

112TH CONGRESS
2^D SESSION

H. R. 2096

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 2012”.

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 lege-age population, members of these minorities
 2 comprise less than 20 percent of bachelor degree re-
 3 cipients in the field of computer sciences.”.

4 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
 5 **VELOPMENT PLAN.**

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

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

24 (1) specify and prioritize near-term, mid-term
 25 and long-term research objectives, including objec-

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; and

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.

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

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

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

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

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

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

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

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

17 **SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBER-**
18 **SECURITY.**

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

21 (1) by inserting “and usability” after “to the
22 structure”;

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

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

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

5 “(J) social and behavioral factors, includ-
6 ing human-computer interactions, usability, and
7 user motivations.”.

8 **SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECU-**
9 **RITY RESEARCH AND DEVELOPMENT PRO-**
10 **GRAMS.**

11 (a) **COMPUTER AND NETWORK SECURITY RESEARCH**
12 **AREAS.**—Section 4(a)(1) of the Cyber Security Research
13 and Development Act (15 U.S.C. 7403(a)(1)) is amend-
14 ed—

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

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

20 (b) **COMPUTER AND NETWORK SECURITY RESEARCH**
21 **GRANTS.**—Section 4(a)(3) of such Act (15 U.S.C.
22 7403(a)(3)) is amended by striking subparagraphs (A)
23 through (E) and inserting the following new subpara-
24 graphs:

25 “(A) \$90,000,000 for fiscal year 2013;

1 “(B) \$90,000,000 for fiscal year 2014; and

2 “(C) \$90,000,000 for fiscal year 2015.”.

3 (c) COMPUTER AND NETWORK SECURITY RESEARCH

4 CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b))

5 is amended—

6 (1) in paragraph (4)—

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

8 “and” after the semicolon;

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

11 (C) by adding at the end the following new
12 subparagraph:

13 “(E) how the center will partner with gov-
14 ernment laboratories, for-profit entities, other
15 institutions of higher education, or nonprofit re-
16 search institutions.”; and

17 (2) in paragraph (7) by striking subparagraphs

18 (A) through (E) and inserting the following new
19 subparagraphs:

20 “(A) \$4,500,000 for fiscal year 2013;

21 “(B) \$4,500,000 for fiscal year 2014; and

22 “(C) \$4,500,000 for fiscal year 2015.”.

23 (d) COMPUTER AND NETWORK SECURITY CAPACITY

24 BUILDING GRANTS.—Section 5(a)(6) of such Act (15

25 U.S.C. 7404(a)(6)) is amended by striking subparagraphs

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

3 “(A) \$19,000,000 for fiscal year 2013;

4 “(B) \$19,000,000 for fiscal year 2014; and

5 “(C) \$19,000,000 for fiscal year 2015.”.

6 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
7 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
8 7404(b)(2)) is amended by striking subparagraphs (A)
9 through (E) and inserting the following new subpara-
10 graphs:

11 “(A) \$2,500,000 for fiscal year 2013;

12 “(B) \$2,500,000 for fiscal year 2014; and

13 “(C) \$2,500,000 for fiscal year 2015.”.

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

19 “(A) \$24,000,000 for fiscal year 2013;

20 “(B) \$24,000,000 for fiscal year 2014; and

21 “(C) \$24,000,000 for fiscal year 2015.”.

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

1 **SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE**
2 **PROGRAM.**

3 (a) IN GENERAL.—The Director of the National
4 Science Foundation shall continue a Scholarship for Serv-
5 ice program under section 5(a) of the Cyber Security Re-
6 search and Development Act (15 U.S.C. 7404(a)) to re-
7 cruit and train the next generation of Federal cybersecu-
8 rity professionals and to increase the capacity of the high-
9 er education system to produce an information technology
10 workforce with the skills necessary to enhance the security
11 of the Nation’s communications and information infra-
12 structure.

