HR 4061 TEXT, SUMMARY AND ANALYSIS

I. BILL TEXT

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the `Cybersecurity Enhancement Act of 2009'.

TITLE I--RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

(1) NATIONAL COORDINATION OFFICE- The term National Coordination Office means the National Coordination Office for the Networking and Information Technology Research and Development program.

(2) PROGRAM- The term Program means the Networking and Information Technology Research and Development program which has been established under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511).

SEC. 102. FINDINGS.

Section 2 of the Cyber Security Research and Development Act (15 U.S.C. 7401) is amended--

(1) by amending paragraph (1) to read as follows:
`(1) Advancements in information and communications technology have resulted in a globally interconnected network of government, commercial, scientific, and education infrastructures, including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services.';

(2) in paragraph (2), by striking `Exponential increases in interconnectivity have facilitated enhanced communications, economic growth,' and inserting `These advancements have significantly contributed to the growth of the United States economy';

(3) by amending paragraph (3) to read as follows:
`(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has `suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and

other entities to steal intellectual property and sensitive military information'.';
(4) by redesignating paragraphs (4) through (6) as paragraphs (5) through (7), respectively;
(5) by inserting after paragraph (3) the following new paragraph:
`(4) In a series of hearings held before Congress in 2009, experts testified that the Federal cybersecurity research and development portfolio was too focused on short-term, incremental research and that it lacked the prioritization and coordination necessary to address the long-term challenge of ensuring a secure and reliable information technology and communications infrastructure.'; and
(6) by amending paragraph (7), as so redesignated by paragraph (4) of this section, to read as follows:
`(7) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.'.

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) In General- Not later than 12 months after the date of enactment of this Act, the agencies identified in subsection 101(a)(3)(B)(i) through (x) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i) through (x)) or designated under section 101(a)(3)(B)(xi) of such Act, working through the National Science and Technology Council and with the assistance of the National Coordination Office, shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. Once every 3 years after the initial strategic plan is transmitted to Congress under this section, such agencies shall prepare and transmit to Congress an update of such plan.
(b) Contents of Plan- The strategic plan required under subsection (a) shall--
(1) specify and prioritize near-term, mid-term and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) and how the near-term objectives complement research and development areas in which the private sector is actively engaged;
(2) describe how the Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure;
(3) describe how the Program will foster the transfer of research and development results into new cybersecurity technologies and applications for the benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;
(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and
(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

(c) Development of Roadmap- The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan required in this section. Such roadmap shall--

(1) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;
(2) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and
(3) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years.

(d) Recommendations- In developing and updating the strategic plan under subsection (a), the agencies involved shall solicit recommendations and advice from--

(1) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and
(2) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions, and other relevant organizations and institutions.

(e) Appending to Report- The implementation roadmap required under subsection (c), and its annual updates, shall be appended to the report required under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

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

(1) by inserting `and usability' after `to the structure';
(2) in subparagraph (H), by striking `and' after the semicolon;
(3) in subparagraph (I), by striking the period at the end and inserting `; and'; and
(4) by adding at the end the following new subparagraph:

`(J) social and behavioral factors, including human-computer interactions, usability, user motivations, and organizational cultures.'.

SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

(a) Computer and Network Security Research Areas- Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended in subparagraph (A) by inserting `identity management,' after `cryptography,'.

(b) Computer and Network Security Research Grants- Section 4(a)(3) of such Act (15 U.S.C. 7403(a)(3)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

`(A) $68,700,000 for fiscal year 2010;

`(B) $73,500,000 for fiscal year 2011;

`(C) $78,600,000 for fiscal year 2012;

`(D) $84,200,000 for fiscal year 2013; and

`(E) $90,000,000 for fiscal year 2014.'.

(c) Computer and Network Security Research Centers- Section 4(b) of such Act (15 U.S.C. 7403(b)) is amended--

(1) in paragraph (4)--

(A) in subparagraph (C), by striking `and' after the semicolon;

(B) in subparagraph (D), by striking the period and inserting `; and'; and

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

`(E) how the center will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions.'; and

(2) by amending paragraph (7) to read as follows:

`(7) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.'.

(d) Computer and Network Security Capacity Building Grants- Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended to read as follows:

`(6) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.'.

(e) Scientific and Advanced Technology Act Grants- Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended to read as follows:

`(2) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.'.

(f) Graduate Traineeships in Computer and Network Security- Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended to read as follows:

`(7) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.'.

