

111TH CONGRESS
2^D SESSION

H. R. 4061

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 2010”.

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’.”;

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

24 (5) by inserting after paragraph (3) the fol-
25 lowing new paragraph:

1 “(4) In a series of hearings held before Con-
2 gress in 2009, experts testified that the Federal cy-
3 bersecurity research and development portfolio was
4 too focused on short-term, incremental research and
5 that it lacked the prioritization and coordination
6 necessary to address the long-term challenge of en-
7 suring a secure and reliable information technology
8 and communications infrastructure.”; and

9 (6) by amending paragraph (7), as so redesign-
10 nated by paragraph (4) of this section, to read as
11 follows:

12 “(7) While African-Americans, Hispanics, and
13 Native Americans constitute 33 percent of the col-
14 lege-age population, members of these minorities
15 comprise less than 20 percent of bachelor degree re-
16 cipients in the field of computer sciences.”.

17 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
18 **VELOPMENT PLAN.**

19 (a) IN GENERAL.—Not later than 12 months after
20 the date of enactment of this Act, the agencies identified
21 in subsection 101(a)(3)(B)(i) through (x) of the High-Per-
22 formance Computing Act of 1991 (15 U.S.C.
23 5511(a)(3)(B)(i) through (x)) or designated under section
24 101(a)(3)(B)(xi) of such Act, working through the Na-
25 tional Science and Technology Council and with the assist-

1 ance of the National Coordination Office, shall transmit
2 to Congress a strategic plan based on an assessment of
3 cybersecurity risk to guide the overall direction of Federal
4 cybersecurity and information assurance research and de-
5 velopment for information technology and networking sys-
6 tems. Once every 3 years after the initial strategic plan
7 is transmitted to Congress under this section, such agen-
8 cies shall prepare and transmit to Congress an update of
9 such plan.

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

12 (1) specify and prioritize near-term, mid-term
13 and long-term research objectives, including objec-
14 tives associated with the research areas identified in
15 section 4(a)(1) of the Cyber Security Research and
16 Development Act (15 U.S.C. 7403(a)(1)) and how
17 the near-term objectives complement research and
18 development areas in which the private sector is ac-
19 tively engaged;

20 (2) describe how the Program will focus on in-
21 novative, transformational technologies with the po-
22 tential to enhance the security, reliability, resilience,
23 and trustworthiness of the digital infrastructure, in-
24 cluding technologies to secure sensitive information
25 shared among Federal agencies;

1 (3) describe how the Program will foster the
2 transfer of research and development results into
3 new cybersecurity technologies and applications for
4 the benefit of society and the national interest, in-
5 cluding through the dissemination of best practices
6 and other 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
14 described in paragraph (4), as well as to relevant
15 data, including event data representing realistic
16 threats and vulnerabilities;

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

22 (7) outline how the United States can work
23 strategically with our international partners on cy-
24 bersecurity research and development issues where
25 appropriate; and

1 (8) describe how the Program will strengthen
2 all levels of cybersecurity education and training
3 programs to ensure an adequate, well-trained work-
4 force.

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

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

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

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

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

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

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

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

14 **SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBER-**
15 **SECURITY.**

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

18 (1) by inserting “and usability” after “to the
19 structure”;

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

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

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

1 “(J) social and behavioral factors, includ-
2 ing human-computer interactions, usability,
3 user motivations, and organizational cultures.”.

4 **SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECU-**
5 **RITY RESEARCH AND DEVELOPMENT PRO-**
6 **GRAMS.**

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

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

13 (2) by amending subparagraph (I) to read as
14 follows:

15 “(I) enhancement of the ability of law en-
16 forcement to detect, investigate, and prosecute
17 cyber-crimes, including crimes that involve pi-
18 racy of intellectual property, crimes against
19 children, and organized crime.”.

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) \$68,700,000 for fiscal year 2010;

1 “(B) \$73,500,000 for fiscal year 2011;
2 “(C) \$78,600,000 for fiscal year 2012;
3 “(D) \$84,200,000 for fiscal year 2013;
4 and
5 “(E) \$90,000,000 for fiscal year 2014.”.

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

9 (1) in paragraph (4)—

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

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

14 (C) by adding at the end the following new
15 subparagraph:

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

20 (2) by amending paragraph (7) to read as fol-
21 lows:

22 “(7) AUTHORIZATION OF APPROPRIATIONS.—
23 There are authorized to be appropriated to the Na-
24 tional Science Foundation such sums as are nec-

1 essary to carry out this subsection for each of the
2 fiscal years 2010 through 2014.”.

