (42 U.S.C. 1885a or 1885b) to foster a more di-
2 verse workforce in this area.

3 (c) DEVELOPMENT OF ROADMAP.—The agencies de-
4 scribed in subsection (a) shall develop and annually update
5 an implementation roadmap for the strategic plan re-
6 quired in this section. Such roadmap shall—

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

12 (2) specify the funding allocated to each major
13 research objective of the strategic plan and the
14 source of funding by agency for the current fiscal
15 year; and

16 (3) estimate the funding required for each
17 major research objective of the strategic plan for the
18 following 3 fiscal years.

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

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

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

6 (e) APPENDING TO REPORT.—The implementation
7 roadmap required under subsection (c), and its annual up-
8 dates, shall be appended to the report required under sec-
9 tion 101(a)(2)(D) of the High-Performance Computing
10 Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

11 **SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBER-**
12 **SECURITY.**

13 Section 4(a)(1) of the Cyber Security Research and
14 Development Act (15 U.S.C. 7403(a)(1)) is amended—

15 (1) by inserting “and usability” after “to the
16 structure”;

17 (2) in subparagraph (H), by striking “and”
18 after the semicolon;

19 (3) in subparagraph (I), by striking the period
20 at the end and inserting “; and”; and

21 (4) by adding at the end the following new sub-
22 paragraph:

23 “(J) social and behavioral factors, includ-
24 ing human-computer interactions, usability, and
25 user motivations.”.

1 **SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.**
2
3

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

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

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

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

18 “(A) \$90,000,000 for fiscal year 2014;

19 “(B) \$90,000,000 for fiscal year 2015; and

20 “(C) \$90,000,000 for fiscal year 2016.”.

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

24 (1) in paragraph (4)—

25 (A) in subparagraph (C), by striking

26 “and” after the semicolon;

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

3 (C) by adding at the end the following new
4 subparagraph:

5 “(E) how the center will partner with gov-
6 ernment laboratories, for-profit entities, other
7 institutions of higher education, or nonprofit re-
8 search institutions.”; and

9 (2) in paragraph (7) by striking subparagraphs
10 (A) through (E) and inserting the following new
11 subparagraphs:

12 “(A) \$4,500,000 for fiscal year 2014;

13 “(B) \$4,500,000 for fiscal year 2015; and

14 “(C) \$4,500,000 for fiscal year 2016.”.

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

20 “(A) \$19,000,000 for fiscal year 2014;

21 “(B) \$19,000,000 for fiscal year 2015; and

22 “(C) \$19,000,000 for fiscal year 2016.”.

23 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
24 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
25 7404(b)(2)) is amended by striking subparagraphs (A)

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

3 “(A) \$2,500,000 for fiscal year 2014;

4 “(B) \$2,500,000 for fiscal year 2015; and

5 “(C) \$2,500,000 for fiscal year 2016.”.

6 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
7 NETWORK SECURITY.—Section 5(c)(7) of such Act (15
8 U.S.C. 7404(c)(7)) is amended by striking subparagraphs
9 (A) through (E) and inserting the following new subpara-
10 graphs:

11 “(A) \$24,000,000 for fiscal year 2014;

12 “(B) \$24,000,000 for fiscal year 2015; and

13 “(C) \$24,000,000 for fiscal year 2016.”.

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

17 **SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE**
18 **PROGRAM.**

19 (a) IN GENERAL.—The Director of the National
20 Science Foundation shall continue a Scholarship for Serv-
21 ice program under section 5(a) of the Cyber Security Re-
22 search and Development Act (15 U.S.C. 7404(a)) to re-
23 cruit and train the next generation of Federal cybersecu-
24 rity professionals and to increase the capacity of the high-
25 er education system to produce an information technology

1 workforce with the skills necessary to enhance the security
2 of the Nation's communications and information infra-
3 structure.

