AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

111TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
111–405

CYBERSECURITY ENHANCEMENT ACT OF 2009

JANUARY 27, 2010.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GORDON of Tennessee, from the Committee on Science and Technology, submitted the following

R E P O R T

[To accompany H.R. 4061]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science and Technology, to whom was referred the bill (H.R. 4061) to advance cybersecurity research, development, and technical standards, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

		Page
I.	Bill	2
II.	Purpose of the Bill	9
III.	Background and Need for the Legislation	9
IV.	Hearing Summary	10
V.	Committee Actions	12
VI.	Summary of Major Provisions of the Bill	13
VII.	Section-by-Section Analysis	13
VIII.	Committee Views	15
IX.	Cost Estimate	17
X.	Congressional Budget Office Cost Estimate	17
XI.	Compliance with Public Law 104–4	19
XII.	Committee Oversight Findings and Recommendations	19
XIII.	Statement on General Performance Goals and Objectives	19
XIV.	Constitutional Authority Statement	19
XV.	Federal Advisory Committee Statement	20
XVI.	Congressional Accountability Act	20
XVII.	Earmark Identification	20
XVIII.	Statement on Preemption of State, Local, or Tribal Law	20
XIX.	Changes in Existing Law Made by the Bill, as Reported	20
XX.	Committee Recommendations	27
XXI.	Proceedings of the Subcommittee Markups	28
	a. Research and Science Education Subcommittee	28

89–006

b. Technology and Innovation Subcommittee 64
XXII. Proceedings of the Full Committee Markup 80

I. BILL

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.

X. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

H.R. 4061—Cybersecurity Enhancement Act of 2009

Summary: H.R. 4061 would reauthorize several National Science Foundation (NSF) programs that aim to enhance cybersecurity (the protection of computers and computer networks from unauthorized access). The bill also would require the National Institute of Standards and Technology (NIST) to establish a cybersecurity awareness program and implement standards for managing personal identifying information stored on computer systems. Finally, the bill

would establish a task force to recommend actions to improve cybersecurity research and development.

Based on information from NSF and NIST and assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 4061 would cost $639 million over the 2010–2014 period and $320 million after 2014. Enacting the legislation would not affect direct spending or revenues.

H.R. 4061 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated Cost to the Federal Government: The estimated budgetary impact of H.R. 4061 is shown in the following table. The costs of this legislation fall within budget function 250 (general science, space, and technology).

	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

[1] H.R. 4061 would authorize the appropriation of $19 million for NSF Cybersecurity Scholarships for Service in 2010. NSF has received an appropriation of $15 million for those scholarships for 2010. CBO expects that under the bill the agency could receive an additional appropriation of $4 million to fund those scholarships in 2010.

Note: NSF = National Science Foundation. NIST = National Institute of Standards and Technology.
* = less than $500,000. Amounts may not sum to totals because of rounding.

Basis of estimate: For this estimate, CBO assumes that H.R. 4061 will be enacted by the middle of calendar year 2010 and that the necessary amounts will be appropriated each fiscal year. Estimated outlays are based on historical spending patterns for similar NSF and NIST programs.

H.R. 4061 would authorize appropriations for several NSF grant programs aimed at enhancing cybersecurity. The bill would authorize appropriations totaling $396 million over the 2010–2014 period to improve research on cybersecurity. The bill also would authorize the appropriation of an additional $94 million over that period to provide scholarships to students who pursue higher education related to cybersecurity and commit to public service after graduating. Finally, the bill would authorize such sums as may be necessary for activities related to improving cybersecurity, including constructing research facilities and enhancing cybersecurity training for faculty and students at colleges and universities. Based on

information from NSF regarding the cost of conducting similar activities and assuming appropriation of the authorized and necessary amounts, CBO estimates that implementing the NSF programs authorized under the bill would cost $609 million over the 2010–2014 period and $319 million after 2014.

H.R. 4061 also would direct NIST to conduct a cybersecurity research program, establish standards and protocols to enhance cybersecurity, and to promote cybersecurity awareness and education. Based on information from NIST regarding the cost of conducting similar activities and assuming appropriation of the necessary amounts, CBO estimates that implementing those programs would cost $29 million over the 2010–2014 period and $1 million after 2014.

Finally, H.R. 4061 would establish a task force of academic and industry experts to advise the Office of Science and Technology Policy on issues related to cybersecurity. Based on information regarding the cost of funding similar activities, CBO estimates that carrying out this provision would cost $1 million over the 2010–2014 period.

Intergovernmental and private-sector impact: H.R. 4061 contains no intergovernmental or private-sector mandates as defined in UMRA. The bill would benefit public institutions of higher education by authorizing grants for research on computer security.

Estimate prepared by: Federal costs: Jeff LaFave; Impact on state, local, and tribal governments: Elizabeth Cove Delisle; Impact on the private sector: Amy Petz.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

XI. COMPLIANCE WITH PUBLIC LAW 104–4

H.R. 4061 contains no unfunded mandates.

XII. COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

The oversight findings and recommendations of the Committee on Science and Technology are reflected in the body of this report.

XIII. STATEMENT ON GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause (3)(c) of House rule XIII, the goals of H.R. 4061 are 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 and the National Institute of Standards and Technology.

XIV. CONSTITUTIONAL AUTHORITY STATEMENT

Article I, section 8 of the Constitution of the United States grants Congress the authority to enact H.R. 4061.

XV. FEDERAL ADVISORY COMMITTEE STATEMENT

The functions of the advisory committee authorized in H.R. 4061 are not currently being nor could they be performed by one or more agencies or by enlarging the mandate of another existing advisory committee.

XVI. CONGRESSIONAL ACCOUNTABILITY ACT

The Committee finds that H.R. 4061 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act (Public Law 104–1).

XVII. EARMARK IDENTIFICATION

H.R. 4061 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.

XVIII. STATEMENT ON PREEMPTION OF STATE, LOCAL, OR TRIBAL LAW

This bill is not intended to preempt any state, local, or tribal law.

XIX. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

* * * * * * *

SEC. 2. FINDINGS.

The Congress finds the following:

¿(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational 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—in a vast, interdependent physical and electronic network.

(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) ¿Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, *These advancements have significantly contributed to the growth of the United States economy* and the delivery of services critical to

the public welfare, but have also increased the consequences of temporary or prolonged failure.

¿(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure".

(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) 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.

¿(4) *(5)* Computer security technology and systems implementation lack—

(A) * * *

* * * * * * *

¿(5) *(6)* Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) * * *

* * * * * * *

¿(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

(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. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure *and usability* of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, *identity management,* and other secure data communications technology;

* * * * * * *

(H) remote access and wireless security; ¿and

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property¿. *; and*

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

* * * * * * *

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

¿(A) $35,000,000 for fiscal year 2003;
¿(B) $40,000,000 for fiscal year 2004;
¿(C) $46,000,000 for fiscal year 2005;
¿(D) $52,000,000 for fiscal year 2006; and
¿(E) $60,000,000 for fiscal year 2007.
(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.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) * * *

* * * * * * *

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) * * *

* * * * * * *

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; ¿and

(D) how the center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services¿. *; and*

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

* * * * * * *

¿(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

¿(A) $12,000,000 for fiscal year 2003;
¿(B) $24,000,000 for fiscal year 2004;
¿(C) $36,000,000 for fiscal year 2005;
¿(D) $36,000,000 for fiscal year 2006; and
¿(E) $36,000,000 for fiscal year 2007.

(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.

* * * * * * *

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) * * *

* * * * * * *

¿(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

¿(A) $15,000,000 for fiscal year 2003;

¿(B) $20,000,000 for fiscal year 2004;

¿(C) $20,000,000 for fiscal year 2005;

¿(D) $20,000,000 for fiscal year 2006; and

¿(E) $20,000,000 for fiscal year 2007.