3 (d) COMPUTER AND NETWORK SECURITY CAPACITY
4 BUILDING GRANTS.—Section 5(a) of such Act (15 U.S.C.
5 7404(a)) is amended—

6 (1) in paragraph (3)(A), by inserting “, includ-
7 ing curriculum on the principles and techniques of
8 designing secure software” after “network security”;
9 and

10 (2) by amending paragraph (6) to read as fol-
11 lows:

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

17 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
18 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
19 7404(b)(2)) is amended to read as follows:

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

1 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
2 NETWORK SECURITY.—Section 5(c)(7) of such Act (15
3 U.S.C. 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 nec-
7 essary to carry out this subsection for each of the
8 fiscal years 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
13 CYBERSECURITY.—

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

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

1 (h) PROHIBITION ON EARMARKS.—None of the funds
2 appropriated under this section, and the amendments
3 made by this section may be used for a Congressional ear-
4 mark as defined in clause 9(d) of rule XXI of the Rules
5 of the House of Representatives.

6 (i) COMPUTER AND NETWORK SECURITY CAPACITY
7 BUILDING GRANTS—MANUFACTURING EXTENSION
8 PARTNERSHIP.—Section 5(a)(3) of the Cyber Security
9 Research and Development Act (15 U.S.C. 7404(a)(3)) is
10 amended—

11 (1) by striking “and” at the end of subpara-
12 graph (I);

13 (2) by redesignating subparagraph (J) as sub-
14 paragraph (K); and

15 (3) by inserting after subparagraph (I) the fol-
16 lowing new subparagraph:

17 “(J) establishing or enhancing collabora-
18 tion in computer and network security between
19 community colleges, universities, and Manufac-
20 turing Extension Partnership Centers; and”.

21 **SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE**
22 **PROGRAM.**

23 (a) IN GENERAL.—The Director of the National
24 Science Foundation shall carry out a Scholarship for Serv-
25 ice program to recruit and train the next generation of

1 Federal cybersecurity professionals and to increase the ca-
2 pacity of the higher education system to produce an infor-
3 mation technology workforce with the skills necessary to
4 enhance the security of the Nation's communications and
5 information infrastructure.

6 (b) CHARACTERISTICS OF PROGRAM.—The program
7 under this section shall—

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

14 (2) provide the scholarship recipients with sum-
15 mer internship opportunities or other meaningful
16 temporary appointments in the Federal information
17 technology workforce or, at the discretion of the Di-
18 rector, with appropriate private sector entities; and

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

24 (A) faculty professional development, in-
25 cluding technical, hands-on experiences in the

1 private sector or government, workshops, semi-
2 nars, conferences, and other professional devel-
3 opment opportunities that will result in im-
4 proved instructional capabilities;

5 (B) institutional partnerships, including
6 minority serving institutions and community
7 colleges;

8 (C) development of cybersecurity-related
9 courses and curricula; and

10 (D) outreach to secondary schools and 2-
11 year institutions to increase the interest and re-
12 cruitment of students into cybersecurity-related
13 fields.

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 infor-
22 mation assurance at an awardee institution;
23 and

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

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

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

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

21 For purposes of subparagraph (B), the term “serv-
22 ice-connected” has the meaning given such term
23 under 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 condi-

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

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

12 (B) teaching cybersecurity courses at an
13 institution of higher education.

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

19 (5) LENGTH OF SERVICE.—The length of serv-
20 ice required in exchange for a scholarship under this
21 subsection shall be as follows:

22 (A) For a recipient in a bachelor’s degree
23 program, 1 year more than the number of years
24 for which the scholarship was received.

1 (B) For a recipient in a master's degree
2 program, 2 years more than the number of
3 years for which the scholarship was received.

4 (C) For a recipient in a doctorate degree
5 program, 3 years more than the number of
6 years for which the scholarship was received.