4 (b) CHARACTERISTICS OF PROGRAM.—The program
5 under this section shall—

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

12 (2) provide the scholarship recipients with sum-
13 mer internship opportunities or other meaningful
14 temporary appointments in the Federal information
15 technology workforce; and

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

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

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

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

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

8 (c) SCHOLARSHIP REQUIREMENTS.—

9 (1) ELIGIBILITY.—Scholarships under this sec-
10 tion shall be available only to students who—

11 (A) are citizens or permanent residents of
12 the United States;

13 (B) are full-time students in an eligible de-
14 gree program, as determined by the Director,
15 that is focused on computer security or infor-
16 mation assurance at an awardee institution;
17 and

18 (C) accept the terms of a scholarship pur-
19 suant to this section.

20 (2) SELECTION.—Individuals shall be selected
21 to receive scholarships primarily on the basis of aca-
22 demic merit, with consideration given to financial
23 need, to the goal of promoting the participation of
24 individuals identified in section 33 or 34 of the
25 Science and Engineering Equal Opportunities Act

1 (42 U.S.C. 1885a or 1885b), and to veterans. For
2 purposes of this paragraph, the term “veteran”
3 means a person who—

4 (A) served on active duty (other than ac-
5 tive duty for training) in the Armed Forces of
6 the United States for a period of more than
7 180 consecutive days, and who was discharged
8 or released therefrom under conditions other
9 than dishonorable; or

10 (B) served on active duty (other than ac-
11 tive duty for training) in the Armed Forces of
12 the United States and was discharged or re-
13 leased from such service for a service-connected
14 disability before serving 180 consecutive days.

15 For purposes of subparagraph (B), the term “serv-
16 ice-connected” has the meaning given such term
17 under section 101 of title 38, United States Code.

18 (3) SERVICE OBLIGATION.—If an individual re-
19 ceives a scholarship under this section, as a condi-
20 tion of receiving such scholarship, the individual
21 upon completion of their degree must serve as a cy-
22 bersecurity professional within the Federal workforce
23 for a period of time as provided in paragraph (5).
24 If a scholarship recipient is not offered employment
25 by a Federal agency or a federally funded research

1 and development center, the service requirement can
2 be satisfied at the Director's discretion by—

3 (A) serving as a cybersecurity professional
4 in a State, local, or tribal government agency;
5 or

6 (B) teaching cybersecurity courses at an
7 institution of higher education.

8 (4) CONDITIONS OF SUPPORT.—As a condition
9 of acceptance of a scholarship under this section, a
10 recipient shall agree to provide the awardee institu-
11 tion with annual verifiable documentation of employ-
12 ment and up-to-date contact information.

13 (5) LENGTH OF SERVICE.—The length of serv-
14 ice required in exchange for a scholarship under this
15 subsection shall be 1 year more than the number of
16 years for which the scholarship was received.

17 (d) FAILURE TO COMPLETE SERVICE OBLIGA-
18 TION.—

19 (1) GENERAL RULE.—If an individual who has
20 received a scholarship under this section—

21 (A) fails to maintain an acceptable level of
22 academic standing in the educational institution
23 in which the individual is enrolled, as deter-
24 mined by the Director;

1 (B) is dismissed from such educational in-
2 stitution for disciplinary reasons;

3 (C) withdraws from the program for which
4 the award was made before the completion of
5 such program;

6 (D) declares that the individual does not
7 intend to fulfill the service obligation under this
8 section; or

9 (E) fails to fulfill the service obligation of
10 the individual under this section,

11 such individual shall be liable to the United States
12 as provided in paragraph (3).

13 (2) MONITORING COMPLIANCE.—As a condition
14 of participating in the program, a qualified institu-
15 tion of higher education receiving a grant under this
16 section shall—

17 (A) enter into an agreement with the Di-
18 rector of the National Science Foundation to
19 monitor the compliance of scholarship recipients
20 with respect to their service obligation; and

21 (B) provide to the Director, on an annual
22 basis, post-award employment information re-
23 quired under subsection (e)(4) for scholarship
24 recipients through the completion of their serv-
25 ice obligation.

1 (3) AMOUNT OF REPAYMENT.—

2 (A) LESS THAN ONE YEAR OF SERVICE.—

3 If a circumstance described in paragraph (1)
4 occurs before the completion of 1 year of a
5 service obligation under this section, the total
6 amount of awards received by the individual
7 under this section shall be repaid or such
8 amount shall be treated as a loan to be repaid
9 in accordance with subparagraph (C).

