

Union Calendar No. 177

112TH CONGRESS
1ST SESSION

H. R. 2096

[Report No. 112-264]

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 2, 2011

Mr. McCAUL (for himself and Mr. LIPINSKI) introduced the following bill;
which was referred to the Committee on Science, Space, and Technology

OCTOBER 31, 2011

Additional sponsors: Mr. WU, Mr. HALL, Mr. SCHOCK, Mr. LUJÁN, Mr.
SMITH of Texas, and Mr. BROOKS

OCTOBER 31, 2011

Reported with an amendment, committed to the Committee of the Whole
House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on June 2, 2011]

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 Enhance-*
5 *ment Act of 2011”.*

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

8 **SEC. 101. DEFINITIONS.**

9 *In this title:*

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

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

19 **SEC. 102. FINDINGS.**

20 *Section 2 of the Cyber Security Research and Develop-*
21 *ment Act (15 U.S.C. 7401) is amended—*

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

24 “(1) *Advancements in information and commu-*
25 *nications technology have resulted in a globally inter-*

1 *connected network of government, commercial, sci-*
2 *entific, and education infrastructures, including crit-*
3 *ical infrastructures for electric power, natural gas*
4 *and petroleum production and distribution, tele-*
5 *communications, transportation, water supply, bank-*
6 *ing and finance, and emergency and government serv-*
7 *ices.”;*

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

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

15 “(3) *The Cyberspace Policy Review published by*
16 *the President in May, 2009, concluded that our infor-*
17 *mation technology and communications infrastruc-*
18 *ture is vulnerable and has ‘suffered intrusions that*
19 *have allowed criminals to steal hundreds of millions*
20 *of dollars and nation-states and other entities to steal*
21 *intellectual property and sensitive military informa-*
22 *tion’.”; and*

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

1 “(6) *While African-Americans, Hispanics, and*
2 *Native Americans constitute 33 percent of the college-*
3 *age population, members of these minorities comprise*
4 *less than 20 percent of bachelor degree recipients in*
5 *the field of computer sciences.”.*

6 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
7 **VELOPMENT PLAN.**

8 (a) *IN GENERAL.*—*Not later than 12 months after the*
9 *date of enactment of this Act, the agencies identified in sub-*
10 *section 101(a)(3)(B)(i) through (x) of the High-Performance*
11 *Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i)*
12 *through (x)) or designated under section 101(a)(3)(B)(xi)*
13 *of such Act, working through the National Science and*
14 *Technology Council and with the assistance of the National*
15 *Coordination Office, shall transmit to Congress a strategic*
16 *plan based on an assessment of cybersecurity risk to guide*
17 *the overall direction of Federal cybersecurity and informa-*
18 *tion assurance research and development for information*
19 *technology and networking systems. Once every 3 years*
20 *after the initial strategic plan is transmitted to Congress*
21 *under this section, such agencies shall prepare and transmit*
22 *to Congress an update of such plan.*

23 (b) *CONTENTS OF PLAN.*—*The strategic plan required*
24 *under subsection (a) shall—*

1 (1) *specify and prioritize near-term, mid-term*
2 *and long-term research objectives, including objectives*
3 *associated with the research areas identified in sec-*
4 *tion 4(a)(1) of the Cyber Security Research and De-*
5 *velopment Act (15 U.S.C. 7403(a)(1)) and how the*
6 *near-term objectives complement research and develop-*
7 *ment areas in which the private sector is actively en-*
8 *gaged;*

9 (2) *describe how the Program will focus on inno-*
10 *vative, transformational technologies with the poten-*
11 *tial to enhance the security, reliability, resilience, and*
12 *trustworthiness of the digital infrastructure, and to*
13 *protect consumer privacy;*

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

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

1 (5) describe how the Program will facilitate ac-
2 cess by academic researchers to the infrastructure de-
3 scribed in paragraph (4), as well as to relevant data,
4 including event data; and

5 (6) describe how the Program will engage females
6 and individuals identified in section 33 or 34 of the
7 Science and Engineering Equal Opportunities Act
8 (42 U.S.C. 1885a or 1885b) to foster a more diverse
9 workforce in this area.

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

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

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

22 (3) estimate the funding required for each major
23 research objective of the strategic plan for the fol-
24 lowing 3 fiscal years.