7 (d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

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

10 (A) fails to maintain an acceptable level of
11 academic standing in the educational institution
12 in which the individual is enrolled, as deter-
13 mined by the Director;

14 (B) is dismissed from such educational in-
15 stitution for disciplinary reasons;

16 (C) withdraws from the program for which
17 the award was made before the completion of
18 such program;

19 (D) declares that the individual does not
20 intend to fulfill the service obligation under this
21 section; or

22 (E) fails to fulfill the service obligation of
23 the individual under this section,

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

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

5 (A) enter into an agreement with the Di-
6 rector of the National Science Foundation to
7 monitor the compliance of scholarship recipients
8 with respect to their service obligation; and

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

14 (3) AMOUNT OF REPAYMENT.—

15 (A) LESS THAN ONE YEAR OF SERVICE.—
16 If a circumstance described in paragraph (1)
17 occurs before the completion of 1 year of a
18 service obligation under this section, the total
19 amount of awards received by the individual
20 under this section shall be repaid or such
21 amount shall be treated as a loan to be repaid
22 in accordance with subparagraph (C).

23 (B) MORE THAN ONE YEAR OF SERVICE.—
24 If a circumstance described in subparagraph
25 (D) or (E) of paragraph (1) occurs after the

1 completion of 1 year of a service obligation
2 under this section, the total amount of scholar-
3 ship awards received by the individual under
4 this section, reduced by the ratio of the number
5 of years of service completed divided by the
6 number of years of service required, shall be re-
7 paid or such amount shall be treated as a loan
8 to be repaid in accordance with subparagraph
9 (C).

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

22 (4) COLLECTION OF REPAYMENT.—

23 (A) IN GENERAL.—In the event that a
24 scholarship recipient is required to repay the

1 scholarship under this subsection, the institu-
2 tion providing the scholarship shall—

3 (i) be responsible for determining the
4 repayment amounts and for notifying the
5 recipient and the Director of the amount
6 owed; and

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

13 (B) RETURNED TO TREASURY.—Except as
14 provided in subparagraph (C) of this para-
15 graph, any such repayment shall be returned to
16 the Treasury of the United States.

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

24 (5) EXCEPTIONS.—The Director may provide
25 for the partial or total waiver or suspension of any

1 service or payment obligation by an individual under
2 this section whenever compliance by the individual
3 with the obligation is impossible or would involve ex-
4 treme hardship to the individual, or if enforcement
5 of such obligation with respect to the individual
6 would be unconscionable.

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

18 (f) **AUTHORIZATION OF APPROPRIATIONS.**—There
19 are authorized to appropriated to the National Science
20 Foundation to carry out this section—

- 21 (1) \$18,700,000 for fiscal year 2010;
- 22 (2) \$20,100,000 for fiscal year 2011;
- 23 (3) \$21,600,000 for fiscal year 2012;
- 24 (4) \$23,300,000 for fiscal year 2013; and
- 25 (5) \$25,000,000 for fiscal year 2014.

1 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

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

6 (1) an examination of the current state of and
7 the projected needs of the Federal cybersecurity
8 workforce, including a comparison of the different
9 agencies and departments, the extent to which dif-
10 ferent agencies and departments rely on contractors
11 to support the Federal cybersecurity workforce, and
12 an analysis of the capacity of such agencies and de-
13 partments to meet those needs;

14 (2) an analysis of the sources and availability of
15 cybersecurity talent, a comparison of the skills and
16 expertise sought by the Federal Government and the
17 private sector, an examination of the current and fu-
18 ture capacity of United States institutions of higher
19 education, including community colleges, to provide
20 cybersecurity professionals with those skills sought
21 by the Federal Government and the private sector,
22 and a description of how successful programs are en-
23 gaging the talents of women and African-Americans,
24 Hispanics, and Native Americans in the cybersecu-
25 rity workforce;

1 (3) an examination of the effectiveness of the
2 National Centers of Academic Excellence in Infor-
3 mation Assurance Education, the Centers of Aca-
4 demic Excellence in Research, and the Federal
5 Cyber Scholarship for Service programs in pro-
6 moting higher education and research in cybersecu-
7 rity and information assurance and in producing a
8 growing number of professionals with the necessary
9 cybersecurity and information assurance expertise;

10 (4) an analysis of any barriers to the Federal
11 Government recruiting and hiring cybersecurity tal-
12 ent, including barriers relating to compensation, the
13 hiring process, job classification, job security clear-
14 ance and suitability requirements, and hiring flexi-
15 bilities;

16 (5) a specific analysis of the capacity of the
17 agency workforce to manage contractors who are
18 performing cybersecurity work on behalf of the Fed-
19 eral Government; and

20 (6) recommendations for Federal policies to en-
21 sure an adequate, well-trained Federal cybersecurity
22 workforce, including recommendations on the tem-
23 porary assignment of private sector cybersecurity
24 professionals to Federal agencies.