10 (B) MORE THAN ONE YEAR OF SERVICE.—

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

22 (C) REPAYMENTS.—A loan described in
23 subparagraph (A) or (B) shall be treated as a
24 Federal Direct Unsubsidized Stafford Loan
25 under part D of title IV of the Higher Edu-

1 cation Act of 1965 (20 U.S.C. 1087a and fol-
2 lowing), and shall be subject to repayment, to-
3 gether with interest thereon accruing from the
4 date of the scholarship award, in accordance
5 with terms and conditions specified by the Di-
6 rector (in consultation with the Secretary of
7 Education) in regulations promulgated to carry
8 out this paragraph.

9 (4) COLLECTION OF REPAYMENT.—

10 (A) IN GENERAL.—In the event that a
11 scholarship recipient is required to repay the
12 scholarship under this subsection, the institu-
13 tion providing the scholarship shall—

14 (i) be responsible for determining the
15 repayment amounts and for notifying the
16 recipient and the Director of the amount
17 owed; and

18 (ii) collect such repayment amount
19 within a period of time as determined
20 under the agreement described in para-
21 graph (2), or the repayment amount shall
22 be treated as a loan in accordance with
23 paragraph (3)(C).

24 (B) RETURNED TO TREASURY.—Except as
25 provided in subparagraph (C) of this para-

1 graph, any such repayment shall be returned to
2 the Treasury of the United States.

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

10 (5) EXCEPTIONS.—The Director may provide
11 for the partial or total waiver or suspension of any
12 service or payment obligation by an individual under
13 this section whenever compliance by the individual
14 with the obligation is impossible or would involve ex-
15 treme hardship to the individual, or if enforcement
16 of such obligation with respect to the individual
17 would be unconscionable.

18 (e) HIRING AUTHORITY.—For purposes of any law
19 or regulation governing the appointment of individuals in
20 the Federal civil service, upon successful completion of
21 their degree, students receiving a scholarship under this
22 section shall be hired under the authority provided for in
23 section 213.3102(r) of title 5, Code of Federal Regula-
24 tions, and be exempted from competitive service. Upon ful-
25 fillment of the service term, such individuals shall be con-

1 verted to a competitive service position without competi-
2 tion if the individual meets the requirements for that posi-
3 tion.

4 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

5 Not later than 180 days after the date of enactment
6 of this Act the President shall transmit to the Congress
7 a report addressing the cybersecurity workforce needs of
8 the Federal Government. The report shall include—

9 (1) an examination of the current state of and
10 the projected needs of the Federal cybersecurity
11 workforce, including a comparison of the different
12 agencies and departments, and an analysis of the ca-
13 pacity of such agencies and departments to meet
14 those needs;

15 (2) an analysis of the sources and availability of
16 cybersecurity talent, a comparison of the skills and
17 expertise sought by the Federal Government and the
18 private sector, an examination of the current and fu-
19 ture capacity of United States institutions of higher
20 education, including community colleges, to provide
21 current and future cybersecurity professionals,
22 through education and training activities, with those
23 skills sought by the Federal Government, State and
24 local entities, and the private sector, and a descrip-
25 tion of how successful programs are engaging the

1 talents of females and individuals identified in sec-
2 tion 33 or 34 of the Science and Engineering Equal
3 Opportunities Act (42 U.S.C. 1885a or 1885b);

4 (3) an examination of the effectiveness of the
5 National Centers of Academic Excellence in Infor-
6 mation Assurance Education, the Centers of Aca-
7 demic Excellence in Research, and the Federal
8 Cyber Scholarship for Service programs in pro-
9 moting higher education and research in cybersecu-
10 rity and information assurance and in producing a
11 growing number of professionals with the necessary
12 cybersecurity and information assurance expertise,
13 including individuals from States or regions in which
14 the unemployment rate exceeds the national average;

15 (4) an analysis of any barriers to the Federal
16 Government recruiting and hiring cybersecurity tal-
17 ent, including barriers relating to compensation, the
18 hiring process, job classification, and hiring flexibili-
19 ties; and

20 (5) recommendations for Federal policies to en-
21 sure an adequate, well-trained Federal cybersecurity
22 workforce.