(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.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) * * *

¿(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

¿(A) $1,000,000 for fiscal year 2003;

¿(B) $1,250,000 for fiscal year 2004;

¿(C) $1,250,000 for fiscal year 2005;

¿(D) $1,250,000 for fiscal year 2006; and

¿(E) $1,250,000 for fiscal year 2007.

(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.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) * * *

* * * * * * *

¿(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

¿(A) $10,000,000 for fiscal year 2003;

¿(B) $20,000,000 for fiscal year 2004;

¿(C) $20,000,000 for fiscal year 2005;

¿(D) $20,000,000 for fiscal year 2006; and

¿(E) $20,000,000 for fiscal year 2007.

(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.

* * * * * * *

¿(e) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—

¿(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

¿(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

¿(3) APPLICATION.—Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

¿(4) USE OF FUNDS.—Funds received by an institution of higher education under this paragraph shall—

¿(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

¿(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

¿(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

¿(5) REPAYMENT.—Each graduate traineeship shall—

¿(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

¿(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

¿(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

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

¿(7) ELIGIBILITY.—To be eligible to receive a graduate traineeship under this section, an individual shall—

¿(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States; and

¿(B) demonstrate a commitment to a career in higher education.

¿(8) CONSIDERATION.—In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent pos-

sible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

¿(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

(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. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) * * *

* * * * * * *

¿(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

¿(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections 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; EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the 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. The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology 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.

¿(3) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

¿(4) 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) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

¿(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

(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).

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. (a) * * *

* * * * * * *

(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.

¿(e) *(f)* As used in this section—

(1) * * *

* * * * * * *

XX. COMMITTEE RECOMMENDATIONS

On November 18, 2009, the Committee on Science and Technology favorably reported H.R. 4061 by voice vote and recommended its enactment.

XXI. a. PROCEEDINGS OF THE MARKUP BY THE SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION ON COMMITTEE PRINT, THE CYBERSECURITY RESEARCH AND DEVELOPMENT AMENDMENTS ACT OF 2009

WEDNESDAY, SEPTEMBER 23, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION,
COMMITTEE ON SCIENCE,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:09 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Daniel Lipinski [Chairman of the Subcommittee] presiding.

Chairman LIPINSKI. The Subcommittee will come to order.

Good morning. Pursuant to notice, the Subcommittee on Research and Science Education meets to consider the following measure: the Committee Print of the *Cybersecurity Research and Development Amendments Act of 2009*. We will now proceed to the markup.

This morning the Subcommittee will consider the Committee Print of the *Cybersecurity Research and Development Amendments Act of 2009*. The Subcommittee has held a series of hearings examining the state of cybersecurity R&D (Research and Development). At these hearings, witnesses emphasized the need to better coordinate and prioritize the federal R&D portfolio, to improve partnerships between the Federal Government and the private sector, and to train an IT workforce that can meet the growing needs of both the public and private sectors. Our witnesses also stressed that cybersecurity research needs to encompass all stages of hardware and software design, from project management to social and behavioral factors arising from human-computer interactions.

The legislation we are considering today addresses these concerns. First, it requires federal agencies to develop and implement a strategic plan for the federal cybersecurity R&D portfolio. The plan must be based on an assessment of cybersecurity risk, to make sure that taxpayer dollars fund the R&D needed to meet the strategic needs of our country and to keep Internet users safe from cybercrime. The strategic plan will contain a description of how the program will transfer technology from our national labs and universities to industry, and how our federal R&D objectives complement, rather than duplicate, R&D occurring in the private sec-

tor. In addition to developing a strategic plan informed by industry and academia, the bill establishes a university-industry task force to explore mechanisms and models for carrying out collaborative research in cybersecurity.

The legislation addresses cybersecurity workforce needs for the Federal Government, and for the Nation as a whole, by requiring an assessment of needs and providing scholarships and fellowships to students to pursue advanced degrees in cybersecurity-related fields.

Finally, the bill reauthorizes and expands the National Science Foundation's (NSF) Trustworthy Computing program, placing a new emphasis on research into the social and behavioral aspects of cybersecurity, an important area identified by our witnesses.

Cyber threats are constantly evolving and cybersecurity R&D must evolve in concert through a combination of near-term fixes and long-term projects that build a more secure foundation. The *Cybersecurity R&D Amendments Act* will ensure an overall vision and an implementation plan for the federal cybersecurity R&D portfolio, and will train the next generation of cybersecurity professionals.

I want to thank Members for their participation this morning, and I look forward to a productive markup.

With that, I will now recognize Dr. Ehlers to present his opening remarks.

[The prepared statement of Chairman Lipinski follows:]

PREPARED STATEMENT OF CHAIRMAN DANIEL LIPINSKI

This morning the Research and Science Education Subcommittee will consider the *Cybersecurity Research and Development Amendments Act of 2009.*

The Subcommittee has held a series of hearings examining the state of cybersecurity R&D. At these hearings witnesses emphasized the need to better coordinate and prioritize the federal R&D portfolio, improve partnerships between the Federal Government and the private sector, and train an IT workforce that can meet the growing needs of both the public and private sectors. Our witnesses also stressed that cybersecurity research needs to encompass all stages of hardware and software design, from project management to social and behavioral factors arising from human-computer interactions.

The legislation we are considering today addresses these concerns. First, it requires federal agencies to develop and implement a strategic plan for the federal cybersecurity R&D portfolio. The plan must be based on an assessment of cybersecurity risk, to make sure that taxpayer dollars fund the R&D needed to meet the strategic needs of our country and to keep Internet users safe from cybercrime. The strategic plan will also contain a description of how the program will transfer technology from our national labs and universities to industry, and how our federal R&D objectives complement, rather than duplicate, R&D occurring in the private sector.

In addition to developing a strategic plan informed by industry and academia, the bill establishes a university-industry task force to explore mechanisms and models for carrying out collaborative research in cybersecurity.

The legislation addresses cybersecurity workforce needs for the Federal Government, and for the Nation as a whole, by requiring an assessment of needs and providing scholarships and fellowships to students to pursue advanced degrees in cybersecurity-related fields.

Finally, the bill reauthorizes and expands NSF's Trustworthy Computing program, placing a new emphasis on research into the social and behavioral aspects of cybersecurity, an important area identified by our witnesses.

Cyber threats are constantly evolving and cybersecurity R&D must evolve in concert through a combination of near-term fixes and long-term projects that build a more secure foundation. The *Cybersecurity R&D Amendments Act* will ensure an overall vision and an implementation plan for the federal cybersecurity R&D portfolio and will train the next generation of cybersecurity professionals.

I want to thank Members for their participation this morning and I look forward to a productive markup.

Mr. EHLERS. Thank you, Mr. Chairman. Today we are examining legislation to reauthorize the *Cybersecurity Research and Development Act.* With the rapid evolution of information technology fields, it is critical that we adopt policies that keep us ahead of impending cyber threats.

This subcommittee has held a series of hearings this year focused on the state of federal cybersecurity research and development. The testimonies we received from industry experts and federal agency officials all pointed to a serious lack of coordination in our cybersecurity strategies. Building on the information we have gleaned, I am hopeful this legislation will effectively refine our efforts by establishing a strategic research and development plan and roadmap. As an educator, I am particularly interested in how we will further support the education and training of students in this rapidly changing field. Consequently, I am pleased that the draft legislation codifies a scholarship program at the National Science Foundation to promote undergraduate and graduate degrees in cybersecurity fields.

I personally did not realize how important this was until I met a year ago with a professor of computer science in which he pointed out the declining enrollments of students in computer science and the decline has been going on for several years to the point that there is a severe shortage of computer scientists, and obviously if you are going to deal with cybersecurity, you have to not only be a computer scientist but a very bright computer scientist, so I am very pleased with the National Science Foundation program established in this legislation.