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

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

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

12 (1) develop options for a collaborative model
13 and an organizational structure for such entity
14 under which the joint research and development ac-
15 tivities could be planned, managed, and conducted
16 effectively, including mechanisms for the allocation
17 of resources among the participants in such entity
18 for support of 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 (4) propose guidelines for assigning intellectual
2 property rights, for the transfer of research and de-
3 velopment results to the private sector, and for the
4 sharing of lessons learned on the effectiveness of
5 new technologies from the private sector with the
6 public 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 community colleges, and from industry with knowledge
15 and expertise in cybersecurity, and shall include represent-
16 atives from minority-serving institutions.

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

1 **SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND**
2 **DISSEMINATION.**

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

6 “(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

7 “(1) IN GENERAL.—The Director of the Na-
8 tional Institute of Standards and Technology shall
9 develop or identify and revise or adapt as necessary,
10 checklists, configuration profiles, and deployment
11 recommendations for products and protocols that
12 minimize the security risks associated with each
13 computer hardware or software system that is, or is
14 likely to become, widely used within the Federal
15 Government.

16 “(2) PRIORITIES FOR DEVELOPMENT.—The Di-
17 rector of the National Institute of Standards and
18 Technology shall establish priorities for the develop-
19 ment of checklists under this subsection. Such prior-
20 ities may be based on the security risks associated
21 with the use of each system, the number of agencies
22 that use a particular system, the usefulness of the
23 checklist to Federal agencies that are users or po-
24 tential users of the system, or such other factors as
25 the Director determines to be appropriate.

1 “(3) EXCLUDED SYSTEMS.—The Director of
2 the National Institute of Standards and Technology
3 may exclude from the requirements of paragraph (1)
4 any computer hardware or software system for
5 which the Director determines that the development
6 of a checklist is inappropriate because of the infre-
7 quency of use of the system, the obsolescence of the
8 system, or the inutility or impracticability of devel-
9 oping a checklist for the system.

10 “(4) AUTOMATION SPECIFICATIONS.—The Di-
11 rector of the National Institute of Standards and
12 Technology shall develop automated security speci-
13 fications (such as the Security Content Automation
14 Protocol) with respect to checklist content and asso-
15 ciated security related data.

16 “(5) DISSEMINATION OF CHECKLISTS.—The
17 Director of the National Institute of Standards and
18 Technology shall ensure that Federal agencies are
19 informed of the availability of any product developed
20 or identified under the National Checklist Program
21 for any information system, including the Security
22 Content Automation Protocol and other automated
23 security specifications.

1 “(6) AGENCY USE REQUIREMENTS.—The devel-
2 opment of a checklist under paragraph (1) for a
3 computer hardware or software system does not—

4 “(A) require any Federal agency to select
5 the specific settings or options recommended by
6 the checklist for the system;

7 “(B) establish conditions or prerequisites
8 for Federal agency procurement or deployment
9 of any such system;

10 “(C) imply an endorsement of any such
11 system by the Director of the National Institute
12 of Standards and Technology; or

13 “(D) preclude any Federal agency from
14 procuring or deploying other computer hard-
15 ware or software systems for which no such
16 checklist has been developed or identified under
17 paragraph (1).”.

18 **SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
19 **NOLOGY CYBERSECURITY RESEARCH AND**
20 **DEVELOPMENT.**

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

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

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

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

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

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

19 **SEC. 111. NATIONAL ACADEMY OF SCIENCES STUDY ON**
20 **THE ROLE OF COMMUNITY COLLEGES IN CY-**
21 **BERSECURITY EDUCATION.**

22 Not later than 120 days after the date of enactment
23 of this Act, the Director of the Office of Science and Tech-
24 nology Policy, in consultation with the Director of the Na-
25 tional Coordination Office, shall enter into a contract with

1 the National Academy of Sciences to conduct and complete
2 a study to describe the role of community colleges in cy-
3 bersecurity education and to identify exemplary practices
4 and partnerships related to cybersecurity education be-
5 tween community colleges and 4-year educational institu-
6 tions.