1 **SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK**
2 **FORCE.**

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

12 (b) FUNCTIONS.—The task force shall—

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

20 (2) propose a process for developing a research
21 and development agenda for such entity, including
22 guidelines to ensure an appropriate scope of work fo-
23 cused on nationally significant challenges and requir-
24 ing collaboration;

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

4 (4) propose guidelines for assigning intellectual
5 property rights and for the transfer of research and
6 development results to the private sector; and

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

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

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

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

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

3 **SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS**
4 **FOR GOVERNMENT SYSTEMS.**

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

8 “(c) SECURITY AUTOMATION AND CHECKLISTS FOR
9 GOVERNMENT SYSTEMS.—

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

23 “(2) PRIORITIES FOR DEVELOPMENT.—The Di-
24 rector of the National Institute of Standards and
25 Technology shall establish priorities for the develop-

1 ment of standards, reference materials, and check-
2 lists under this subsection on the basis of—

3 “(A) the security risks associated with the
4 use of the system;

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

7 “(C) the usefulness of the standards, ref-
8 erence materials, or checklists to Federal agen-
9 cies that are users or potential users of the sys-
10 tem;

11 “(D) the effectiveness of the associated
12 standard, reference material, or checklist in cre-
13 ating or enabling continuous monitoring of in-
14 formation security; or

15 “(E) such other factors as the Director of
16 the National Institute of Standards and Tech-
17 nology determines to be appropriate.

18 “(3) EXCLUDED SYSTEMS.—The Director of
19 the National Institute of Standards and Technology
20 may exclude from the application of paragraph (1)
21 any information technology hardware or software
22 system or security tool for which such Director de-
23 termines that the development of a standard, ref-
24 erence material, or checklist is inappropriate because
25 of the infrequency of use of the system, the obsoles-

1 cence of the system, or the inutility or imprac-
2 ticability of developing a standard, reference mate-
3 rial, or checklist for the system.

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

10 “(5) AGENCY USE REQUIREMENTS.—The devel-
11 opment of standards, reference materials, and check-
12 lists under paragraph (1) for an information tech-
13 nology hardware or software system or tool does
14 not—

15 “(A) require any Federal agency to select
16 the specific settings or options recommended by
17 the standard, reference material, or checklist
18 for the system;

19 “(B) establish conditions or prerequisites
20 for Federal agency procurement or deployment
21 of any such system;

22 “(C) imply an endorsement of any such
23 system by the Director of the National Institute
24 of Standards and Technology; or

1 “(D) preclude any Federal agency from
2 procuring or deploying other information tech-
3 nology hardware or software systems for which
4 no such standard, reference material, or check-
5 list has been developed or identified under para-
6 graph (1).”.

7 **SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
8 **NOLOGY CYBERSECURITY RESEARCH AND**
9 **DEVELOPMENT.**

10 Section 20 of the National Institute of Standards and
11 Technology Act (15 U.S.C. 278g-3) is amended by redес-
12 ignating subsection (e) as subsection (f), and by inserting
13 after subsection (d) the following:

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

17 “(1) conduct a research program to develop a
18 unifying and standardized identity, privilege, and ac-
19 cess control management framework for the execu-
20 tion of a wide variety of resource protection policies
21 and that is amenable to implementation within a
22 wide variety of existing and emerging computing en-
23 vironments;

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

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

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

9 **TITLE II—ADVANCEMENT OF CY-**
10 **BERSECURITY TECHNICAL**
11 **STANDARDS**

12 **SEC. 201. DEFINITIONS.**

13 In this title:

14 (1) DIRECTOR.—The term “Director” means
15 the Director of the National Institute of Standards
16 and Technology.

17 (2) INSTITUTE.—The term “Institute” means
18 the National Institute of Standards and Technology.

19 **SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL**
20 **STANDARDS.**

21 (a) IN GENERAL.—The Director, in coordination with
22 appropriate Federal authorities, shall—

23 (1) as appropriate, ensure coordination of Fed-
24 eral agencies engaged in the development of inter-

1 national technical standards related to information
2 system security; and

3 (2) not later than 1 year after the date of en-
4 actment of this Act, develop and transmit to the
5 Congress a plan for ensuring such Federal agency
6 coordination.