13 (b) CHARACTERISTICS OF PROGRAM.—The program
14 under this section shall—

15 (1) provide, through qualified institutions of
16 higher education, scholarships that provide tuition,
17 fees, and a competitive stipend for up to 2 years to
18 students pursuing a bachelor’s or master’s degree and
19 up to 3 years to students pursuing a doctoral degree
20 in a cybersecurity field;

21 (2) provide the scholarship recipients with sum-
22 mer internship opportunities or other meaningful
23 temporary appointments in the Federal information
24 technology workforce; and

25 (3) increase the capacity of institutions of high-
26 er education throughout all regions of the United

1 States to produce highly qualified cybersecurity pro-
2 fessionals, through the award of competitive, merit-
3 reviewed grants that support such activities as—

4 (A) faculty professional development, in-
5 cluding technical, hands-on experiences in the
6 private sector or government, workshops, semi-
7 nars, conferences, and other professional devel-
8 opment opportunities that will result in im-
9 proved instructional capabilities;

10 (B) institutional partnerships, including
11 minority serving institutions and community
12 colleges; and

13 (C) development of cybersecurity-related
14 courses and curricula.

15 (c) SCHOLARSHIP REQUIREMENTS.—

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

18 (A) are citizens or permanent residents of
19 the United States;

20 (B) are full-time students in an eligible de-
21 gree program, as determined by the Director,
22 that is focused on computer security or infor-
23 mation assurance at an awardee institution;
24 and

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

3 (2) SELECTION.—Individuals shall be selected
4 to receive scholarships primarily on the basis of aca-
5 demic merit, with consideration given to financial
6 need, to the goal of promoting the participation of
7 individuals identified in section 33 or 34 of the
8 Science and Engineering Equal Opportunities Act
9 (42 U.S.C. 1885a or 1885b), and to veterans. For
10 purposes of this paragraph, the term “veteran”
11 means a person who—

12 (A) served on active duty (other than ac-
13 tive duty for training) in the Armed Forces of
14 the United States for a period of more than
15 180 consecutive days, and who was discharged
16 or released therefrom under conditions other
17 than dishonorable; or

18 (B) served on active duty (other than ac-
19 tive duty for training) in the Armed Forces of
20 the United States and was discharged or re-
21 leased from such service for a service-connected
22 disability before serving 180 consecutive days.

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

1 (3) SERVICE OBLIGATION.—If an individual re-
2 ceives a scholarship under this section, as a condi-
3 tion of receiving such scholarship, the individual
4 upon completion of their degree must serve as a cy-
5 bersecurity professional within the Federal workforce
6 for a period of time as provided in paragraph (5).
7 If a scholarship recipient is not offered employment
8 by a Federal agency or a federally funded research
9 and development center, the service requirement can
10 be satisfied at the Director’s discretion by—

11 (A) serving as a cybersecurity professional
12 in a State, local, or tribal government agency;
13 or

14 (B) teaching cybersecurity courses at an
15 institution of higher education.

16 (4) CONDITIONS OF SUPPORT.—As a condition
17 of acceptance of a scholarship under this section, a
18 recipient shall agree to provide the awardee institu-
19 tion with annual verifiable documentation of employ-
20 ment and up-to-date contact information.

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

1 (d) FAILURE TO COMPLETE SERVICE OBLIGA-
2 TION.—

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

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

9 (B) is dismissed from such educational in-
10 stitution for disciplinary reasons;

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

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

17 (E) fails to fulfill the service obligation of
18 the individual under this section,

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

21 (2) MONITORING COMPLIANCE.—As a condition
22 of participating in the program, a qualified institu-
23 tion of higher education receiving a grant under this
24 section shall—

1 (A) enter into an agreement with the Di-
2 rector of the National Science Foundation to
3 monitor the compliance of scholarship recipients
4 with respect to their service obligation; and

5 (B) provide to the Director, on an annual
6 basis, post-award employment information re-
7 quired under subsection (e)(4) for scholarship
8 recipients through the completion of their serv-
9 ice obligation.

10 (3) AMOUNT OF REPAYMENT.—

11 (A) LESS THAN ONE YEAR OF SERVICE.—

12 If a circumstance described in paragraph (1)
13 occurs before the completion of 1 year of a
14 service obligation under this section, the total
15 amount of awards received by the individual
16 under this section shall be repaid or such
17 amount shall be treated as a loan to be repaid
18 in accordance with subparagraph (C).

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

20 If a circumstance described in subparagraph
21 (D) or (E) of paragraph (1) occurs after the
22 completion of 1 year of a service obligation
23 under this section, the total amount of scholar-
24 ship awards received by the individual under
25 this section, reduced by the ratio of the number

1 of years of service completed divided by the
2 number of years of service required, shall be re-
3 paid or such amount shall be treated as a loan
4 to be repaid in accordance with subparagraph
5 (C).

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

18 (4) COLLECTION OF REPAYMENT.—

19 (A) IN GENERAL.—In the event that a
20 scholarship recipient is required to repay the
21 scholarship under this subsection, the institu-
22 tion providing the scholarship shall—

23 (i) be responsible for determining the
24 repayment amounts and for notifying the

1 recipient and the Director of the amount
2 owed; and

3 (ii) collect such repayment amount
4 within a period of time as determined
5 under the agreement described in para-
6 graph (2), or the repayment amount shall
7 be treated as a loan in accordance with
8 paragraph (3)(C).

9 (B) RETURNED TO TREASURY.—Except as
10 provided in subparagraph (C) of this para-
11 graph, any such repayment shall be returned to
12 the Treasury of the United States.

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

20 (5) EXCEPTIONS.—The Director may provide
21 for the partial or total waiver or suspension of any
22 service or payment obligation by an individual under
23 this section whenever compliance by the individual
24 with the obligation is impossible or would involve ex-
25 treme hardship to the individual, or if enforcement

1 of such obligation with respect to the individual
2 would be unconscionable.

3 (e) **HIRING AUTHORITY.**—For purposes of any law
4 or regulation governing the appointment of individuals in
5 the Federal civil service, upon successful completion of
6 their degree, students receiving a scholarship under this
7 section shall be hired under the authority provided for in
8 section 213.3102(r) of title 5, Code of Federal Regula-
9 tions, and be exempted from competitive service. Upon ful-
10 fillment of the service term, such individuals shall be con-
11 verted to a competitive service position without competi-
12 tion if the individual meets the requirements for that posi-
13 tion.

14 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

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

19 (1) an examination of the current state of and
20 the projected needs of the Federal cybersecurity
21 workforce, including a comparison of the different
22 agencies and departments, and an analysis of the ca-
23 pacity of such agencies and departments to meet
24 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) propose a process for developing a research
4 and development agenda for such entity, including
5 guidelines to ensure an appropriate scope of work fo-
6 cused on nationally significant challenges and requir-
7 ing collaboration;

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

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

14 (5) make recommendations for how such entity
15 could be funded from Federal, State, and nongovern-
16 mental sources.

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

24 (d) REPORT.—Not later than 12 months after the
25 date of enactment of this Act, the Director of the Office

1 of Science and Technology Policy shall transmit to the
2 Congress a report describing the findings and rec-
3 ommendations of the task force.

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

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

9 **SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS**
10 **FOR GOVERNMENT SYSTEMS.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23 “(1) conduct a research program to develop a
24 unifying and standardized identity, privilege, and ac-
25 cess control management framework for the execu-

1 tion of a wide variety of resource protection policies
2 and that is amenable to implementation within a
3 wide variety of existing and emerging computing en-
4 vironments;

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

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

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

13 **TITLE II—ADVANCEMENT OF CY-**
14 **BERSECURITY TECHNICAL**
15 **STANDARDS**

16 **SEC. 201. DEFINITIONS.**

17 In this title:

18 (1) **DIRECTOR.**—The term “Director” means
19 the Director of the National Institute of Standards
20 and Technology.

21 (2) **INSTITUTE.**—The term “Institute” means
22 the National Institute of Standards and Technology.

1 **SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL**
2 **STANDARDS.**

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

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

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

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

17 **SEC. 203. CLOUD COMPUTING STRATEGY.**

18 (a) IN GENERAL.—The Director, in collaboration
19 with the Federal CIO Council, and in consultation with
20 other relevant Federal agencies and stakeholders from the
21 private sector, shall continue to develop and encourage the
22 implementation of a comprehensive strategy for the use
23 and adoption of cloud computing services by the Federal
24 Government.

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

4 (1) accelerate the development, in collaboration
5 with the private sector, of standards that address
6 interoperability and portability of cloud computing
7 services;

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

11 (3) support, in consultation with the private
12 sector, the development of appropriate security
13 frameworks and reference materials, and the identi-
14 fication of best practices, for use by Federal agen-
15 cies to address security and privacy requirements to
16 enable the use and adoption of cloud computing
17 services, including activities—

18 (A) to ensure the physical security of cloud
19 computing data centers and the data stored in
20 such centers;

21 (B) to ensure secure access to the data
22 stored in cloud computing data centers;

23 (C) to develop security standards as re-
24 quired under section 20 of the National Insti-

1 tute of Standards and Technology Act (15
2 U.S.C. 278g-3); and

3 (D) to support the development of the au-
4 tomation of continuous monitoring systems.

5 **SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND**
6 **EDUCATION.**

7 (a) PROGRAM.—The Director, in collaboration with
8 relevant Federal agencies, industry, educational institu-
9 tions, National Laboratories, the National Coordination
10 Office of the Networking and Information Technology Re-
11 search and Development program, and other organiza-
12 tions, shall continue to coordinate a cybersecurity aware-
13 ness and education program to increase knowledge, skills,
14 and awareness of cybersecurity risks, consequences, and
15 best practices through—

16 (1) the widespread dissemination of cybersecu-
17 rity technical standards and best practices identified
18 by the Institute;

19 (2) efforts to make cybersecurity best practices
20 usable by individuals, small to medium-sized busi-
21 nesses, State, local, and tribal governments, and
22 educational institutions; and

23 (3) efforts to attract, recruit, and retain quali-
24 fied professionals to the Federal cybersecurity work-
25 force.

1 (b) STRATEGIC PLAN.—The Director shall, in co-
2 operation with relevant Federal agencies and other stake-
3 holders, develop and implement a strategic plan to guide
4 Federal programs and activities in support of a com-
5 prehensive cybersecurity awareness and education pro-
6 gram as described under subsection (a).

7 (c) REPORT TO CONGRESS.—Not later than 1 year
8 after the date of enactment of this Act and every 5 years
9 thereafter, the Director shall transmit the strategic plan
10 required under subsection (b) to the Committee on
11 Science, Space, and Technology of the House of Rep-
12 resentatives and the Committee on Commerce, Science,
13 and Transportation of the Senate.

14 **SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
15 **OPMENT.**

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

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

22 (2) strengthen authentication methods of iden-
23 tity management systems;

24 (3) improve privacy protection in identity man-
25 agement systems, including health information tech-

1 nology systems, through authentication and security
2 protocols; and

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

5 **SEC. 206. AUTHORIZATIONS.**

6 No additional funds are authorized to carry out this
7 title and the amendments made by this title or to carry
8 out the amendments made by sections 109 and 110 of this
9 Act. This title and the amendments made by this title and
10 the amendments made by sections 109 and 110 of this
11 Act shall be carried out using amounts otherwise author-
12 ized or appropriated.

Passed the House of Representatives April 27, 2012.

Attest:

Clerk.

112TH CONGRESS
2^D SESSION

H. R. 2096

AN ACT

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