1 (d) *RECOMMENDATIONS.*—*In developing and updating*
2 *the strategic plan under subsection (a), the agencies in-*
3 *volved shall solicit recommendations and advice from—*

4 (1) *the advisory committee established under sec-*
5 *tion 101(b)(1) of the High-Performance Computing*
6 *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 minor-*
9 *ity serving institutions and community colleges, Na-*
10 *tional Laboratories, and other relevant organizations*
11 *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 section*
15 *101(a)(2)(D) of the High-Performance Computing Act of*
16 *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, including
6 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 amended—

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

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

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

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

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

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

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

5 (1) *in paragraph (4)—*

6 (A) *in subparagraph (C), by striking “and”*
7 *after the semicolon;*

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

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

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

16 (2) *in paragraph (7) by striking subparagraphs*
17 *(A) through (E) and inserting the following new sub-*
18 *paragraphs:*

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

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

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

22 (d) *COMPUTER AND NETWORK SECURITY CAPACITY*
23 *BUILDING GRANTS.*—Section 5(a)(6) of such Act (15 U.S.C.
24 *7404(a)(6)) is amended by striking subparagraphs (A)*

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

3 “(A) \$19,000,000 for fiscal year 2012;
4 “(B) \$19,000,000 for fiscal year 2013; and
5 “(C) \$19,000,000 for fiscal year 2014.”.

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 2012;
12 “(B) \$2,500,000 for fiscal year 2013; and
13 “(C) \$2,500,000 for fiscal year 2014.”.

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

19 “(A) \$24,000,000 for fiscal year 2012;
20 “(B) \$24,000,000 for fiscal year 2013; and
21 “(C) \$24,000,000 for fiscal year 2014.”.

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 recruit*
7 *and train the next generation of Federal cybersecurity pro-*
8 *fessionals and to increase the capacity of the higher edu-*
9 *cation system to produce an information technology work-*
10 *force with the skills necessary to enhance the security of the*
11 *Nation’s communications and information infrastructure.*

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

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

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

24 (3) *increase the capacity of institutions of higher*
25 *education throughout all regions of the United States*
26 *to produce highly qualified cybersecurity profes-*

1 *sionals, through the award of competitive, merit-re-*
2 *viewed grants that support such activities as—*

3 *(A) faculty professional development, in-*
4 *cluding technical, hands-on experiences in the*
5 *private sector or government, workshops, semi-*
6 *nars, conferences, and other professional develop-*
7 *ment opportunities that will result in improved*
8 *instructional capabilities;*

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

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

14 *(c) SCHOLARSHIP REQUIREMENTS.—*

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

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

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

23 *(C) accept the terms of a scholarship pursu-*
24 *ant to this section.*

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

10 (A) *served on active duty (other than active*
11 *duty for training) in the Armed Forces of the*
12 *United States for a period of more than 180 con-*
13 *secutive days, and who was discharged or re-*
14 *leased therefrom under conditions other than dis-*
15 *honorable; or*

16 (B) *served on active duty (other than active*
17 *duty for training) in the Armed Forces of the*
18 *United States and was discharged or released*
19 *from such service for a service-connected dis-*
20 *ability before serving 180 consecutive days.*

21 *For purposes of subparagraph (B), the term “service-*
22 *connected” has the meaning given such term under*
23 *section 101 of title 38, United States Code.*

24 (3) *SERVICE OBLIGATION.*—*If an individual re-*
25 *ceives a scholarship under this section, as a condition*

1 of receiving such scholarship, the individual upon
2 completion of their degree must serve as a cybersecu-
3 rity professional within the Federal workforce for a
4 period of time as provided in paragraph (5). If a
5 scholarship recipient is not offered employment by a
6 Federal agency or a federally funded research and de-
7 velopment center, the service requirement can be satis-
8 fied at the Director's discretion by—

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

11 (B) teaching cybersecurity courses at an in-
12 stitution of higher education.

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

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

22 (d) *FAILURE TO COMPLETE SERVICE OBLIGATION.*—

23 (1) *GENERAL RULE.*—If an individual who has
24 received a scholarship under this section—

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

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

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

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

13 (E) fails to fulfill the service obligation of
14 the individual under this section,
15 such individual shall be liable to the United States as
16 provided in paragraph (3).

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

21 (A) enter into an agreement with the Direc-
22 tor of the National Science Foundation to mon-
23 itor the compliance of scholarship recipients with
24 respect to their service obligation; and

1 (B) provide to the Director, on an annual
2 basis, post-award employment information re-
3 quired under subsection (c)(4) for scholarship re-
4 cipients through the completion of their service
5 obligation.

6 (3) AMOUNT OF REPAYMENT.—

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

15 (B) MORE THAN ONE YEAR OF SERVICE.—
16 If a circumstance described in subparagraph (D)
17 or (E) of paragraph (1) occurs after the comple-
18 tion of 1 year of a service obligation under this
19 section, the total amount of scholarship awards
20 received by the individual under this section, re-
21 duced by the ratio of the number of years of serv-
22 ice completed divided by the number of years of
23 service required, shall be repaid or such amount
24 shall be treated as a loan to be repaid in accord-
25 ance with subparagraph (C).