7 (b) CONSULTATION WITH THE PRIVATE SECTOR.—

8 In carrying out the activities specified in subsection (a)(1),
9 the Director shall ensure consultation with appropriate
10 private sector stakeholders.

11 **SEC. 203. CLOUD COMPUTING STRATEGY.**

12 (a) IN GENERAL.—The Director, in collaboration
13 with the Federal CIO Council, and in consultation with
14 other relevant Federal agencies and stakeholders from the
15 private sector, shall continue to develop and encourage the
16 implementation of a comprehensive strategy for the use
17 and adoption of cloud computing services by the Federal
18 Government.

19 (b) ACTIVITIES.—In carrying out the strategy devel-
20 oped under subsection (a), the Director shall give consid-
21 eration to activities that—

22 (1) accelerate the development, in collaboration
23 with the private sector, of standards that address
24 interoperability and portability of cloud computing
25 services;

1 (2) advance the development of conformance
2 testing performed by the private sector in support of
3 cloud computing standardization; and

4 (3) support, in consultation with the private
5 sector, the development of appropriate security
6 frameworks and reference materials, and the identi-
7 fication of best practices, for use by Federal agen-
8 cies to address security and privacy requirements to
9 enable the use and adoption of cloud computing
10 services, including activities—

11 (A) to ensure the physical security of cloud
12 computing data centers and the data stored in
13 such centers;

14 (B) to ensure secure access to the data
15 stored in cloud computing data centers;

16 (C) to develop security standards as re-
17 quired under section 20 of the National Insti-
18 tute of Standards and Technology Act (15
19 U.S.C. 278g-3); and

20 (D) to support the development of the au-
21 tomation of continuous monitoring systems.

22 **SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND**
23 **EDUCATION.**

24 (a) PROGRAM.—The Director, in collaboration with
25 relevant Federal agencies, industry, educational institu-

1 tions, National Laboratories, the National Coordination
2 Office of the Networking and Information Technology Re-
3 search and Development program, and other organiza-
4 tions, shall continue to coordinate a cybersecurity aware-
5 ness and education program to increase knowledge, skills,
6 and awareness of cybersecurity risks, consequences, and
7 best practices through—

8 (1) the widespread dissemination of cybersecu-
9 rity technical standards and best practices identified
10 by the Institute;

11 (2) efforts to make cybersecurity best practices
12 usable by individuals, small to medium-sized busi-
13 nesses, State, local, and tribal governments, and
14 educational institutions; and

15 (3) efforts to attract, recruit, and retain quali-
16 fied professionals to the Federal cybersecurity work-
17 force.

18 (b) STRATEGIC PLAN.—The Director shall, in co-
19 operation with relevant Federal agencies and other stake-
20 holders, develop and implement a strategic plan to guide
21 Federal programs and activities in support of a com-
22 prehensive cybersecurity awareness and education pro-
23 gram as described under subsection (a).

24 (c) REPORT TO CONGRESS.—Not later than 1 year
25 after the date of enactment of this Act and every 5 years

1 thereafter, the Director shall transmit the strategic plan
2 required under subsection (b) to the Committee on
3 Science, Space, and Technology of the House of Rep-
4 resentatives and the Committee on Commerce, Science,
5 and Transportation of the Senate.

6 **SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
7 **OPMENT.**

8 The Director shall continue a program to support the
9 development of technical standards, metrology, testbeds,
10 and conformance criteria, taking into account appropriate
11 user concerns, to—

12 (1) improve interoperability among identity
13 management technologies;

14 (2) strengthen authentication methods of iden-
15 tity management systems;

16 (3) improve privacy protection in identity man-
17 agement systems, including health information tech-
18 nology systems, through authentication and security
19 protocols; and

20 (4) improve the usability of identity manage-
21 ment systems.

22 **SEC. 206. AUTHORIZATIONS.**

23 No additional funds are authorized to carry out this
24 title and the amendments made by this title or to carry
25 out the amendments made by sections 109 and 110 of this

1 Act. This title and the amendments made by this title and
2 the amendments made by sections 109 and 110 of this
3 Act shall be carried out using amounts otherwise author-
4 ized or appropriated.

○