

Union Calendar No. 236

111TH CONGRESS
2^D SESSION

H. R. 4061

[Report No. 111-405]

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

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 7, 2009

Mr. LIPINSKI (for himself, Mr. McCAUL, Mr. WU, Mr. EHLERS, Ms. EDDIE BERNICE JOHNSON of Texas, Mr. SMITH of Nebraska, Mr. GORDON of Tennessee, Mr. HALL of Texas, Mr. LUJÁN, and Mr. ROTHMAN of New Jersey) introduced the following bill; which was referred to the Committee on Science and Technology

JANUARY 27, 2010

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 November 7, 2009]

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 2009”.*

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’.”;*

23 (4) *by redesignating paragraphs (4) through (6)*
24 *as paragraphs (5) through (7), respectively;*

1 (5) by inserting after paragraph (3) the fol-
2 lowing new paragraph:

3 “(4) In a series of hearings held before Congress
4 in 2009, experts testified that the Federal cybersecu-
5 rity research and development portfolio was too fo-
6 cused on short-term, incremental research and that it
7 lacked the prioritization and coordination necessary
8 to address the long-term challenge of ensuring a se-
9 cure and reliable information technology and commu-
10 nications infrastructure.”; and

11 (6) by amending paragraph (7), as so redesign-
12 ated by paragraph (4) of this section, to read as fol-
13 lows:

14 “(7) While African-Americans, Hispanics, and
15 Native Americans constitute 33 percent of the college-
16 age population, members of these minorities comprise
17 less than 20 percent of bachelor degree recipients in
18 the field of computer sciences.”.

19 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
20 **VELOPMENT PLAN.**

21 (a) *IN GENERAL.*—Not later than 12 months after the
22 date of enactment of this Act, the agencies identified in sub-
23 section 101(a)(3)(B)(i) through (x) of the High-Performance
24 Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i)
25 through (x)) or designated under section 101(a)(3)(B)(xi)

1 *of such Act, working through the National Science and*
2 *Technology Council and with the assistance of the National*
3 *Coordination Office, shall transmit to Congress a strategic*
4 *plan based on an assessment of cybersecurity risk to guide*
5 *the overall direction of Federal cybersecurity and informa-*
6 *tion assurance research and development for information*
7 *technology and networking systems. Once every 3 years*
8 *after the initial strategic plan is transmitted to Congress*
9 *under this section, such agencies shall prepare and transmit*
10 *to Congress an update of such plan.*

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

13 *(1) specify and prioritize near-term, mid-term*
14 *and long-term research objectives, including objectives*
15 *associated with the research areas identified in sec-*
16 *tion 4(a)(1) of the Cyber Security Research and De-*
17 *velopment Act (15 U.S.C. 7403(a)(1)) and how the*
18 *near-term objectives complement research and develop-*
19 *ment areas in which the private sector is actively en-*
20 *gaged;*

21 *(2) describe how the Program will focus on inno-*
22 *vative, transformational technologies with the poten-*
23 *tial to enhance the security, reliability, resilience, and*
24 *trustworthiness of the digital infrastructure;*

1 (3) describe how the Program will foster the
2 transfer of research and development results into new
3 cybersecurity technologies and applications for the
4 benefit of society and the national interest, including
5 through the dissemination of best practices and other
6 outreach activities;

7 (4) describe how the Program will establish and
8 maintain a national research infrastructure for cre-
9 ating, testing, and evaluating the next generation of
10 secure networking and information technology sys-
11 tems;

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

16 (6) describe how the Program will engage females
17 and individuals identified in section 33 or 34 of the
18 Science and Engineering Equal Opportunities Act
19 (42 U.S.C. 1885a or 1885b) to foster a more diverse
20 workforce in this area.

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

1 (1) *specify the role of each Federal agency in*
2 *carrying out or sponsoring research and development*
3 *to meet the research objectives of the strategic plan,*
4 *including a description of how progress toward the re-*
5 *search objectives will be evaluated;*

6 (2) *specify the funding allocated to each major*
7 *research objective of the strategic plan and the source*
8 *of funding by agency for the current fiscal year; and*

9 (3) *estimate the funding required for each major*
10 *research objective of the strategic plan for the fol-*
11 *lowing 3 fiscal years.*

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

15 (1) *the advisory committee established under sec-*
16 *tion 101(b)(1) of the High-Performance Computing*
17 *Act of 1991 (15 U.S.C. 5511(b)(1)); and*

18 (2) *a wide range of stakeholders, including in-*
19 *dustry, academia, including representatives of minor-*
20 *ity serving institutions, and other relevant organiza-*
21 *tions and institutions.*

22 (e) *APPENDING TO REPORT.—The implementation*
23 *roadmap required under subsection (c), and its annual up-*
24 *dates, shall be appended to the report required under section*

1 101(a)(2)(D) of the High-Performance Computing Act of
2 1991 (15 U.S.C. 5511(a)(2)(D)).