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

12 (4) *COLLECTION OF REPAYMENT.*—

13 (A) *IN GENERAL.*—In the event that a schol-
14 arship recipient is required to repay the scholar-
15 ship under this subsection, the institution pro-
16 viding the scholarship shall—

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

21 (ii) collect such repayment amount
22 within a period of time as determined
23 under the agreement described in paragraph
24 (2), or the repayment amount shall be treat-

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

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

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

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

22 *(e) HIRING AUTHORITY.—For purposes of any law or*
23 *regulation governing the appointment of individuals in the*
24 *Federal civil service, upon successful completion of their de-*
25 *gree, students receiving a scholarship under this section*

1 *shall be hired under the authority provided for in section*
2 *213.3102(r) of title 5, Code of Federal Regulations, and be*
3 *exempted from competitive service. Upon fulfillment of the*
4 *service term, such individuals shall be converted to a com-*
5 *petitive service position without competition if the indi-*
6 *vidual meets the requirements for that position.*

7 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

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

12 *(1) an examination of the current state of and*
13 *the projected needs of the Federal cybersecurity work-*
14 *force, including a comparison of the different agencies*
15 *and departments, and an analysis of the capacity of*
16 *such agencies and departments to meet those needs;*

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

1 *local entities, and the private sector, and a descrip-*
2 *tion of how successful programs are engaging the tal-*
3 *ents of females and individuals identified in section*
4 *33 or 34 of the Science and Engineering Equal Op-*
5 *portunities Act (42 U.S.C. 1885a or 1885b);*

6 *(3) an examination of the effectiveness of the Na-*
7 *tional Centers of Academic Excellence in Information*
8 *Assurance Education, the Centers of Academic Excel-*
9 *lence in Research, and the Federal Cyber Scholarship*
10 *for Service programs in promoting higher education*
11 *and research in cybersecurity and information assur-*
12 *ance and in producing a growing number of profes-*
13 *sionals with the necessary cybersecurity and informa-*
14 *tion assurance expertise, including individuals from*
15 *States or regions in which the unemployment rate ex-*
16 *ceeds the national average;*

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

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

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

3 (a) *ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK*
4 *FORCE.*—Not later than 180 days after the date of enact-
5 ment of this Act, the Director of the Office of Science and
6 Technology Policy shall convene a task force to explore
7 mechanisms for carrying out collaborative research, devel-
8 opment, education, and training activities for cybersecurity
9 through a consortium or other appropriate entity with par-
10 ticipants from institutions of higher education and indus-
11 try.

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

13 (1) *develop options for a collaborative model and*
14 *an organizational structure for such entity under*
15 *which the joint research and development activities*
16 *could be planned, managed, and conducted effectively,*
17 *including mechanisms for the allocation of resources*
18 *among the participants in such entity for support of*
19 *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, for the transfer of research and devel-*
6 *opment 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 date*
18 *of enactment of this Act, the Director of the Office of Science*
19 *and Technology Policy shall transmit to the Congress a re-*
20 *port describing the findings and recommendations of the*
21 *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 the*
2 *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 Devel-*
6 *opment Act (15 U.S.C. 7406(c)) is amended to read as fol-*
7 *lows:*

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

10 “(1) *IN GENERAL.*—*The Director of the National*
11 *Institute of Standards and Technology shall develop,*
12 *and revise as necessary, security automation stand-*
13 *ards, associated reference materials (including proto-*
14 *cols), and checklists providing settings and option se-*
15 *lections that minimize the security risks associated*
16 *with each information technology hardware or soft-*
17 *ware system and security tool that is, or is likely to*
18 *become, widely used within the Federal Government*
19 *in order to enable standardized and interoperable*
20 *technologies, architectures, and frameworks for contin-*
21 *uous monitoring of information security within the*
22 *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 checklists*
2 *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 par-*
6 *ticular system or security tool;*

7 *“(C) the usefulness of the standards, ref-*
8 *erence materials, or checklists to Federal agencies*
9 *that are users or potential users of the system;*

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

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

17 *“(3) EXCLUDED SYSTEMS.—The Director of the*
18 *National Institute of Standards and Technology may*
19 *exclude from the application of paragraph (1) any in-*
20 *formation technology hardware or software system or*
21 *security tool for which such Director determines that*
22 *the development of a standard, reference material, or*
23 *checklist is inappropriate because of the infrequency*
24 *of use of the system, the obsolescence of the system, or*
25 *the inutility or impracticability of developing a*

1 *standard, reference material, or checklist for the sys-*
2 *tem.*

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

9 “(5) *AGENCY USE REQUIREMENTS.—The develop-*
10 *ment of standards, reference materials, and checklists*
11 *under paragraph (1) for an information technology*
12 *hardware or software system or tool does not—*

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

17 “(B) *establish conditions or prerequisites for*
18 *Federal agency procurement or deployment of*
19 *any such system;*

20 “(C) *imply an endorsement of any such sys-*
21 *tem by the Director of the National Institute of*
22 *Standards and Technology; or*