7 **SEC. 112. NATIONAL CENTER OF EXCELLENCE FOR CYBER-**
8 **SECURITY.**

9 (a) IN GENERAL.—As part of the Program, the Di-
10 rector of the National Science Foundation shall, in coordi-
11 nation with other Federal agencies participating in the
12 Program, establish a National Center of Excellence for
13 Cybersecurity.

14 (b) MERIT REVIEW.—The National Center of Excel-
15 lence for Cybersecurity shall be awarded on a merit-re-
16 viewed, competitive basis.

17 (c) ACTIVITIES SUPPORTED.—The National Center
18 of Excellence for Cybersecurity shall—

19 (1) involve institutions of higher education or
20 national laboratories and other partners, which may
21 include States and industry;

22 (2) make use of existing expertise in cybersecu-
23 rity;

1 (3) interact and collaborate with Computer and
2 Network Security Research Centers to foster the ex-
3 change of technical information and best practices;

4 (4) perform research to support the develop-
5 ment of technologies for testing hardware and soft-
6 ware products to validate operational readiness and
7 certify stated security levels;

8 (5) coordinate cybersecurity education and
9 training opportunities nationally;

10 (6) enhance technology transfer and commer-
11 cialization that promote cybersecurity innovation;
12 and

13 (7) perform research on cybersecurity social
14 and behavioral factors, including human-computer
15 interactions, usability, user motivations, and organi-
16 zational cultures.

17 **SEC. 113. CYBERSECURITY INFRASTRUCTURE REPORT.**

18 Not later than 1 year after the date of enactment
19 of this Act, the Comptroller General shall transmit to the
20 Congress a report examining key weaknesses within the
21 current cybersecurity infrastructure, along with rec-
22 ommendations on how to address such weaknesses in the
23 future and on the technology that is needed to do so.

1 **TITLE II—ADVANCEMENT OF CY-**
2 **BERSECURITY TECHNICAL**
3 **STANDARDS**

4 **SEC. 201. DEFINITIONS.**

5 In this title:

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

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

11 **SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL**
12 **STANDARDS.**

13 The Director, in coordination with appropriate Fed-
14 eral authorities, shall—

15 (1) ensure coordination of United States Gov-
16 ernment representation in the international develop-
17 ment of technical standards related to cybersecurity;
18 and

19 (2) not later than 1 year after the date of en-
20 actment of this Act, develop and transmit to the
21 Congress a proactive plan to engage international
22 standards bodies with respect to the development of
23 technical standards related to cybersecurity.

1 **SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND**
2 **EDUCATION.**

3 (a) PROGRAM.—The Director, in collaboration with
4 relevant Federal agencies, industry, educational institu-
5 tions, and other organizations, shall develop and imple-
6 ment a cybersecurity awareness and education program to
7 increase public awareness, including among children and
8 young adults, of cybersecurity risks, consequences, and
9 best practices through—

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

13 (2) efforts to make cybersecurity technical
14 standards and best practices usable by individuals,
15 small to medium-sized businesses, State, local, and
16 tribal governments, and educational institutions, es-
17 pecially with respect to novice computer users, elder-
18 ly populations, low-income populations, and popu-
19 lations in areas of planned broadband expansion or
20 deployment.

21 (b) WORKSHOPS.—In carrying out activities under
22 subsection (a)(1), the Institute is authorized to host re-
23 gional workshops to provide an overview of cybersecurity
24 risks and best practices to businesses, State, local, and
25 tribal governments, and educational institutions.

1 (c) MANUFACTURING EXTENSION PARTNERSHIP.—
2 The Director shall, to the extent appropriate, implement
3 subsection (a) through the Manufacturing Extension Part-
4 nership program under section 25 of the National Insti-
5 tute of Standards and Technology Act (15 U.S.C. 278k).

6 (d) REPORT TO CONGRESS.—Not later than 90 days
7 after the date of enactment of this Act, the Director shall
8 transmit to the Congress a report containing a strategy
9 for implementation of this section.

10 **SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
11 **OPMENT.**

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

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

18 (2) strengthen authentication methods of iden-
19 tity 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. 205. PRACTICES AND STANDARDS.**

2 The National Institute of Standards and Technology
3 shall work with other Federal, State, and private sector
4 partners, as appropriate, to develop a framework that
5 States may follow in order to achieve effective cybersecu-
6 rity practices in a timely and cost-effective manner.

 Passed the House of Representatives February 4,
2010.

Attest:

Clerk.

111TH CONGRESS
2^D SESSION

H. R. 4061

AN ACT

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