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, including
16 human-computer interactions, usability, user
17 motivations, and organizational cultures.”.

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 amended
24 in subparagraph (A) by inserting “identity management,”
25 after “cryptography,”.

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

6 “(A) \$68,700,000 for fiscal year 2010;

7 “(B) \$73,500,000 for fiscal year 2011;

8 “(C) \$78,600,000 for fiscal year 2012;

9 “(D) \$84,200,000 for fiscal year 2013; and

10 “(E) \$90,000,000 for fiscal year 2014.”.

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

14 (1) in paragraph (4)—

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

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

19 (C) by adding at the end the following new
20 subparagraph:

21 “(E) how the center will partner with gov-
22 ernment laboratories, for-profit entities, other in-
23 stitutions of higher education, or nonprofit re-
24 search institutions.”; and

1 (2) *by amending paragraph (7) to read as fol-*
2 *lows:*

3 “(7) *AUTHORIZATION OF APPROPRIATIONS.—*
4 *There are authorized to be appropriated to the Na-*
5 *tional Science Foundation such sums as are necessary*
6 *to carry out this subsection for each of the fiscal years*
7 *2010 through 2014.”.*

8 (d) *COMPUTER AND NETWORK SECURITY CAPACITY*
9 *BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C.*
10 *7404(a)(6)) is amended to read as follows:*

11 “(6) *AUTHORIZATION OF APPROPRIATIONS.—*
12 *There are authorized to be appropriated to the Na-*
13 *tional Science Foundation such sums as are necessary*
14 *to carry out this subsection for each of the fiscal years*
15 *2010 through 2014.”.*

16 (e) *SCIENTIFIC AND ADVANCED TECHNOLOGY ACT*
17 *GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.*
18 *7404(b)(2)) is amended to read as follows:*

19 “(2) *AUTHORIZATION OF APPROPRIATIONS.—*
20 *There are authorized to be appropriated to the Na-*
21 *tional Science Foundation such sums as are necessary*
22 *to carry out this subsection for each of the fiscal years*
23 *2010 through 2014.”.*

1 (f) *GRADUATE TRAINEESHIPS IN COMPUTER AND NET-*
2 *WORK SECURITY.*—Section 5(c)(7) of such Act (15 U.S.C.
3 7404(c)(7)) is amended to read as follows:

4 “(7) *AUTHORIZATION OF APPROPRIATIONS.*—
5 *There are authorized to be appropriated to the Na-*
6 *tional Science Foundation such sums as are necessary*
7 *to carry out this subsection for each of the fiscal years*
8 *2010 through 2014.”.*

9 (g) *POSTDOCTORAL RESEARCH FELLOWSHIPS IN CY-*
10 *BERSECURITY.*—Section 5(e) of such Act (15 U.S.C.
11 7404(e)) is amended to read as follows:

12 “(e) *POSTDOCTORAL RESEARCH FELLOWSHIPS IN CY-*
13 *BERSECURITY.*—

14 “(1) *IN GENERAL.*—*The Director shall carry out*
15 *a program to encourage young scientists and engi-*
16 *neers to conduct postdoctoral research in the fields of*
17 *cybersecurity and information assurance, including*
18 *the research areas described in section 4(a)(1),*
19 *through the award of competitive, merit-based fellow-*
20 *ships.*

21 “(2) *AUTHORIZATION OF APPROPRIATIONS.*—
22 *There are authorized to be appropriated to the Na-*
23 *tional Science Foundation such sums as are necessary*
24 *to carry out this subsection for each of the fiscal years*
25 *2010 through 2014.”.*

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

3 (a) *IN GENERAL.*—*The Director of the National*
4 *Science Foundation shall carry out a Scholarship for Serv-*
5 *ice program to recruit and train the next generation of Fed-*
6 *eral cybersecurity professionals and to increase the capacity*
7 *of the higher education system to produce an information*
8 *technology workforce with the skills necessary to enhance*
9 *the security of the Nation’s communications and informa-*
10 *tion infrastructure.*

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

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

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

23 (3) *increase the capacity of institutions of higher*
24 *education throughout all regions of the United States*
25 *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*

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

13 *(c) SCHOLARSHIP REQUIREMENTS.—*

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

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

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

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

24 *(2) SELECTION.—Individuals shall be selected to*
25 *receive scholarships primarily on the basis of aca-*

1 *ademic merit, with consideration given to financial*
2 *need and to the goal of promoting the participation*
3 *of individuals identified in section 33 or 34 of the*
4 *Science and Engineering Equal Opportunities Act*
5 *(42 U.S.C. 1885a or 1885b).*

6 (3) *SERVICE OBLIGATION.*—*If an individual re-*
7 *ceives a scholarship under this section, as a condition*
8 *of receiving such scholarship, the individual upon*
9 *completion of their degree must serve as a cybersecu-*
10 *rity professional within the Federal workforce for a*
11 *period of time equal to the length of the scholarship.*
12 *If a scholarship recipient is not offered employment*
13 *by a Federal agency or a federally funded research*
14 *and development center, the service requirement can*
15 *be satisfied at the Director’s discretion by—*

16 (A) *serving as a cybersecurity professional*
17 *in a State, local, or tribal government agency; or*

18 (B) *teaching cybersecurity courses at an in-*
19 *stitution of higher education.*

20 (4) *CONDITIONS OF SUPPORT.*—*As a condition of*
21 *acceptance of a scholarship under this section, a re-*
22 *ipient shall agree to provide the awardee institution*
23 *with annual verifiable documentation of employment*
24 *and up-to-date contact information.*

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

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

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

7 (B) *is dismissed from such educational in-*
8 *stitution for disciplinary reasons;*

9 (C) *withdraws from the program for which*
10 *the award was made before the completion of*
11 *such program;*

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

15 (E) *fails to fulfill the service obligation of*
16 *the individual under this section,*

17 *such individual shall be liable to the United States as*
18 *provided in paragraph (3).*

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

23 (A) *enter into an agreement with the Direc-*
24 *tor of the National Science Foundation to mon-*

1 itor the compliance of scholarship recipients with
2 respect to their service obligation; and

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

8 (3) *AMOUNT OF REPAYMENT.*—

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

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

1 *shall be treated as a loan to be repaid in accord-*
2 *ance with subparagraph (C).*

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

14 (4) *COLLECTION OF REPAYMENT.*—

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

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

23 (ii) *collect such repayment amount*
24 *within a period of time as determined*
25 *under the agreement described in paragraph*

1 (2), or the repayment amount shall be treat-
2 ed as a loan in accordance with paragraph
3 (3)(C).

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

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

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

23 (e) *HIRING AUTHORITY.*—For purposes of any law or
24 regulation governing the appointment of individuals in the
25 Federal civil service, upon successful completion of their de-

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

8 (f) *AUTHORIZATION OF APPROPRIATIONS.*—There are
9 authorized to appropriated to the National Science Founda-
10 tion to carry out this section—

11 (1) \$18,700,000 for fiscal year 2010;

12 (2) \$20,100,000 for fiscal year 2011;

13 (3) \$21,600,000 for fiscal year 2012;

14 (4) \$23,300,000 for fiscal year 2013; and

15 (5) \$25,000,000 for fiscal year 2014.

16 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

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

21 (1) an examination of the current state of and
22 the projected needs of the Federal cybersecurity work-
23 force, including a comparison of the different agencies
24 and departments, and an analysis of the capacity of
25 such agencies and departments to meet 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, and an examination of the current and*
5 *future capacity of United States institutions of higher*
6 *education to provide cybersecurity professionals with*
7 *those skills sought by the Federal Government and the*
8 *private sector;*

9 (3) *an examination of the effectiveness of the Na-*
10 *tional Centers of Academic Excellence in Information*
11 *Assurance Education, the Centers of Academic Excel-*
12 *lence in Research, and the Federal Cyber Scholarship*
13 *for Service programs in promoting higher education*
14 *and research in cybersecurity and information assur-*
15 *ance and in producing a growing number of profes-*
16 *sionals with the necessary cybersecurity and informa-*
17 *tion assurance expertise;*

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

23 (5) *recommendations for Federal policies to en-*
24 *sure an adequate, well-trained Federal cybersecurity*
25 *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 and de-*
8 *velopment activities for cybersecurity through a consortium*
9 *or other appropriate entity with participants from institu-*
10 *tions of higher education and industry.*

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

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

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

24 (3) *define the roles and responsibilities for the*
25 *participants from institutions of higher education*
26 *and industry in such entity;*

1 *lists, configuration profiles, and deployment rec-*
2 *ommendations for products and protocols that mini-*
3 *mize the security risks associated with each computer*
4 *hardware or software system that is, or is likely to be-*
5 *come, widely used within 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 checklists under this subsection. Such prior-*
10 *ities may be based on the security risks associated*
11 *with the use of each system, the number of agencies*
12 *that use a particular system, the usefulness of the*
13 *checklist to Federal agencies that are users or poten-*
14 *tial users of the system, or such other factors as the*
15 *Director determines to be appropriate.*

16 *“(3) EXCLUDED SYSTEMS.—The Director of the*
17 *National Institute of Standards and Technology may*
18 *exclude from the requirements of paragraph (1) any*
19 *computer hardware or software system for which the*
20 *Director determines that the development of a check-*
21 *list is inappropriate because of the infrequency of use*
22 *of the system, the obsolescence of the system, or the*
23 *inutility or impracticability of developing a checklist*
24 *for the system.*

1 “(4) *AUTOMATION SPECIFICATIONS.*—*The Direc-*
2 *tor of the National Institute of Standards and Tech-*
3 *nology shall develop automated security specifications*
4 *(such as the Security Content Automation Protocol)*
5 *with respect to checklist content and associated secu-*
6 *rity related data.*

7 “(5) *DISSEMINATION OF CHECKLISTS.*—*The Di-*
8 *rector of the National Institute of Standards and*
9 *Technology shall ensure that Federal agencies are in-*
10 *formed of the availability of any product developed or*
11 *identified under the National Checklist Program for*
12 *any information system, including the Security Con-*
13 *tent Automation Protocol and other automated secu-*
14 *rity specifications.*

15 “(6) *AGENCY USE REQUIREMENTS.*—*The develop-*
16 *ment of a checklist under paragraph (1) for a com-*
17 *puter hardware or software system does not—*

18 “(A) *require any Federal agency to select*
19 *the specific settings or options recommended by*
20 *the checklist for the system;*

21 “(B) *establish conditions or prerequisites for*
22 *Federal agency procurement or deployment of*
23 *any such system;*

1 “(C) imply an endorsement of any such sys-
2 tem by the Director of the National Institute of
3 Standards and Technology; or

4 “(D) preclude any Federal agency from pro-
5 curing or deploying other computer hardware or
6 software systems for which no such checklist has
7 been developed or identified under paragraph
8 (1).”.

9 **SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
10 **NOLOGY CYBERSECURITY RESEARCH AND DE-**
11 **VELOPMENT.**

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

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

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

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

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

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

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

11 **SEC. 201. DEFINITIONS.**

12 *In this title:*

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

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

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

20 *The Director, in coordination with appropriate Fed-*
21 *eral authorities, shall—*

22 (1) *ensure coordination of United States Govern-*
23 *ment representation in the international development*
24 *of technical standards related to cybersecurity; and*

1 (2) *not later than 1 year after the date of enact-*
 2 *ment of this Act, develop and transmit to the Con-*
 3 *gress a proactive plan to engage international stand-*
 4 *ards bodies with respect to the development of tech-*
 5 *nical standards related to cybersecurity.*

6 **SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND**
 7 **EDUCATION.**

8 (a) *PROGRAM.*—*The Director, in collaboration with*
 9 *relevant Federal agencies, industry, educational institu-*
 10 *tions, and other organizations, shall develop and implement*
 11 *a cybersecurity awareness and education program to in-*
 12 *crease public awareness of cybersecurity risks, consequences,*
 13 *and best practices through—*

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

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

21 (b) *MANUFACTURING EXTENSION PARTNERSHIP.*—*The*
 22 *Director shall, to the extent appropriate, implement sub-*
 23 *section (a) through the Manufacturing Extension Partner-*
 24 *ship program under section 25 of the National Institute of*
 25 *Standards and Technology Act (15 U.S.C. 278k).*

1 (c) *REPORT TO CONGRESS.*—Not later than 90 days
2 *after the date of enactment of this Act, the Director shall*
3 *transmit to the Congress a report containing a strategy for*
4 *implementation of this section.*

5 **SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
6 **OPMENT.**

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

11 (1) *improve interoperability among identity*
12 *management technologies;*

13 (2) *strengthen authentication methods of identity*
14 *management systems;*

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

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

Union Calendar No. 236

11TH CONGRESS
2^D Session

H. R. 4061

[Report No. 111-405]

A BILL

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

JANUARY 27, 2010

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