(g) Postdoctoral Research Fellowships in Cybersecurity- Section 5(e) of such Act (15 U.S.C. 7404(e)) is amended to read as follows:

`(e) Postdoctoral Research Fellowships in Cybersecurity-

`(1) IN GENERAL- The Director shall carry out a program to encourage young scientists and engineers to conduct postdoctoral research in the fields of cybersecurity and information assurance, including the research areas described in section 4(a)(1), through the award of competitive, merit-based fellowships.

`(2) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.'.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) In General- The Director of the National Science Foundation shall carry out a Scholarship for Service program to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure.

(b) Characteristics of Program- The program under this section shall--

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

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as--

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional development opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions; and

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

(c) Scholarship Requirements-

(1) ELIGIBILITY- Scholarships under this section shall be available only to students who--

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

(B) are full-time students in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution; and

(C) accept the terms of a scholarship pursuant to this section.

(2) SELECTION- Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need and to the goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b).

(3) SERVICE OBLIGATION- If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time equal to the length of the scholarship. If a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by--

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

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

(4) CONDITIONS OF SUPPORT- As a condition of acceptance of a scholarship under this section, a recipient shall agree to provide the awardee institution with annual verifiable documentation of employment and up-to-date contact information.

(d) Failure to Complete Service Obligation-

(1) GENERAL RULE- If an individual who has received a scholarship under this section--

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

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

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

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

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

(2) MONITORING COMPLIANCE- As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall--

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligation; and

(B) provide to the Director, on an annual basis, post-award employment information required under subsection (c)(4) for scholarship recipients through the completion of their service obligation.

(3) AMOUNT OF REPAYMENT-

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

(B) MORE THAN ONE YEAR OF SERVICE- If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS- A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a and following), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT-

(A) IN GENERAL- In the event that a scholarship recipient is required to repay the scholarship under this subsection, the institution providing the scholarship shall--

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

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

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

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

(5) EXCEPTIONS- The Director may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(e) Hiring Authority- For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon successful completion of their degree, students receiving a scholarship under this section shall be hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations, and be exempted from competitive service. Upon fulfillment of the service term, such individuals shall be converted to a competitive service position without competition if the individual meets the requirements for that position.

(f) Authorization of Appropriations- There are authorized to appropriated to the National Science Foundation to carry out this section--

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

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

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

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

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

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.

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

(1) an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs;

(2) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, and an examination of the current and future capacity of United States institutions of higher education to provide cybersecurity professionals with those skills sought by the Federal Government and the private sector;

(3) an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise;
(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities; and
(5) recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) Establishment of University-Industry Task Force- Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.
(b) Functions- The task force shall--
(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;
(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;
(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;
(4) propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector; and
(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources.
(c) Composition- In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cybersecurity.
(d) Report- Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force.

SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

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

`(c) Checklists for Government Systems-

`(1) IN GENERAL- The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

`(2) PRIORITIES FOR DEVELOPMENT- The Director of the National Institute of Standards and Technology shall establish priorities for the development of checklists under this subsection. Such priorities may be based on the security risks associated with the use of each system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate.

`(3) EXCLUDED SYSTEMS- The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any computer hardware or software system for which the Director determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

`(4) AUTOMATION SPECIFICATIONS- The Director of the National Institute of Standards and Technology shall develop automated security specifications (such as the Security Content Automation Protocol) with respect to checklist content and associated security related data.

`(5) DISSEMINATION OF CHECKLISTS- The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any product developed or identified under the National Checklist Program for any information system, including the Security Content Automation Protocol and other automated security specifications.

`(6) AGENCY USE REQUIREMENTS- The development of a checklist under paragraph (1) for a computer hardware or software system does not--

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

`(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

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

`(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed or identified under paragraph (1).'.

SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

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

`(e) Intramural Security Research- As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall--

`(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

`(2) carry out research associated with improving the security of information systems and networks;

`(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

`(4) carry out research associated with improving security of industrial control systems.'.

TITLE II--ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

(1) DIRECTOR- The term `Director' means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE- The term `Institute' means the National Institute of Standards and Technology.

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

The Director, in coordination with appropriate Federal authorities, shall--

(1) ensure coordination of United States Government representation in the international development of technical standards related to cybersecurity; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a proactive plan to engage international

standards bodies with respect to the development of technical standards related to cybersecurity.