23 “(D) *preclude any Federal agency from pro-*
24 *curing or deploying other information technology*
25 *hardware or software systems for which no such*

1 *standard, reference material, or checklist has*
2 *been developed or identified under paragraph*
3 *(1).”.*

4 **SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
5 **NOLOGY CYBERSECURITY RESEARCH AND DE-**
6 **VELOPMENT.**

7 *Section 20 of the National Institute of Standards and*
8 *Technology Act (15 U.S.C. 278g–3) is amended by redesi-*
9 *gnating subsection (e) as subsection (f), and by inserting*
10 *after subsection (d) the following:*

11 “(e) *INTRAMURAL SECURITY RESEARCH.*—*As part of*
12 *the research activities conducted in accordance with sub-*
13 *section (d)(3), the Institute shall—*

14 “(1) *conduct a research program to develop a*
15 *unifying and standardized identity, privilege, and ac-*
16 *cess control management framework for the execution*
17 *of a wide variety of resource protection policies and*
18 *that is amenable to implementation within a wide*
19 *variety of existing and emerging computing environ-*
20 *ments;*

21 “(2) *carry out research associated with improv-*
22 *ing the security of information systems and networks;*

23 “(3) *carry out research associated with improv-*
24 *ing the testing, measurement, usability, and assur-*
25 *ance of information systems and networks; and*

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

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

6 **SEC. 201. DEFINITIONS.**

7 *In this title:*

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

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

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

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

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

21 (2) *not later than 1 year after the date of enact-*
22 *ment of this Act, develop and transmit to the Con-*
23 *gress a plan for ensuring such Federal agency coordi-*
24 *nation.*

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

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

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

12 **(b) ACTIVITIES.**—In carrying out the strategy devel-
13 oped under subsection (a), the Director shall give consider-
14 ation to activities that—

15 (1) accelerate the development of standards that
16 address interoperability and portability of cloud com-
17 puting services;

18 (2) support the development of conformance test
19 systems; and

20 (3) address appropriate security frameworks and
21 reference materials for use by Federal agencies to ad-
22 dress their security and privacy requirements, includ-
23 ing—

1 (A) *the physical security of cloud computing*
2 *data centers and the data stored in such centers;*
3 *and*

4 (B) *accessibility of the data stored in cloud*
5 *computing data centers.*

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

8 (a) *PROGRAM.*—*The Director, in collaboration with*
9 *relevant Federal agencies, industry, educational institu-*
10 *tions, National Laboratories, and other organizations, shall*
11 *continue to coordinate a cybersecurity awareness and edu-*
12 *cation program to increase knowledge, skills, and awareness*
13 *of cybersecurity risks, consequences, and best practices*
14 *through—*

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

18 (2) *efforts to make cybersecurity technical stand-*
19 *ards and best practices usable by individuals, small*
20 *to medium-sized businesses, State, local, and tribal*
21 *governments, and educational institutions.*

22 (b) *STRATEGIC PLAN.*—*The Director shall, in coopera-*
23 *tion with relevant Federal agencies and other stakeholders,*
24 *develop and implement a strategic plan to guide Federal*
25 *programs and activities in support of a comprehensive cy-*

1 *bersecurity awareness and education program as described*
2 *under subsection (a).*

3 (c) *REPORT TO CONGRESS.*—*Not later than 1 year*
4 *after the date of enactment of this Act and every 5 years*
5 *thereafter, the Director shall transmit the strategic plan re-*
6 *quired under subsection (b) to the Committee on Science,*
7 *Space, and Technology of the House of Representatives and*
8 *the Committee on Commerce, Science, and Transportation*
9 *of the Senate.*

10 **SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
11 **OPMENT.**

12 *The Director shall continue a program to support the*
13 *development of technical standards, metrology, testbeds, and*
14 *conformance criteria, taking into account appropriate user*
15 *concerns, to—*

16 (1) *improve interoperability among identity*
17 *management technologies;*

18 (2) *strengthen authentication methods of identity*
19 *management systems;*

20 (3) *improve privacy protection in identity man-*
21 *agement systems, including health information tech-*
22 *nology systems, through authentication and security*
23 *protocols; and*

24 (4) *improve the usability of identity manage-*
25 *ment systems.*

1 **SEC. 206. AUTHORIZATIONS.**

2 *No additional funds are authorized to carry out this*
3 *title and the amendments made by this title or to carry*
4 *out the amendments made by sections 109 and 110 of this*
5 *Act. This title and the amendments made by this title and*
6 *the amendments made by sections 109 and 110 of this Act*
7 *shall be carried out using amounts otherwise authorized or*
8 *appropriated.*

Union Calendar No. 177

112TH CONGRESS
1ST Session

H. R. 2096

[Report No. 112-264]

A BILL

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

OCTOBER 31, 2011

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed