

113TH CONGRESS
1ST SESSION

H. R. 756

IN THE SENATE OF THE UNITED STATES

APRIL 17, 2013

Received; read twice and referred to the Committee on Commerce, Science,
and Transportation

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

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

4 **TITLE I—RESEARCH AND**
5 **DEVELOPMENT**

6 **SEC. 101. DEFINITIONS.**

7 In this title:

8 (1) **NATIONAL COORDINATION OFFICE.**—The
9 term National Coordination Office means the Na-
10 tional Coordination Office for the Networking and
11 Information Technology Research and Development
12 program.

13 (2) **PROGRAM.**—The term Program means the
14 Networking and Information Technology Research
15 and Development program which has been estab-
16 lished under section 101 of the High-Performance
17 Computing Act of 1991 (15 U.S.C. 5511).

18 **SEC. 102. FINDINGS.**

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

21 (1) by amending paragraph (1) to read as fol-
22 lows:

23 “(1) Advancements in information and commu-
24 nications technology have resulted in a globally
25 interconnected network of government, commercial,
26 scientific, and education infrastructures, including

1 critical infrastructures for electric power, natural
2 gas and petroleum production and distribution, tele-
3 communications, transportation, water supply, bank-
4 ing and finance, and emergency and government
5 services.”;

6 (2) in paragraph (2), by striking “Exponential
7 increases in interconnectivity have facilitated en-
8 hanced communications, economic growth,” and in-
9 serting “These advancements have significantly con-
10 tributed to the growth of the United States econ-
11 omy,”;

12 (3) by amending paragraph (3) to read as fol-
13 lows:

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

22 (4) by amending paragraph (6) to read as fol-
23 lows:

24 “(6) While African-Americans, Hispanics, and
25 Native Americans constitute 33 percent of the col-

1 tives associated with the research areas identified in
2 section 4(a)(1) of the Cyber Security Research and
3 Development Act (15 U.S.C. 7403(a)(1)) and how
4 the near-term objectives complement research and
5 development areas in which the private sector is ac-
6 tively engaged;

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

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

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

23 (5) describe how the Program will facilitate ac-
24 cess by academic researchers to the infrastructure

1 described in paragraph (4), as well as to relevant
2 data, including event data;

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

8 (7) describe how the Program will help to re-
9 cruit and prepare veterans for the Federal cyberse-
10 curity workforce.

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

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

20 (2) specify the funding allocated to each major
21 research objective of the strategic plan and the
22 source of funding by agency for the current fiscal
23 year; and

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

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

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

10 (2) a wide range of stakeholders, including in-
11 dustry, academia, including representatives of mi-
12 nority serving institutions and community colleges,
13 National Laboratories, and other relevant organiza-
14 tions and institutions.

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

20 (f) CYBERSECURITY RESEARCH DATABASE.—The
21 agencies involved in developing and updating the strategic
22 plan under subsection (a) shall establish, in coordination
23 with the Office of Management and Budget, a mechanism
24 to track ongoing and completed Federal cybersecurity re-

1 search and development projects and associated funding,
2 and shall make such information publically available.

3 **SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBER-**
4 **SECURITY.**

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

7 (1) by inserting “and usability” after “to the
8 structure”;

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

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

13 (4) by adding at the end the following new sub-
14 paragraph:

15 “(J) social and behavioral factors, includ-
16 ing human-computer interactions, usability, and
17 user motivations.”.

18 **SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECU-**
19 **RITY RESEARCH AND DEVELOPMENT PRO-**
20 **GRAMS.**

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

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

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

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

11 “(A) \$119,000,000 for fiscal year 2014;

12 “(B) \$119,000,000 for fiscal year 2015;

13 and

14 “(C) \$119,000,000 for fiscal year 2016.”.

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

18 (1) in paragraph (4)—

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

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

23 (C) by adding at the end the following new
24 subparagraph:

1 “(E) how the center will partner with gov-
2 ernment laboratories, for-profit entities, other
3 institutions of higher education, or nonprofit re-
4 search institutions.”; and

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

8 “(A) \$5,000,000 for fiscal year 2014;

9 “(B) \$5,000,000 for fiscal year 2015; and

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

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

16 “(A) \$25,000,000 for fiscal year 2014;

17 “(B) \$25,000,000 for fiscal year 2015; and

18 “(C) \$25,000,000 for fiscal year 2016.”.

19 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
20 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
21 7404(b)(2)) is amended by striking subparagraphs (A)
22 through (E) and inserting the following new subpara-
23 graphs:

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

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

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

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

7 “(A) \$32,000,000 for fiscal year 2014;

8 “(B) \$32,000,000 for fiscal year 2015; and

9 “(C) \$32,000,000 for fiscal year 2016.”.

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

13 **SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE**
14 **PROGRAM.**

15 (a) IN GENERAL.—The Director of the National
16 Science Foundation shall continue a Scholarship for Serv-
17 ice program under section 5(a) of the Cyber Security Re-
18 search and Development Act (15 U.S.C. 7404(a)) to re-
19 cruit and train the next generation of Federal cybersecu-
20 rity professionals and to increase the capacity of the high-
21 er education system to produce an information technology
22 workforce with the skills necessary to enhance the security
23 of the Nation’s communications and information infra-
24 structure.

1 (b) CHARACTERISTICS OF PROGRAM.—The program
2 under this section shall—

3 (1) provide, through qualified institutions of
4 higher education, including community colleges,
5 scholarships that provide tuition, fees, and a com-
6 petitive stipend for up to 2 years to students pursuing
7 a bachelor’s or master’s degree and up to 3 years to
8 students pursuing a doctoral degree in a cybersecu-
9 rity field;

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

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

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

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

4 (C) development and evaluation of cyberse-
5 curity-related courses and curricula; and

6 (D) public-private partnerships that will
7 integrate research experiences and hands-on
8 learning into cybersecurity degree programs.

9 (c) SCHOLARSHIP REQUIREMENTS.—

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

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

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

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

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

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

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

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

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

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

1 by a Federal agency or a federally funded research
2 and development center, the service requirement can
3 be satisfied at the Director's discretion by—

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

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

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

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

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

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

22 (A) fails to maintain an acceptable level of
23 academic standing in the educational institution
24 in which the individual is enrolled, as deter-
25 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.—

19 (1) APPOINTMENT IN EXCEPTED SERVICE.—
20 Notwithstanding any provision of chapter 33 of title
21 5, United States Code, governing appointments in
22 the competitive service, an agency shall appoint in
23 the excepted service an individual who has completed
24 the academic program for which a scholarship was
25 awarded.

1 (2) NONCOMPETITIVE CONVERSION.—Except as
2 provided in paragraph (4), upon fulfillment of the
3 service term, an employee appointed under para-
4 graph (1) may be converted noncompetitively to
5 term, career-conditional or career appointment.

6 (3) TIMING OF CONVERSION.—An agency may
7 noncompetitively convert a term employee appointed
8 under paragraph (2) to a career-conditional or ca-
9 reer appointment before the term appointment ex-
10 pires.

11 (4) AUTHORITY TO DECLINE CONVERSION.—An
12 agency may decline to make the noncompetitive con-
13 version or appointment under paragraph (2) for
14 cause.

15 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

16 Not later than 180 days after the date of enactment
17 of this Act the President shall transmit to the Congress
18 a report addressing the cybersecurity workforce needs of
19 the Federal Government. The report shall include—

20 (1) an examination of the current state of and
21 the projected needs of the Federal cybersecurity
22 workforce, including a comparison of the different
23 agencies and departments, and an analysis of the ca-
24 pacity of such agencies and departments to meet
25 those needs;

1 (2) an analysis of the sources and availability of
2 cybersecurity talent, a comparison of the skills and
3 expertise sought by the Federal Government and the
4 private sector, an examination of the current and fu-
5 ture capacity of United States institutions of higher
6 education, including community colleges, to provide
7 current and future cybersecurity professionals,
8 through education and training activities, with those
9 skills sought by the Federal Government, State and
10 local entities, and the private sector, and a descrip-
11 tion of how successful programs are engaging the
12 talents of females and individuals identified in sec-
13 tion 33 or 34 of the Science and Engineering Equal
14 Opportunities Act (42 U.S.C. 1885a or 1885b);

15 (3) an examination of the effectiveness of the
16 National Centers of Academic Excellence in Infor-
17 mation Assurance Education, the Centers of Aca-
18 demic Excellence in Research, and the Federal
19 Cyber Scholarship for Service programs in pro-
20 moting higher education and research in cybersecu-
21 rity and information assurance and in producing a
22 growing number of professionals with the necessary
23 cybersecurity and information assurance expertise,
24 including individuals from States or regions in which
25 the unemployment rate exceeds the national average;

1 (4) an analysis of any barriers to the Federal
2 Government recruiting and hiring cybersecurity tal-
3 ent, including barriers relating to compensation, the
4 hiring process, job classification, and hiring flexibili-
5 ties; and

6 (5) recommendations for Federal policies to en-
7 sure an adequate, well-trained Federal cybersecurity
8 workforce.

9 **SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK**
10 **FORCE.**

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

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

21 (1) develop options for a collaborative model
22 and an organizational structure for such entity
23 under which the joint research and development ac-
24 tivities could be planned, managed, and conducted
25 effectively, including mechanisms for the allocation

1 of resources among the participants in such entity
2 for support of such activities;

3 (2) identify and prioritize at least three cyberse-
4 curity grand challenges, focused on nationally sig-
5 nificant problems requiring collaborative and inter-
6 disciplinary solutions;

7 (3) propose a process for developing a research
8 and development agenda for such entity to address
9 the grand challenges identified under paragraph (2);

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

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

16 (6) make recommendations for how such entity
17 could be funded from Federal, State, and nongovern-
18 mental sources.