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) Program- The Director, in collaboration with relevant Federal agencies, industry, educational institutions, and other organizations, shall develop and implement a cybersecurity awareness and education program to increase public awareness of cybersecurity risks, consequences, and best practices through--

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State, local, and tribal governments, and educational institutions.

(b) Manufacturing Extension Partnership- The Director shall, to the extent appropriate, implement subsection (a) through the Manufacturing Extension Partnership program under section 25 of the National Institute of Standards and Technology Act (15 U.S.C. 278k).

(c) Report to Congress- Not later than 90 days after the date of enactment of this Act, the Director shall transmit to the Congress a report containing a strategy for implementation of this section.

SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

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

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

(3) improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) improve the usability of identity management systems.

II. PURPOSE OF THE BILL

The purpose of this bill is to improve cybersecurity in the Federal, private, and public sectors through: coordination and prioritization of federal cybersecurity research and development activities; strengthening of the cybersecurity workforce; coordination of U.S. representation in international cybersecurity technical standards development; and reauthorization of cybersecurity related programs at the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST).

III. BACKGROUND AND NEED FOR THE LEGISLATION

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulnerability of these systems. Reports of cyber criminals and possibly nation-states accessing sensitive information and disrupting services have risen steadily over the last decade, heightening concerns over the adequacy of our cybersecurity measures.

The Office of Management and Budget cites that federal agencies spend $6 billion on cybersecurity to protect a $72 billion IT infrastructure. In addition, the Federal government funds approximately $350 million in cybersecurity research and development (R&D) each year. Despite this Federal spending, the Government Accountability Office testified as recently as June 2009 that the U.S. IT infrastructure is vulnerable to attack and the Federal agencies tasked with its protection are not fulfilling their responsibilities.

On May 29, 2009, the Obama Administration released the Cyberspace Policy Review, a 60-day review of cyberspace policies across the Federal government. The findings of the review include: strengthening partnerships between the Federal government and the private sector to guarantee a secure and reliable infrastructure, increasing public awareness of the risks associated with cybersecurity, expanding and training the Federal cybersecurity workforce, advancing cybersecurity R&D, and better coordination among Federal agencies.

Specifically, the review recommends the development of an R&D framework that focuses on strategies for innovative technologies and calls for a single entity to coordinate United States representation in international cybersecurity technical standards setting bodies. In the mid-term, it recommends that Federal agencies expand support for cybersecurity education and R&D to ensure the Nation's continued ability to compete in the information age economy.

The task of coordinating unclassified cybersecurity R&D lies with the Networking and Information Technology Research and Development (NITRD) program, which was originally authorized in statute by the High-Performance Computing Act of 1991 (P.L. 102-194). The NITRD program, which consists of 13 Federal agencies, coordinates a broad spectrum of R&D activities related to information technology. It also includes an interagency working group and program component area focused specifically on cybersecurity and information R&D. However, many expert panels, including the President's Council of Advisors on Science and Technology, have argued that the portfolio of Federal investments in cybersecurity R&D is not properly balanced and is focused on short-term reactive technologies at the expense of long-term, fundamental R&D.

With a budget of $127 million for FY 2010, NSF is the principal agency supporting unclassified cybersecurity R&D and education. NSF's cybersecurity research activities

are primarily funded through the Directorate for Computer & Information Science & Engineering (CISE). CISE supports cybersecurity R&D through a targeted program, Trustworthy Computing, as well as through a number of its core activities in Computer Systems Research, Computing Research Infrastructure, and Network and Science Engineering. In addition to its basic research activities, NSF's Directorate for Education & Human Resources (EHR) manages the Scholarship for Service program which provides funding to colleges and universities for the award of 2-year scholarships in information assurance and computer security fields.

NIST is tasked with protecting the Federal information technology network by developing and promulgating cybersecurity standards for Federal non-classified network systems (Federal Information Processing Standard [FIPS]), identifying methods for assessing effectiveness of security requirements, conducting tests to validate security in information systems, and conducting outreach exercises. Experts have stated that NIST's technical standards and best practices are too highly technical for general public use, and making this information more usable to average computer users with less technical expertise will help raise the base level of cybersecurity knowledge among individuals, business, education, and government.

Currently, the United States is represented on international bodies dealing with cybersecurity by an array of organizations, including the Department of State, Department of Commerce, Federal Communications Commission, and the United States Trade Representative without a coordinated and comprehensive strategy or plan. The Cyberspace Policy Review called for a comprehensive international cybersecurity strategy that defines what cybersecurity standards we need, where they are being developed, and ensures that the United States Federal government has agency representation for each. At a hearing before the Committee's Technology and Innovation Subcommittee, witnesses stated that NIST is the appropriate Federal agency to coordinate the development of this strategy due to its status as a non-regulatory agency known and respected among international and private sector stakeholders.

In the 107th Congress, the Science and Technology Committee developed the Cyber Security Research and Development Act (P.L. 107-305). The bill created new programs and expanded existing programs at NSF and NIST for computer and network security. The authorizations established under the Cyber Security Research and Development Act expired in fiscal year 2007.

IV. HEARING SUMMARY

During the 111th Congress, the Committee on Science and Technology held four hearings relevant to H.R. 4061.

On June 10, 2009, the Subcommittee on Research and Science Education held a hearing focused on priorities and existing gaps in the cybersecurity research and development portfolio, as well as the adequacy of cybersecurity education and workforce training programs. The Subcommittee heard from witnesses from academia and the private sector,

including: (1) Dr. Seymour Goodman, Professor of International Affairs and Computing and Co-Director, Georgia Tech Information Security Center, Georgia Institute of Technology; (2) Ms. Liesyl Franz, Vice President, Information Security and Global Public Policy, TechAmerica; (3) Dr. Anita D'Amico, Director, Secure Decisions Division, Applied Visions, Inc.; (4) Dr. Fred Schneider, Samuel B. Eckert Professor of Computer Science, Department of Computer Science, Cornell University; (5) Mr. Timothy Brown, Vice President and Chief Architect, CA Security Management.

On June 16, 2009, the Subcommittee on Research and Science Education and the Subcommittee on Technology and Innovation held a joint hearing entitled `Agency Response to Cyberspace Policy Review.' The hearing reviewed the response of the Department of Homeland Security (DHS), NIST, NSF, and the Defense Advanced Research Projects Agency (DARPA) to the findings and recommendations in the Administration's Cyberspace Policy Review. There were four witnesses: (1) Ms. Cita Furlani, Director, Information Technology Laboratory, NIST; (2) Dr. Jeannette Wing, Assistant Director, Directorate for Computer & Information Science & Engineering, NSF; (3) Dr. Robert F. Leheny, Acting Director, DARPA; and (4) Dr. Peter Fonash, Acting Deputy Assistant Secretary, Office of Cyber Security Communications, DHS.

On June 25, 2009, the Subcommittee on Technology and Innovation held a hearing to assess the cybersecurity efforts of DHS and NIST. Witnesses from the hearing indicated that cybersecurity performance should be more systematically assessed through enhanced metrics and success criteria. Witnesses also highlighted the need to improve the monitoring of Federal networks and the role Federal cybersecurity activities can have on privately-owned critical infrastructure. There were four witnesses: (1) Mr. Greg Wilshusen, Director, Information Security Issues, Government Accountability Office (GAO); (2) Mr. Mark Bregman, Executive Vice President and Chief Technology Officer, Symantec Corporation; (3) Mr. Scott Charney, Corporate Vice President, Trustworthy Computing Group, Microsoft Corporation; and (4) Mr. Jim Harper, Director, Information Policy Studies, Cato Institute.

On October 22, 2009, the Subcommittee on Technology and Innovation held a hearing entitled `Cybersecurity Activities at NIST's Information Technology Laboratories.' The hearing examined recommendations made in the Cyberspace Policy Review, culminating in three recommendations for NIST: (1) NIST should coordinate U.S. Federal representation in international cybersecurity technical standards development because it has the technical expertise required; (2) NIST should carry out cybersecurity awareness activities; and (3) NIST should increase efforts in the area of identity management. Six witnesses testified: (1) Ms. Cita Furlani, Director, Information Technology Laboratory, NIST; (2) Dr. Susan Landau, Distinguished Engineer, Sun Microsystems; (3) Professor Fred Schneider, Samuel B. Eckert Professor, Computer Science, Cornell University; (4) Dr. Phyllis Schneck, Vice President, Threat Intelligence, McAfee; (5) Mr. William Wyatt Starnes, Founder and CEO, SignaCert, Inc.; (6) Mr. Mark Bohannon, General Counsel and Senior Vice President, Public Policy, Software and Information Industry Association.

V. COMMITTEE ACTIONS

As summarized in Section IV of this report, the Committee on Science and Technology heard testimony relevant to H.R. 4061 in the 111th Congress at hearings held on June 10, June 16, June 25 and October 22, 2009.

H.R. 4061 is a combination of two Committee discussion drafts: the *Cybersecurity Research and Development Amendments Act of 2009* and the *Cybersecurity Coordination and Awareness Act of 2009*.

On September, 23, 2009, the Subcommittee on Research and Science Education met to consider the *Cybersecurity Research and Development Amendments Act of 2009* and the following amendments to the bill:

Mr. Lipinski offered an amendment to reauthorize NSF's cybersecurity research centers program, and to clarify the responsibilities and requirements of scholarship recipients and awardee institutions in the monitoring and reporting of information related to a scholarship recipient's service obligation. The amendment was agreed to by a voice vote.

Ms. Johnson offered an amendment requiring that the strategic plan describe how the program will increase the diversity of the cybersecurity workforce and specifying that the goal of promoting diversity be considered in the selection of scholarship recipients. The amendment was agreed to by a voice vote.

Mr. Lipinski moved that the Subcommittee favorably report the bill, as amended, to the full Committee. The motion was agreed to by a voice vote.

On November 4, 2009, the Subcommittee on Technology and Innovation met to consider the *Cybersecurity Coordination and Awareness Act of 2009.* The Subcommittee considered a joint manager's amendment offered by Representatives Wu and Smith to make technical and clarifying changes, which was agreed to by a voice vote.

Mr. Wu moved that the Subcommittee favorably report the bill, as amended, to the full Committee with the recommendation that the bill pass. The motion was agreed to by voice vote.

On November 7, 2009, Representative Lipinski, for himself, Mr. McCaul, Mr. Wu , Mr. Ehlers, Ms. Johnson, Mr. Smith (NE), Mr. Gordon, Mr. Hall, Mr. Lujan, and Mr. Rothman, introduced H.R. 4061, the *Cybersecurity Enhancement Act of 2009,* a bill to advance cybersecurity research, development, and technical standards, and for other purposes.

On November 18, 2009, the Committee on Science and Technology met to consider H.R. 4061 and the following amendments to the bill:

An amendment in the nature of a substitute offered by Mr. Lipinski. The amendment makes several technical and clarifying changes to the bill, including the addition of items

that were part of the Committee print reported by the Subcommittee on Research and Science Education. The amendment was adopted by voice vote.

An amendment offered by Mr. Lujan clarifying that capacity building grants offered through the Scholarship for Service program should be available to qualified institutions of higher education `throughout all regions of the United States,' and that tribal governments are included as recipients of information on best practices and technical standards disseminated by NIST. The amendment was adopted by voice vote.

An amendment offered by Mr. McCaul clarifying the manner in which security checklists produced by NIST shall be disseminated, and emphasizing that the implementation of such checklists by federal agencies should remain flexible. The amendment was adopted by voice vote.

An amendment offered by Mr. Wu requiring the identity management R&D program established by NIST improves the `usability of identity management systems.' The amendment was adopted by voice vote.

Mr. Wu moved that the Committee favorably report the bill, H.R. 4061, as amended, to the House. The motion was agreed to by a voice vote.

VI. SUMMARY OF MAJOR PROVISIONS OF THE BILL

Requires agencies participating in the NITRD program to develop, update, and implement a strategic plan guiding the overall direction of Federal cybersecurity and information assurance R&D.

Reauthorizes cybersecurity workforce and traineeship programs at NSF, including through the Advanced Technological Education program, the Integrative Graduate Education and Research Traineeship program and the Graduate Research Fellowship program.

Requires the President to conduct an assessment of cybersecurity workforce needs across the Federal government and formally authorizes NSF to carry out the Scholarship for Service program.

Reauthorizes cybersecurity research at NSF, including through the Trustworthy Computing program.

Requires the Director of the Office of Science and Technology Policy to convene a university-industry task force to explore mechanisms for carrying out collaborative R&D.

Requires NIST to develop and implement a plan to coordinate U.S. representation in the development of international cybersecurity technical standards. Requires NIST to develop and implement a cybersecurity awareness and education program for the dissemination of user-friendly cybersecurity best practices and technical standards.

VII. SECTION-BY-SECTION ANALYSIS

TITLE I--RESEARCH AND DEVELOPMENT

Sec. 101. Definitions

Defines the terms National Coordination Office and Program in the title.

Sec. 102. Findings

Describes the findings of this title.

Sec. 103. Cybersecurity strategic R&D plan

Requires the agencies to develop, update and implement a strategic plan for cybersecurity research and development (R&D). Requires that the strategic plan be based on an assessment of cybersecurity risk, that it specify and prioritize near-term, mid-term and long-term research objectives, and that it describe how the near-term objectives complement R&D occurring in the private sector.

Requires the agencies to solicit input from an advisory committee and outside stakeholders in the development of the strategic plan. Additionally, requires the agencies to describe how they will promote innovation, foster technology transfer, and maintain a national infrastructure for the development of secure, reliable, and resilient networking and information technology systems.

Requires the development of an implementation roadmap that specifies the role of each agency and the level of funding needed to meet each of the research objectives outlined in the strategic plan.

Sec. 104. Social and behavioral research in cybersecurity

Requires the National Science Foundation (NSF) to support research on the social and behavioral aspects of cybersecurity as part of its total cybersecurity research portfolio.

Sec. 105. NSF cybersecurity R&D programs

Reauthorizes the cybersecurity research program at the NSF and includes identity management as one of the research areas supported.

Reauthorizes programs at NSF that provide funding for capacity building grants, graduate student fellowships, graduate student traineeships and research centers in cybersecurity.

Requires NSF to establish a postdoctoral fellowship program in cybersecurity.

Sec. 106. Federal cyber scholarship for service program

Authorizes the cybersecurity scholarship for service program at NSF. The program provides grants to institutions of higher education for the award of scholarships to students pursuing undergraduate and graduate degrees in cybersecurity fields and requires an equal number of years of service as a cybersecurity professional in the federal government as a condition of the scholarship.

The program also provides capacity building grants to institutions of higher education, supporting such activities as faculty professional development and the development of cybersecurity-related curricula and courses.

Sec. 107. Cybersecurity workforce assessment

Requires the President to issue a report assessing the current and future cybersecurity workforce needs of the federal government, including a comparison of the skills sought by Federal agencies and the private sector; an examination of the supply of cybersecurity talent and the capacity of institutions of higher education to produce cybersecurity professionals; and the identification of any barriers to the recruitment and hiring of cybersecurity professionals.

Sec. 108. Cybersecurity University--Industry Task Force

Establishes a university-industry task force to explore mechanisms and models for carrying out public-private research partnerships in the area of cybersecurity.

Sec. 109. Cybersecurity checklist and dissemination

Updates NIST's authority for the National Checklist Program (NCP), which provides detailed guidance on setting the security configuration of operating systems and applications and requires NIST to develop automated security specifications with respect to checklist content.

Sec. 110. NIST Cybersecurity R&D

Amends the National Institute of Standards and Technology Act to authorize NIST, as part of its in-house research program, to continue efforts to develop a unifying and standardized identity, privilege, and access control management framework. Authorizes NIST to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.

TITLE II--ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

Sec. 201. Definitions

Defines the terms Director and Institute in the title.

Sec. 202. International cybersecurity technical standards

Requires NIST to develop and implement a plan to ensure a coordinated United States Government representation in international cybersecurity technical standards development. This plan is due to Congress no later than one year after enactment.

Sec. 203. Promoting cybersecurity awareness and education

Requires NIST to deliver a plan to Congress within 90 days describing how it will develop and implement a cybersecurity awareness and education program. Requires the program to be aimed at disseminating cybersecurity best practices and standards and shall include how NIST will make these usable by individuals, small business, state and local governments, and educational institutions. Requires the plan to include how NIST can utilize established Manufacturing Extension Partnership networks to have cybersecurity information readily available to small manufacturing companies.

Sec. 204. Identity management research and development

Requires NIST to engage in research and development programs to improve identity management systems.

VIII. COMMITTEE VIEWS

Cybersecurity strategic R&D plan and implementation roadmap

The Committee expects the strategic plan to be a useful guide for setting program priorities and estimating time scales for reaching program objectives. The strategic plan should not be limited to time scales of 2-3 years, but should include mid-term and long-term research objectives based on known research gaps and an assessment of cybersecurity risks to ensure that R&D objectives are informed and prioritized by the Nation's needs. Furthermore, the Committee intends for the development of the plan to be informed by the research needs of industry and academia and expects the National Coordination Office to actively solicit stakeholder input through meetings, requests for information and other appropriate means.

The Committee believes the development of an implementation roadmap is essential to the furtherance of cybersecurity and information assurance R&D. The roadmap should be aligned with the program's strategic plan and overall objectives, and should be detailed enough to clearly define the roles and responsibilities of individual Federal agencies in the achievement of the overall R&D objectives. While each Federal agency has its own mission and objectives in the area of cybersecurity and information assurance, the Committee considers the development of an implementation roadmap essential to comprehensively addressing our cybersecurity challenges.

Cybersecurity education and workforce

Over the next several years, the Bureau of Labor Statistics estimates that the number of jobs requiring a background in computer science or mathematics will average approximately 150,000 annually. However, the number of computer science undergraduate degrees granted has dropped 34 percent from 2002 to 2006. Additionally, according to the report entitled, `Cyber In-Security: Strengthening the Federal Cybersecurity Workforce,' there is a shortfall of between 500 and 1000 cybersecurity professionals each year across the Federal government. The Committee believes that the required assessment of Federal cybersecurity workforce needs, necessary skills, and the capacity of our colleges and universities to produce cybersecurity professionals is an essential first step in ensuring an adequate, well-trained workforce.

When promoting cybersecurity awareness and education for the public, NIST should fully utilize existing resources within the Federal government, private industry, academia, and independent organizations to minimize duplicative effort.

Cybersecurity University--Industry Task Force

In considering options for a collaborative model for carrying out cybersecurity research and development, it is the Committee's intention that the objective of such a potential entity would be to supplement, not supplant, the traditional functions and activities of the individual participating entities. Therefore, in developing guidelines in accordance with subsection (b)(2) of section 108, it is the Committee's expectation that the task force work to identify activities that (1) would address nationally significant challenges that advance common objectives; and (2) require collaboration that could not otherwise be reasonably addressed by individual entities acting independently.

NIST's checklist development and dissemination

The Committee believes that advancements of technology have presented an opportunity to evolve security checklists into automated auditing programs capable of verifying information security policy compliance, as well as the measurement and management of vulnerabilities. NIST's Security Content Automation Protocol program is an excellent example of a public-private partnership developing interoperable security specifications to automate the assessment, documentation, and reporting of information security requirements. The Committee also believes that NIST should be more proactive in disseminating checklists to other Federal agencies.

United States Federal Government representation

The Committee intends that NIST will develop an international cybersecurity technical standards engagement strategy, in coordination with relevant Federal agencies that: addresses the needs outlined in the Cyberspace Policy Review; accounts for the constant evolution and introduction of technology; and fosters technical cybersecurity standards that maintain security without interfering with the freedom of the internet. NIST will not dictate specific agency representation in international standards development, but should ensure that there is adequate United States government representation and coordination

for all appropriate development activities. Given the global nature of networked systems, it is imperative that the Federal government has a coordinated, comprehensive strategy to address international cybersecurity technical standards needs.

IX. COST ESTIMATE

A cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the *Congressional Budget Act of 1974* has been timely submitted to the Committee on Science and Technology prior to the filing of this report and is included in Section X of this report pursuant to House Rule XIII, clause 3(c)(3).

H.R. 4061 does not contain new budget authority, credit authority, or changes in revenues or tax expenditures. Assuming that the sums authorized under the bill are appropriated, H.R.4061 does authorize additional discretionary spending, as described in the Congressional Budget Office report on the bill, which is contained in Section X of this report.

	By fiscal year, in millions of dollars--					
	2010	2011	2012	2013	2014	2010-2014
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
NSF Cybersecurity Research Grants:						
Authorization Level	69	74	79	84	90	396
Estimated Outlays	9	41	61	71	79	261
NSF Cybersecurity Scholarships for Service:						
Authorization Level 1	4	20	22	23	25	94
Estimated Outlays	*	3	11	17	21	53
Other NSF Programs:						
Estimated Authorization Level	87	87	87	88	89	438
Estimated Outlays	9	49	70	81	86	295
Subtotal NSF Programs:						
Estimated Authorization Level	160	181	188	195	204	928
Estimated Outlays	18	93	142	169	186	609
NIST Programs:						
Estimated Authorization Level	6	6	6	6	6	30
Estimated Outlays	5	6	6	6	6	29
Cybersecurity Task Force:						
Estimated Authorization Level	*	*	*	*	*	1
Estimated Outlays	*	*	*	*	*	1
Total Changes under H.R. 4061:						
Estimated Authorization Level	166	187	194	201	210	959
Estimated Outlays	23	99	148	175	192	639