19 (c) COMPOSITION.—In establishing the task force
20 under subsection (a), the Director of the Office of Science
21 and Technology Policy shall appoint an equal number of
22 individuals from institutions of higher education, including
23 minority-serving institutions and community colleges, and
24 from industry with knowledge and expertise in cybersecu-
25 rity.

1 (d) REPORT.—Not later than 12 months after the
2 date of enactment of this Act, the Director of the Office
3 of Science and Technology Policy shall transmit to the
4 Congress a report describing the findings and rec-
5 ommendations 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. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS**
12 **FOR GOVERNMENT SYSTEMS.**

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

16 “(c) SECURITY AUTOMATION AND CHECKLISTS FOR
17 GOVERNMENT SYSTEMS.—

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

1 to become, widely used within the Federal Govern-
2 ment in order to enable standardized and interoper-
3 able technologies, architectures, and frameworks for
4 continuous monitoring of information security within
5 the Federal Government.

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

11 “(A) the security risks associated with the
12 use of the system;

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

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

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

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

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

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

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

23 “(A) require any Federal agency to select
24 the specific settings or options recommended by

1 the standard, reference material, or checklist
2 for the system;

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

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

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

15 **SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
16 **NOLOGY CYBERSECURITY RESEARCH AND**
17 **DEVELOPMENT.**

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

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

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

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

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

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

16 “(5) carry out research associated with improv-
17 ing the security and integrity of the information
18 technology supply chain.”.

19 **SEC. 111. RESEARCH ON THE SCIENCE OF CYBERSECURITY.**

20 The Director of the National Science Foundation and
21 the Director of the National Institute of Standards and
22 Technology shall, through existing programs and activi-
23 ties, support research that will lead to the development
24 of a scientific foundation for the field of cybersecurity, in-
25 cluding research that increases understanding of the un-

1 derlying principles of securing complex networked sys-
2 tems, enables repeatable experimentation, and creates
3 quantifiable security metrics.

4 **TITLE II—ADVANCEMENT OF CY-**
5 **BERSECURITY TECHNICAL**
6 **STANDARDS**

7 **SEC. 201. DEFINITIONS.**

8 In this title:

9 (1) DIRECTOR.—The term “Director” means
10 the Director of the National Institute of Standards
11 and Technology.

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

14 **SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL**
15 **STANDARDS.**

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

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

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

1 (b) CONSULTATION WITH THE PRIVATE SECTOR.—
2 In carrying out the activities specified in subsection (a)(1),
3 the Director shall ensure consultation with appropriate
4 private sector stakeholders.

5 **SEC. 203. CLOUD COMPUTING STRATEGY.**

6 (a) IN GENERAL.—The Director, in collaboration
7 with the Federal CIO Council, and in consultation with
8 other relevant Federal agencies and stakeholders from the
9 private sector, shall continue to develop and encourage the
10 implementation of a comprehensive strategy for the use
11 and adoption of cloud computing services by the Federal
12 Government.

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

16 (1) accelerate the development, in collaboration
17 with the private sector, of standards that address
18 interoperability and portability of cloud computing
19 services;

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

23 (3) support, in consultation with the private
24 sector, the development of appropriate security
25 frameworks and reference materials, and the identi-

1 fication of best practices, for use by Federal agen-
2 cies to address security and privacy requirements to
3 enable the use and adoption of cloud computing
4 services, including activities—

5 (A) to ensure the physical security of cloud
6 computing data centers and the data stored in
7 such centers;

8 (B) to ensure secure access to the data
9 stored in cloud computing data centers;

10 (C) to develop security standards as re-
11 quired under section 20 of the National Insti-
12 tute of Standards and Technology Act (15
13 U.S.C. 278g-3); and

14 (D) to support the development of the au-
15 tomation of continuous monitoring systems.

16 **SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND**
17 **EDUCATION.**

18 (a) PROGRAM.—The Director, in collaboration with
19 relevant Federal agencies, industry, educational institu-
20 tions, National Laboratories, the National Coordination
21 Office of the Networking and Information Technology Re-
22 search and Development program, and other organiza-
23 tions, shall continue to coordinate a cybersecurity aware-
24 ness and education program to increase knowledge, skills,

1 and awareness of cybersecurity risks, consequences, and
2 best practices through—

3 (1) the widespread dissemination of cybersecu-
4 rity technical standards and best practices identified
5 by the Institute;

6 (2) efforts to make cybersecurity best practices
7 usable by individuals, small to medium-sized busi-
8 nesses, State, local, and tribal governments, and
9 educational institutions;

10 (3) improving the state of cybersecurity edu-
11 cation at all educational levels;

12 (4) efforts to attract, recruit, and retain quali-
13 fied professionals to the Federal cybersecurity work-
14 force; and

15 (5) improving the skills, training, and profes-
16 sional development of the Federal cybersecurity
17 workforce.

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 Act, and the amendments made by this Act. This Act, and

- 1 the amendments made by this Act, shall be carried out
- 2 using amounts otherwise authorized or appropriated.

Passed the House of Representatives April 16, 2013.

Attest:

KAREN L. HAAS,

Clerk.