As we become more dependent on virtual information and services, security becomes more difficult to manage. Attaining and maintaining a safe and trustworthy information technology and communications infrastructure is imperative and we must not forget that it is an ongoing challenge. I look forward to refining and promoting this legislation as it moves through the legislative process.

I would like to add a note here also regarding cybersecurity. I do not claim to be an expert in the field but some years ago I was on a NATO taskforce studying the issue and I ended up being assigned the task of writing a report. It was astounding to me to recognize how vulnerable we were to cybersecurity attacks and also how ill prepared we were to deal with the problem. We have made some progress since that time but we have quite a ways to go, and it is down right frightening to recognize what damage can be done through cybersecurity attacks. So I am very pleased to support this bill and to participate in bringing it to the House. With that, I yield back.

[The prepared statement of Mr. Ehlers follows:]

PREPARED STATEMENT OF REPRESENTATIVE VERNON J. EHLERS

Today we are examining legislation to reauthorize the *Cybersecurity Research and Development Act.* With the rapid evolution of information technology fields, it is critical that we adopt policies that keep us ahead of impending cyber threats.

This subcommittee has held a series of hearings this year focused on the state of federal cybersecurity research and development. The testimonies we received

from industry experts and federal agency officials all pointed to a serious lack of coordination in our cybersecurity strategies. Building on the information we have gleaned, I am hopeful this legislation will effectively refine our efforts by establishing a strategic research and development plan and roadmap. As an educator, I am particularly interested in how we will further support the education and training of students in this rapidly changing field. Consequently, I am pleased that the draft legislation codifies a scholarship program at the National Science Foundation to promote undergraduate and graduate degrees in cybersecurity fields.

As we become more dependent on virtual information and services, security becomes more difficult to manage. Attaining and maintaining a safe and trustworthy information technology and communications infrastructure is imperative, and we must not forget that it is an ongoing challenge. I look forward to refining and promoting this legislation as it moves through the legislative process.

Chairman LIPINSKI. Thank you, Dr. Ehlers. I think at every hearing and markup we learn more and more of the expertise that you do have in a lot of different areas in science and technology. We appreciate your contributions, and certainly we know with everything that is now available, everything that is done electronically, cyber attacks are more and more of a security issue, so that is why it is so important we move forward with legislation.

Does anyone else wish to be recognized?

With that, we will move on to the markup. I ask unanimous consent that the Committee Print is considered as read and open to amendment at any point and that the Members proceed with the amendments in the order of the roster. Without objection, so ordered.

The first amendment on the roster is a Manager's Amendment offered by the Chair. The Clerk will report the amendment.

The CLERK. Amendment to the Committee Print, amendment number 042, offered by Mr. Lipinski of Illinois.

Chairman LIPINSKI. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize myself for five minutes to explain the amendment.

This amendment makes technical corrections to the Committee Print, including language for the reauthorization of NSF Cybersecurity Research Centers program for fiscal years 2010 through 2014. It also clarifies 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, and I urge my colleagues to support this amendment.

Is there any further discussion on the amendment?

Mr. EHLERS. Mr. Chairman, I support the amendment and urge that we adopt it.

Chairman LIPINSKI. Thank you, Dr. Ehlers. Any other discussion on the amendment? If no, the vote will occur on the amendment. All in favor, say aye. Those opposed, say no. The ayes have it and the amendment is agreed to.

The second amendment on the roster is an amendment offered by the gentlelady from Texas, Ms. Johnson. Are you ready to proceed with your amendment?

Ms. JOHNSON. Yes, Mr. Chairman, I have an amendment at the desk.

Chairman LIPINSKI. The Clerk will report the amendment.

The CLERK. Amendment to the Committee Print, amendment number 084, offered by Ms. Eddie Bernice Johnson of Texas.

Chairman LIPINSKI. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentlelady for five minutes to explain the amendment.

Ms. JOHNSON. Thank you very much, Mr. Chairman, and our Ranking Member and fellow Member of the Subcommittee.

My amendment to the *Cybersecurity Research and Development Amendments Act of 2009* contains several changes to the legislation. All changes are intended to make this initiative more inclusive to under-represented minorities.

This week, the Congressional Black Caucus is busy with meetings, panel discussions, briefings and other events that are part of the annual legislative conference. As a matter of fact, I am hosting my 17th Science and Technology Brain Trust. It will be held at the Washington Conventional Center and on Capitol Hill. A wide variety of discussions are occurring this week on policies that are of interest to the African-American community and to the broader policy community. The CBC Foundation is the host, and the Science and Technology Brain Trust is Friday at 9:00 a.m. in Room 143A, if anyone is willing. Mr. Norm Augustine will be there as well as several other panelists. At this free event that is open to the public, we will be discussing models of education excellence, and this would be one of the things that we would continue to emphasize—that is, more diversity.

Along these lines, programs such as the Federal Scholarship For Service program as well as the research program can do much to engage under-represented minorities in the area of computer science. My amendment affects four parts of the bill. First, it states that the Cybersecurity Strategic Research and Development Plan should include a description of how the research program will include women and minorities to help to foster a more diverse workforce in this area. Secondly, my amendment says that in developing the plan, the agencies involved shall seek advice from minority-serving institutions in addition to stakeholders in the industry, academia and other relevant organizations, and third, it addresses the Federal Scholarship For Service program which seeks to recruit and train the next generation of federal cybersecurity professionals and increase the capacity of the higher education system in training such a workforce. The bill states that merit review grants will support several different activities to increase the capacity of colleges and universities to train such individuals. My amendment states that one of those activities in support of institutional partnerships—especially including minority-serving institutions, because these institutions historically receive a disproportionately small share of federal research and education funding—more should be done to help them.

And finally, my amendment addresses the selection process for the Cyber Scholarship For Service program. Scholarship awards will reflect the goal of promoting broader participation in under-represented minorities, and Mr. Chairman, I understand that you will support these changes and I want to express my gratitude for your partnership in this endeavor. We really must be proactive to devise federal policies and programs that promote inclusiveness of diverse groups.

House Concurrent Resolution 53 that I introduced this March celebrates the strides that Latin-American and African-American students have made in terms of educational attainment in computer science. In 2006, African-Americans made up 12.4 percent of the candidates receiving computer science degrees, a portion almost equal to that representation in the United States population, which is 12.8 percent. This good news can be examined in more detail in an article published by the National Society of Black Engineers called *Blacks and Computer Science: The Secrets of Their Success.* The progress has been slow, Mr. Chairman, but I believe that we are making a difference, and I want to thank you again for your support, and I urge my colleagues to support this amendment also, and I yield back the remainder of time. Thank you.

Chairman LIPINSKI. Thank you, Ms. Johnson.

Is there any further discussion of this amendment? Dr. Ehlers.

Mr. EHLERS. Mr. Chairman, I support the amendment and urge its adoption.

Chairman LIPINSKI. Thank you, Dr. Ehlers.

Any further discussion on the amendment? I thank the gentlelady for her amendment, which I support, and thank the gentlelady for her work on this issue. Seeing as there is no further discussion, the vote will occur on the amendment. All those in favor, say aye. Those opposed, say no. The ayes have it and the amendment is agreed to.

Are there any other amendments? If no, then the vote is on the Committee Print as amended. All those in favor will say aye. All those opposed will say no. In the opinion of the Chair, the ayes have it.

I recognize myself to offer a motion. I move that the Subcommittee favorably report the Committee Print as amended to the Full Committee. Furthermore, I move that staff be instructed to prepare the Subcommittee report and make necessary technical and conforming change to the Committee Print in accordance with the recommendations of the Subcommittee.

The question is on the motion to report the Committee Print favorably. Those in favor of the motion will signify by saying aye. Opposed, no. The ayes have it and the print is favorably reported.

Without objection, the motion to reconsider is laid upon the table. Members will have two subsequent calendar days in which to submit supplemental Minority or additional views on the measure. I want to thank all the Members for their attendance. It was a very quick markup but a very critical, important issue and I look forward to working with all of you as we move forward on this.

This concludes our Subcommittee markup.

[Whereupon, at 10:24 a.m., the Subcommittee was adjourned.]

Appendix:

COMMITTEE PRINT, SECTION-BY-SECTION ANALYSIS, AMENDMENT ROSTER

[COMMITTEE PRINT]

SEPTEMBER 18, 2009

111TH CONGRESS
1ST SESSION

H. R. _____

To authorize activities for support of cybersecurity research and development and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M . introduced the following bill; which was referred to the Committee on

---

A BILL

To authorize activities for support of cybersecurity research and development and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Research and Development Amendments Act of 2009".

SEC. 2. DEFINITIONS.

In this Act:

(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. 3. 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

1 necessary to address the long-term challenge of en-
2 suring a secure and reliable information technology
3 and communications infrastructure.''; and
4 (6) by amending paragraph (7), as so redesig-
5 nated by paragraph (4) of this section, to read as
6 follows:
7 ''(7) While African-Americans, Hispanics, and
8 Native Americans constitute 33 percent of the col-
9 lege-age population, members of these minorities
10 comprise less than 20 percent of bachelor degree re-
11 cipients in the field of computer sciences.''.

12 **SEC. 4. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
13 **VELOPMENT PLAN.**

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

1 tems. Once every 3 years after the initial strategic plan
2 is transmitted to Congress under this section, such agen-
3 cies shall prepare and transmit to Congress an update of
4 such plan.

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

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

15 (2) describe how the Program will focus on in-
16 novative, transformational technologies with the po-
17 tential to enhance the security, reliability, resilience,
18 and trustworthiness of the digital infrastructure;

19 (3) describe how the Program will foster the
20 transfer of research and development results into
21 new cybersecurity technologies and applications for
22 the benefit of society and the national interest, in-
23 cluding through the dissemination of best practices
24 and other outreach activities;

1 (4) describe how the Program will establish and
2 maintain a national research infrastructure for cre-
3 ating, testing, and evaluating the next generation of
4 secure networking and information technology sys-
5 tems; and
6 (5) describe how the Program will facilitate ac-
7 cess by academic researchers to the infrastructure
8 described in paragraph (4), as well as to event data.
9 (c) DEVELOPMENT OF ROADMAP.—The agencies de-
10 scribed in subsection (a) shall develop and annually update
11 an implementation roadmap for the strategic plan re-
12 quired in this section. Such roadmap shall—
13 (1) specify the role of each Federal agency in
14 carrying out or sponsoring research and development
15 to meet the research objectives of the strategic plan,
16 including a description of how progress toward the
17 research objectives will be evaluated;
18 (2) specify the funding allocated to each major
19 research objective of the strategic plan and the
20 source of funding by agency for the current fiscal
21 year; and
22 (3) estimate the funding required for each
23 major research objective of the strategic plan for the
24 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, 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. 5. 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. 6. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a) 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.".

1 (c) COMPUTER AND NETWORK SECURITY RESEARCH
2 CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b))
3 is amended—
4 (1) in paragraph (4)—
5 (A) in subparagraph (C), by inserting
6 ''and'' after the semicolon;
7 (B) in subparagraph (D), by striking the
8 period and inserting ''; and''; and
9 (C) by striking subparagraph (D); and
10 (2) by adding at the end the following new sub-
11 paragraph:''.
12 ''(E) how the center will partner with gov-
13 ernment laboratories, for-profit entities, other
14 institutions of higher education, or nonprofit re-
15 search institutions.''.
16 (c) COMPUTER AND NETWORK SECURITY CAPACITY
17 BUILDING GRANTS.—Section 5(a)(6) of such Act (15
18 U.S.C. 7404(a)(6)) is amended to read as follows:
19 ''(6) AUTHORIZATION OF APPROPRIATIONS.—
20 The are authorized to be appropriated to the Na-
21 tional Science Foundation such sums as are nec-
22 essary to carry out this subsection for each of the
23 fiscal years 2010 through 2014.''.

1 (d) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
2 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
3 7404(b)(2)) is amended to read as follows:
4 "(2) AUTHORIZATION OF APPROPRIATIONS.—
5 The 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 (e) GRADUATE TRAINEESHIPS IN COMPUTER AND
10 NETWORK SECURITY.—Section 5(c)(7) of such Act (15
11 U.S.C. 7404(c)(7)) is amended to read as follows:
12 "(7) AUTHORIZATION OF APPROPRIATIONS.—
13 The 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 (f) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CY-
18 BERSECURITY.—Section 5(e) of such Act (15 U.S.C.
19 7404(e)) is amended to read as follows:
20 "(e) POSTDOCTORAL RESEARCH FELLOWSHIPS IN
21 CYBERSECURITY.—
22 "(1) IN GENERAL.—The Director shall carry
23 out a program to encourage young scientists and en-
24 gineers to conduct postdoctoral research in the fields
25 of cybersecurity and information assurance, includ-

1 ing the research areas described in section 4(a)(1),
2 through the award of competitive, merit-reviewed fel-
3 lowships.
4 "(2) AUTHORIZATION OF APPROPRIATIONS.—
5 The 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 **SEC. 7. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PRO-**
10 **GRAM.**

11 (a) IN GENERAL.—The Director of the National
12 Science Foundation shall carry out a Scholarship for Serv-
13 ice program to recruit and train the next generation of
14 Federal cybersecurity professionals and to increase the ca-
15 pacity of the higher education system to produce a tech-
16 nology workforce with the skills necessary to enhance the
17 security of the Nation's communications and information
18 infrastructure.
19 (b) CHARACTERISTICS OF PROGRAM.—The program
20 under this section shall—
21 (1) provide, through qualified institutions of
22 higher education, scholarships that provide tuition,
23 fees, and a competitive stipend for up to 3 years to
24 students pursuing undergraduate and graduate de-
25 grees in cybersecurity fields;

1 (2) provide the scholarship recipients with sum-
2 mer internship opportunities or other meaningful
3 temporary appointments in the Federal information
4 technology workforce; and
5 (3) increase the capacity of institutions of high-
6 er education to produce highly qualified cybersecu-
7 rity professionals, through the award of competitive,
8 merit-reviewed grants that support such activities
9 as—
10 (A) faculty professional development, in-
11 cluding technical, hands-on experiences in the
12 private sector or government, workshops, semi-
13 nars, conferences, and other professional devel-
14 opment opportunities that will result in im-
15 proved instructional capabilities;
16 (B) institutional partnerships; and
17 (C) development of cybersecurity-related
18 courses and curricula.
19 (c) SCHOLARSHIP REQUIREMENTS.—
20 (1) ELIGIBILITY.—Scholarships under this sec-
21 tion shall be available only to students who—
22 (A) are citizens or permanent residents of
23 the United States; and
24 (B) are full-time students in an eligible de-
25 gree program, as determined by the Director,

1 that is focused on computer security or infor-
2 mation assurance at an awardee institution.
3 (2) SELECTION.—Individuals shall be selected
4 to receive scholarships primarily on the basis of aca-
5 demic merit, with consideration given to financial
6 need.
7 (3) SERVICE OBLIGATION.—If an individual re-
8 ceives a scholarship under this section, as a condi-
9 tion of receiving such scholarship, the individual
10 upon completion of their degree must serve as a cy-
11 bersecurity professional within the Federal workforce
12 for a period of time equal to the length of the schol-
13 arship. If a scholarship recipient is not offered em-
14 ployment by a Federal agency, the service require-
15 ment can be satisfied by —
16 (A) serving as a cybersecurity professional
17 in a State or local government agency; or
18 (B) teaching cybersecurity courses at an
19 institution of higher education.
20 (d) FAILURE TO COMPLETE SERVICE OBLIGATION.—
21 (1) GENERAL RULE.—If an individual who has
22 received a scholarship under this section—
23 (A) fails to maintain an acceptable level of
24 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.—A qualified institution of higher education receiving a grant under this section shall, as a condition of participating in the program, enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their respective service requirements.

(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

1 service obligation under this section, the total
2 amount of awards received by the individual
3 under this section shall be repaid or such
4 amount shall be treated as a loan to be repaid
5 in accordance with subparagraph (C).

6 (B) MORE THAN ONE YEAR OF SERVICE.—
7 If a circumstance described in subparagraph
8 (D) or (E) of paragraph (1) occurs after the
9 completion of 1 year of a service obligation
10 under this section, the total amount of scholar-
11 ship awards received by the individual under
12 this section, reduced by the ratio of the number
13 of years of service completed divided by the
14 number of years of service required, shall be re-
15 paid or such amount shall be treated as a loan
16 to be repaid in accordance with subparagraph
17 (C).

18 (C) REPAYMENTS.—A loan described in
19 subparagraph (A) or (B) shall be treated as a
20 Federal Direct Unsubsidized Stafford Loan
21 under part D of title IV of the Higher Edu-
22 cation Act of 1965 (20 U.S.C. 1087a and fol-
23 lowing), and shall be subject to repayment, to-
24 gether with interest thereon accruing from the
25 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

1 any repayment the institution collects under
2 this paragraph to defray administrative costs
3 associated with the collection. The Director
4 shall establish a single, fixed percentage that
5 will apply to all eligible entities.
6 (5) EXCEPTIONS.—The Director may provide
7 for the partial or total waiver or suspension of any
8 service or payment obligation by an individual under
9 this section whenever compliance by the individual
10 with the obligation is impossible or would involve ex-
11 treme hardship to the individual, or if enforcement
12 of such obligation with respect to the individual
13 would be unconscionable.
14 (e) HIRING AUTHORITY.—For purposes of any law
15 or regulation governing the appointment of individuals in
16 the Federal civil service, upon successful completion of
17 their degree, students receiving a scholarship under this
18 section shall be hired under the authority provided for in
19 section 213.3102(r) of title 5, Code of Federal Regula-
20 tions, and be exempted from competitive service. Upon ful-
21 fillment of the service term, such individuals shall be con-
22 verted to a competitive service position without competi-
23 tion if the individual meets the requirements for that posi-
24 tion.

1 (f) AUTHORIZATION OF APPROPRIATIONS.—There
2 are authorized to appropriated to the National Science
3 Foundation to carry out this section—
4 (1) $18,700,000 for fiscal year 2010;
5 (2) $20,100,000 for fiscal year 2011;
6 (3) $21,600,000 for fiscal year 2012;
7 (4) $23,300,000 for fiscal year 2013; and
8 (5) $25,000,000 for fiscal year 2014.

9 **SEC. 8. CYBERSECURITY WORKFORCE ASSESSMENT.**

10 Not later than 180 days after the date of enactment
11 of this Act the President shall transmit to the Congress
12 a report addressing the cybersecurity workforce needs of
13 the Federal Government. The report shall include—
14 (1) an examination of the current state of and
15 the projected needs of the Federal cybersecurity
16 workforce, including a comparison of the different
17 agencies and departments, and an analysis of the ca-
18 pacity of such agencies and departments to meet
19 those needs;
20 (2) an analysis of the sources and availability of
21 cybersecurity talent, including a comparison of the
22 Federal Government's needs with the cybersecurity
23 skills and expertise sought by the private sector; and
24 (3) an analysis of any barriers to the Federal
25 Government recruiting and hiring cybersecurity tal-

ent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities, along with recommendations to overcome identified barriers.

SEC. 9. 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 fo-

1 cused on nationally significant challenges and requir-
2 ing collaboration;
3 (3) define the roles and responsibilities for the
4 participants from institutions of higher education
5 and industry in such entity;
6 (4) propose guidelines for assigning intellectual
7 property rights and for the transfer of research and
8 development results to the private sector; and
9 (5) make recommendations for how such entity
10 could be funded from Federal, State, and nongovern-
11 mental sources.
12 (c) COMPOSITION.—In establishing the task force
13 under subsection (a), the Director of the Office of Science
14 and Technology Policy shall appoint an equal number of
15 individuals from institutions of higher education and from
16 industry with knowledge and expertise in cybersecurity.
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.

SECTION-BY-SECTION ANALYSIS OF CYBERSECURITY RESEARCH AND DEVELOPMENT AMENDMENTS ACT OF 2009

SECTION 1. SHORT TITLE.

Cybersecurity Research and Development Amendments Act of 2009

SECTION 2. DEFINITIONS

Defines terms used in this Act.

SECTION 3. FINDINGS

Describes findings of this Act.

SECTION 4. 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, it 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.

SECTION 5. 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 their total cybersecurity research portfolio.

SECTION 6. 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.

SECTION 7. 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.

SECTION 8. CYBERSECURITY WORKFORCE ASSESSMENT

Requires the President to issue a report assessing the current and future cybersecurity workforce needs of the Federal Government, including comparison of the skills needed by each federal agency, the supply of cybersecurity talent, and any barriers to the recruitment and hiring of cybersecurity professionals.

SECTION 9. 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.

COMMITTEE ON SCIENCE AND TECHNOLOGY
RESEARCH AND SCIENCE EDUCATION
SUBCOMMITTEE MARKUP
SEPTEMBER 23, 2009

AMENDMENT ROSTER

Committee Print, the *Cybersecurity Research and Development Amendments Act of 2009*

No.	Sponsor	Description	Results
1	Mr. Lipinski (Manager's Amendment)	Makes clarifying and technical changes. Amends Section 6 ("National Science Foundation Cybersecurity Research and Development Programs") to add an authorization of appropriations for such sums as are necessary for the Computer and Network Security Research Centers program for Fiscal Year 2010 through Fiscal Year 2014. Amends Section 7 ("Federal Cyber Scholarship for Service Program") to add "accept the terms of a scholarships pursuant to this section" as a new eligibility requirement for a scholarship. Amends Section 7 ("Federal Cyber Scholarship for Service Program") to add a new subsection entitled "Conditions of Support" which requires scholarship recipients to agree to provide the awardee institution with annual verifiable documentation of employment and up-to-date contact information as a condition of acceptance of a scholarship; also adds language to the subsection entitled "Monitoring Compliance" to clarify that an institution of higher education receiving a grant must provide to the Director of the National Science Foundation post-award employment information for scholarship recipients, on an annual basis, through the completion of recipient's service obligation. Amends Section 8 ("Cybersecurity Workforce Assessment") to require that the	Agreed to by voice vote.

		report include recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.	
2	Ms. Johnson	Amends Section 4 ("Cybersecurity Strategic Research and Development Plan") to add "describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act to foster a more diverse workforce" as an item that must be included in the strategic plan. Amends Section 4 ("Cybersecurity Strategic Research and Development Plan") to specify that academia that must be consulted in developing and updating the strategic plan includes "representatives of minority serving institutions". Amends Section 7 ("Federal Cyber Scholarship for Service Program") to specify that the institutional partnerships that may be supported through grants includes "minority serving institutions". Amends Section 7 ("Federal Cyber Scholarship for Service Program") to specify that consideration must be given to the "goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act" in selecting individuals to receive scholarships.	Agreed to by voice vote.

AMENDMENT TO THE COMMITTEE PRINT OFFERED BY MR. LIPINSKI OF ILLINOIS

Page, 3, line 22, insert a comma after "in 2009".

Page 9, line 9, strike "and".

Page 9, line 15, strike the period following the closing quotation mark and insert "; and".

Page 9, after line 15, insert the following new paragraph:

1 (3) by amending paragraph (7) to read as fol-
2 lows:
3 "(7) AUTHORIZATION OF APPROPRIATIONS.—
4 There are authorized to be appropriated to the Na-
5 tional Science Foundation such sums as are nec-
6 essary to carry out this subsection for each of the
7 fiscal years 2010 through 2014.".

Page 9, line 20, strike "The are" and insert "There are".

Page 10, line 5, strike "The are" and insert "There are".

Page 10, line 13, strike "The are" and insert "There are".

Page 11, line 2, strike "merit-reviewed" and insert "merit-based".

Page 11, line 5, strike "The are" and insert "There are".

Page 11, lines 15 and 16, strike "a technology" and insert "an information technology".

Page 12, line 23, strike "and".

Page 13, line 2, strike the period and insert "; and".

Page 13, after line 2, insert the following new subparagraph:

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

Page 13, after line 19, insert the following new paragraph:

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

Page 14, lines 15 through 21, amend paragraph (2) to read as follows:

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 (c)(4) for scholarship
12 recipients through the completion of their serv-
13 ice obligation.

Page 18, lines 22 and 23, strike ''Federal Government's needs with the cybersecurity skills and expertise sought by'' and insert ''cybersecurity skills and expertise sought by the Federal Government and''.

Page 18, line 23, strike ''and'' at the end of paragraph (2).

Page 19, lines 3 and 4, strike '', along with recommendations to overcome identified barriers.'' and insert ''; and''.

Page 19, after line 4, insert the following new paragraph:

1 (4) recommendations for Federal policies to en-
2 sure an adequate, well-trained Federal cybersecurity
3 workforce.

☒

AMENDMENT TO THE COMMITTEE PRINT OFFERED BY MS. EDDIE BERNICE JOHNSON OF TEXAS

Page 6, line 5, strike "and".

Page 6, line 8, strike the period and insert "; and".

Page 6, after line 8, insert the following new paragraph:

1 (6) describe how the Program will engage fe-
2 males and individuals identified in section 33 or 34
3 of the Science and Engineering Equal Opportunities
4 Act (42 U.S.C. 1885a or 1885b) to foster a more di-
5 verse workforce in this area.

Page 7, line 8, insert "including representatives of minority serving institutions," after " "academia,".

Page 12, line 16, insert ", including minority serving institutions" after "institutional partnerships".

Page 13, line 6, insert "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)" after "need".

XXI. b. PROCEEDINGS OF THE MARKUP BY THE SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION ON THE COMMITTEE PRINT, THE CYBERSECURITY COORDINATION AND AWARENESS ACT

WEDNESDAY, NOVEMBER 4, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,
COMMITTEE ON SCIENCE,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:44 a.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

Chairman WU. Pursuant to notice, the Subcommittee on Technology and Innovation meets this morning to consider the Committee Print, the *Cybersecurity Coordination and Awareness Act.* I recognize myself for five minutes.

The Committee Print implements recommendations made in the Cybersecurity Policy Review, which was completed in May of this year in the recent Subcommittee hearing, and also amends the *Cybersecurity Research and Development Act of 2002.*

Twenty-two years ago, this committee paved the way for federal cybersecurity efforts with the *Computer Security Act of 1987,* which charged NIST with developing technical standards to protect non-classified information on federal computer systems and was the first of 13 major laws relating to cybersecurity. The Cyberspace Policy Review recommended coordination of U.S. Government representation in international cybersecurity technical standards development. Currently, responsibilities are parsed among different agencies without any consistent policy. The convergence of telecommunication, the Internet, and video devices requires a corresponding convergence in cybersecurity technical standards development. A coordinated policy will ensure that these representatives operate with the overarching need of the U.S. infrastructure in mind. Two weeks ago, witnesses testified in front of this Subcommittee that NIST is suited for the role of coordinator due to its extensive technical expertise, established relationships with international bodies, and its existence as a non-regulatory body.

The Cyberspace Policy Review also called for a cybersecurity awareness and education campaign. NIST could be a valuable resource to all Internet users in providing them with the same guidance as it gives federal agencies. This committee print tasks NIST

with developing a plan to disseminate cybersecurity technical standards and best practices to the general public. However, while NIST is a great resource for technical standards and best practices, witnesses have stated that NIST guidance is often too technical for the average Internet user. Therefore, the print also tasks NIST with making its standards and best practices usable by those with less technical expertise. The dissemination of more user-friendly standards will help raise the base level of cybersecurity knowledge among individuals, business, educational institutions and governments.

The Cyberspace Policy Review also notes that cybersecurity cannot be improved without first improving identity management. The Committee Print also amends the *Cybersecurity R&D Act of 2002* to reinforce the important R&D work currently done by NIST that specifically reflects witness testimony on the importance of NIST work automated security specifications such as those in the S–CAP program. We also update language in the Act to reflect more-modern technological terms.

I urge my colleagues to support this bill and look forward to working with Members on both sides of the aisle to improve this legislation as we move forward.

Now I recognize Mr. Smith to present his opening remarks.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

Good afternoon. Today the Subcommittee will consider a committee print, the *Cybersecurity Coordination and Awareness Act*. This committee print implements recommendations made in the Cyberspace Policy Review and the recent Subcommittee hearing, and also amends the *Cybersecurity Research and Development Act of 2002*.

Twenty-two years ago, this committee paved the way for federal cybersecurity efforts with the *Computer Security Act of 1987*, which charged NIST with developing technical standards to protect non-classified information on federal computer systems and was the first of 13 major laws related to cybersecurity.

The Cyberspace Policy Review recommended coordination of U.S. Government representation in international cybersecurity technical standards development. Currently, responsibilities are parsed among different agencies without any consistent policy. The convergence of telecommunication, Internet, and video devices requires a corresponding convergence in cybersecurity technical standards development. A coordinated policy will ensure that these representatives operate with the overarching need of the U.S. infrastructure in mind. Two weeks ago, witnesses testified in front of this subcommittee that NIST is suited for the role of coordinator due to its extensive technical expertise, established relationships with international bodies, and existence as a non-regulatory body.

The Cyberspace Policy Review also called for a cybersecurity awareness and education campaign. NIST could be a valuable resource to all Internet users in providing them with the same guidance as it gives federal agencies. The Committee Print tasks NIST with developing a plan to disseminate cybersecurity technical standards and best practices to the general public. However, while NIST is a great resource for technical standards and best practices, witnesses have stated that NIST guidance is often too technical for the average Internet user. Therefore, the print also tasks NIST with making its standards and best practices usable by those with less technical expertise. The dissemination of more user-friendly standards will help raise the base level of cybersecurity knowledge among individuals, business, education, and government.

The Cyberspace Policy Review also states that cybersecurity cannot be improved without first improving identity management. NIST currently performs work on identity management systems such as biometrics, but this print will task NIST with improving the inter-operability of these systems to encourage more widespread use. By focusing on the usability and privacy aspects of identity management, this committee print will ensure that biometric and other systems will be accepted by the

public because they will have confidence in the security of their personal information.

The Committee Print also amends the *Cybersecurity R&D Act of 2002* to reinforce the important R&D work currently done by NIST and specifically reflects witness testimony on the importance of NIST's work with automated security specifications, such as those in the S–CAP program. The amendment will also update language in the Act to reflect more modern technological terms.

Mr. SMITH. Mr. Chairman, thank you for calling this markup this morning of the *Cybersecurity Coordination and Awareness Act.* The Committee print we are marking up makes a number of modest but important changes to NIST's information security programs and authorities.

Throughout the summer and into the fall, the Subcommittee held numerous hearings in which we heard from federal agencies and leading private-sector experts regarding the current state of computer and network security efforts and how they can be improved. These discussions made clear any successful comprehensive effort to improve cybersecurity must include NIST. From its critical capabilities and expertise in research and development and in standards development to its reputation as a proven and trusted entity within the Federal Government, the private sector and internationally, NIST is well suited to take on this expanded role in this arena.

This legislation will help to do just that by authorizing new or expanded activities in three areas: one, coordination of U.S. Government representation in international standards development forums; two, improve dissemination of cybersecurity best practices to small businesses, State and local governments, educational institutions and the general public; and three, research and standards development in identity management.

Identity management is a particularly important area which warrants increased attention, especially as it relates to the security and management of personally identifiable information now a common aspect of our computer systems. To this end, I appreciate the Chairman's willingness to work with me to refine this section and incorporate language explicitly stating privacy protection, including privacy as it relates to health IT systems, should be part of NIST's identity management efforts.

Together, the provisions of this Committee Print will strengthen and clarify NIST's cybersecurity roles and responsibilities representing a small but important step in our efforts to address cybersecurity issues.

I want to thank the Chairman for working closely with Republicans on this legislation. I certainly look forward to continued cooperative efforts as we move forward to consideration by Full Committee and on the Floor. Thank you.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Mr. Chairman, thank you for calling this markup this morning of the *Cybersecurity Coordination and Awareness Act.* The Committee Print we are marking up makes a number of modest but important changes to NIST's information security programs and authorities.

Throughout the summer and into the fall, the Subcommittee held numerous hearings in which we heard from federal agencies and leading private sector experts regarding the current state of computer and network security efforts and how they could be improved.

These discussions made clear any successful, comprehensive effort to improve cybersecurity must include NIST. From its critical capabilities and expertise in research and standards development, to its reputation as a proven and trusted entity within the Federal Government, the private sector, and internationally, NIST is well-suited to take on an expanded role in this area.

This legislation will help to do just that by authorizing new or expanded activities in three areas: (1) coordination of U.S. Government representation in international standards development forums; (2) improved dissemination of cybersecurity best practices to small businesses, State and local governments, educational institutions, and the general public; and (3) research and standards development in identity management.

Identity management is a particularly important area which warrants increased attention, especially as it relates to the security and management of pe4rsonallyt identifiable information now a common aspect of our computer systems. To this end, I appreciate the Chairman's willingness to work with me to refine this section and incorporate language explicitly stating privacy protection—including privacy as it relates to health IT systems—should be part of NIST's identity management efforts.

Together, the provisions in this committee print will strengthen and clarify NIST's cybersecurity roles and responsibilities, representing a small but important step in our efforts to address cybersecurity issues.

I want to thank the Chairman for working closely with Republicans on this legislation, and I look forward to continued cooperative efforts as we move to consideration in Full Committee and on the Floor.

Chairman WU. Thank you, Mr. Smith. It is indeed positive and refreshing to find these bipartisan issues and efforts and look forward to working with you going forward.

Does anyone else wish to be recognized? Hearing none, I ask unanimous consent that the Print is considered as read and open to amendment at any point and that the Members proceed with amendments in the order of the roster. Without objection, so ordered.

The first amendment on the roster is an Manager's Amendment offered by the Chair. The Clerk will report the amendment.

The CLERK. Amendment number 026, amendment to the Committee print, offered by Mr. Wu of Oregon and Mr. Smith of Nebraska.

Chairman WU. I ask unanimous consent to dispense with the reading. Without objection, so ordered. I recognize myself for five minutes to explain the amendment.

This manager's amendment includes two simple provisions that we have worked on with the Minority. The first incorporates explicit mention of health information technology systems as part of NIST's work on identity management research and standards development. As we work to increase the adoption of health IT into our medical system, it is important to recognize that the increased digitization and sharing of records must be accompanied by adequate privacy safeguards. Ensuring that advanced technologies and methods used to protect privacy should be central to NIST's work in health care IT.

The second change is also simple in the legislation's technical update codifying NIST's intramural security research activities related to access control management on computer systems. The manager's amendment substitutes the word "execution" in place of "enforcement" to clarify that these research activities are to support the use of protection policies, not to be part of or to guide their enforcement.

Is there any further discussion of the manager's amendment? If not, the vote occurs on the amendment. All in favor, say aye. Those opposed, say no. The ayes have it and the amendment is agreed to.

Are there any other amendments? If not, the vote is on the Committee Print as amended. All those in favor will say aye. All those opposed will say no. In the opinion of the Chair, the ayes have it. And I now recognize myself to make a motion.

I move that the Subcommittee favorably report the Committee print as amended to the Full Committee. Furthermore, I move that staff be instructed to prepare the Subcommittee report and make necessary technical and conforming changes to the print in accordance with the recommendations of the Subcommittee.

The question is on the motion to report the print favorably. Those in favor of the motion will signify by saying aye. Those opposed, no. The ayes have it and the bill is favorably reported.

Without objection, the motion to reconsider is laid upon the table. Members will have two subsequent calendar days in which to submit supplemental Minority or additional views on the measure. And I want to thank all the Members for their attendance, and this concludes our Subcommittee markup. Thank you.

[Whereupon, at 10:53 a.m., the Subcommittee was adjourned.]

Appendix:

COMMITTEE PRINT, SECTION-BY-SECTION ANALYSIS, AMENDMENT ROSTER

[COMMITTEE PRINT]

111TH CONGRESS
1ST SESSION

H. R. _____

To authorize the Director of the National Institute of Standards and Technology to coordinate United States Government representation in international cybersecurity technical standards development, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

introduced the following bill; which was referred to the Committee on

---

A BILL

To authorize the Director of the National Institute of Standards and Technology to coordinate United States Government representation in international cybersecurity technical standards development, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Coordination and Awareness Act".

SEC. 2. DEFINITIONS.

In this Act:

1 (1) DIRECTOR.—The term ''Director'' means
2 the Director of the National Institute of Standards
3 and Technology.
4 (2) INSTITUTE.—The term ''Institute'' means
5 the National Institute of Standards and Technology.

6 **SEC. 3. INTERNATIONAL CYBERSECURITY TECHNICAL**
7 **STANDARDS.**

8 The Director, in coordination with appropriate Fed-
9 eral authorities, shall—
10 (1) ensure coordination of United States Gov-
11 ernment representation in the international develop-
12 ment of technical standards related to cybersecurity;
13 and
14 (2) not later than 1 year after the date of en-
15 actment of this Act, develop and transmit to the
16 Congress a proactive plan to engage international
17 standards bodies with respect to the development of
18 technical standards related to cybersecurity.

19 **SEC. 4. PROMOTING CYBERSECURITY AWARENESS AND**
20 **EDUCATION.**

21 (a) PROGRAM.—The Director, in collaboration with
22 relevant Federal agencies, industry, educational institu-
23 tions, and other organizations, shall develop and imple-
24 ment a cybersecurity awareness and education program to

1 increase public awareness of cybersecurity risks, con-
2 sequences, and best practices through—
3 (1) the widespread dissemination of cybersecu-
4 rity technical standards and best practices identified
5 by the Institute; and
6 (2) efforts to make cybersecurity technical
7 standards and best practices usable by individuals,
8 small to medium-sized businesses, State and local
9 governments, and educational institutions.
10 (b) MANUFACTURING EXTENSION PARTNERSHIP.—
11 The Director shall, to the extent appropriate, implement
12 subsection (a) through the Manufacturing Extension Part-
13 nership program under section 25 of the National Insti-
14 tute of Standards and Technology Act (15 U.S.C. 278k).
15 (c) REPORT TO CONGRESS.—Not later than 90 days
16 after the date of enactment of this Act, the Director shall
17 transmit to the Congress a report containing a strategy
18 for implementation of this section.

19 **SEC. 5. IDENTITY MANAGEMENT RESEARCH AND DEVELOP-**
20 **MENT.**

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

1 (1) improve interoperability among identity
2 management technologies;
3 (2) strengthen authentication methods of iden-
4 tity management systems; and
5 (3) improve privacy protection in identity man-
6 agement systems through authentication and secu-
7 rity protocols.

8 **SEC. 6. AMENDMENT TO CYBERSECURITY RESEARCH AND**
9 **DEVELOPMENT ACT.**

10 (a) CHECKLISTS FOR GOVERNMENT SYSTEMS.—Sec-
11 tion 8(c) of the Cybersecurity Research and Development
12 Act (15 U.S.C. 7406(c)) is amended to read as follows:
13 "(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—
14 "(1) IN GENERAL.—The Director of the Na-
15 tional Institute of Standards and Technology shall
16 develop or identify and revise or adapt as necessary,
17 checklists, configuration profiles, and deployment
18 recommendations for products and protocols that
19 minimize the security risks associated with each
20 computer hardware or software system that is, or is
21 likely to become, widely used within the Federal
22 Government.
23 "(2) PRIORITIES FOR DEVELOPMENT.—The Di-
24 rector of the National Institute of Standards and
25 Technology shall establish priorities for the develop-

1 ment of checklists under this subsection. Such prior-
2 ities may be based on the security risks associated
3 with the use of each system, the number of agencies
4 that use a particular system, the usefulness of the
5 checklist to Federal agencies that are users or po-
6 tential users of the system, or such other factors as
7 the Director determines to be appropriate.
8 "(3) EXCLUDED SYSTEMS.— The Director of
9 the National Institute of Standards and Technology
10 may exclude from the requirements of paragraph (1)
11 any computer hardware or software system for
12 which the Director determines that the development
13 of a checklist is inappropriate because of the infre-
14 quency of use of the system, the obsolescence of the
15 system, or the inutility or impracticability of devel-
16 oping a checklist for the system.
17 "(4) AUTOMATION SPECIFICATIONS.—The Di-
18 rector of the National Institute of Standards and
19 Technology shall develop automated security speci-
20 fications (such as the Security Content Automation
21 Protocol) with respect to checklist content and asso-
22 ciated security related data.
23 "(5) DISSEMINATION OF CHECKLISTS.—The
24 Director of the National Institute of Standards and
25 Technology shall ensure that any product developed

1 under the National Checklist Program for any infor-
2 mation system, including the Security Content Auto-
3 mation Protocol and other automated security speci-
4 fications, is made available to Federal agencies.
5 "(6) AGENCY USE REQUIREMENTS.—Federal
6 agencies shall use checklists developed or identified
7 under paragraph (1) to secure computer hardware
8 and software systems. This paragraph does not—
9 "(A) require any Federal agency to select
10 the specific settings or options recommended by
11 the checklist for the system;
12 "(B) establish conditions or prerequisites
13 for Federal agency procurement or deployment
14 of any such system;
15 "(C) imply an endorsement of any such
16 system by the Director of the National Institute
17 of Standards and Technology; or
18 "(D) preclude any Federal agency from
19 procuring or deploying other computer hard-
20 ware or software systems for which no such
21 checklist has been developed or identified under
22 paragraph (1).".
23 (b) INTRAMURAL SECURITY RESEARCH.—Section 20
24 of the National Institute of Standards and Technology Act
25 (15 U.S.C. 278g–3) is amended by redesignating sub-

1 section (e) as subsection (f), and by inserting after sub-
2 section (d) the following:
3 "(e) INTRAMURAL SECURITY RESEARCH.—As part of
4 the research activities conducted in accordance with sub-
5 section (d)(3), the Institute shall—
6 "(1) conduct a research program to develop a
7 unifying and standardized identity, privilege, and ac-
8 cess control management framework for the enforce-
9 ment of a wide variety of resource protection policies
10 and that is amenable to implementation within a
11 wide variety of existing and emerging computing en-
12 vironments;
13 "(2) carry out research associated with improv-
14 ing the security of information systems and net-
15 works;
16 "(3) carry out research associated with improv-
17 ing the testing, measurement, usability, and assur-
18 ance of information systems and networks; and
19 "(4) carry out research associated with improv-
20 ing security of industrial control systems.".

SECTION-BY-SECTION ANALYSIS

COMMITTEE PRINT, THE CYBERSECURITY COORDINATION AND AWARENESS ACT

SECTION 1. Short Title

Sets the title as, "Cybersecurity Coordination and Awareness Act".

SECTION 2. Definitions

Defines the terms Director and Institute.

SECTION 3. International Cybersecurity Technical Standards

NIST shall 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.

SECTION 4. Promoting Cybersecurity Awareness and Education

NIST shall deliver a plan to Congress within 90 days describing how it will develop and implement a cybersecurity awareness and education program. The program shall 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. This plan will include how NIST can utilize established Manufacturing Extension Partnership networks to have cybersecurity information readily available to small manufacturing companies.

SECTION 5. Identity Management Research and Development

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

SECTION 6. Amendment to the Cybersecurity Research and Development Act of 2002

The section amends Sec. 8(c) of the *Cybersecurity R&D Act* (P.L. 107–305) and updates the technical terms in original statute to reflect the extant technologies and networked systems.

COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
MARKUP
November 4, 2009

AMENDMENT ROSTER

Committee Print, the *Cybersecurity Coordination and Awareness Act*

No.	Sponsor	Description	Results
1	Mr. Wu and Mr. Smith	Makes technical and clarifying changes to the Committee Print.	Agreed to by voice vote.

AMENDMENT TO THE COMMITTEE PRINT OFFERED BY MR. WU OF OREGON AND MR. SMITH OF NEBRASKA

Page 4, line 6, insert ", including health information technology systems," after "identity management systems".

Page 7, lines 8 and 9, strike "enforcement" and insert "execution".

☒

XXII. PROCEEDINGS OF THE FULL COMMITTEE MARKUP ON H.R. 4061, THE CYBERSECURITY ENHANCEMENT ACT OF 2009

WEDNESDAY, NOVEMBER 18, 2009

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
Washington, DC.

The Committee met, pursuant to call, at 10:00 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Bart Gordon [Chairman of the Committee] presiding.

Chairman GORDON. Good morning. The Committee will come to order.

Pursuant to notice, the Committee on Science and Technology meets to consider H.R. 4061, the *Cybersecurity Enhancement Act of 2009*. H.R. 4061 is a good bipartisan bill based on input we received in four hearings on cybersecurity. I would like to thank my colleagues, Dr. Lipinski, Mr. Wu, Dr. Ehlers and Mr. Smith, for their leadership and bipartisan work on the bill.

As many of you know, October was Cybersecurity Awareness Month. I think it is timely that we are considering this legislation on the heels of that effort to encourage people to protect their computers and the Nation's critical cyberinfrastructure. The theme of the recent awareness campaign was "Our Shared Responsibility." I find the theme particularly fitting as it also reflects an overarching recommendation in this year's Administration review of cyberspace policy. The common thread through all of the recommendations of the review was the importance of partnerships between the Federal Government and the private sector in advancing a more secure cyberspace.

Specific recommendations of the Administration review included developing a skilled cybersecurity workforce, coordinating and prioritizing the federal R&D portfolio, improving technology transfer to make sure new technologies make it into the marketplace, promoting cybersecurity education and awareness for the general public, and coordinating U.S. representation in the development of international standards.

Today's bill addresses every one of these recommendations. H.R. 4061 is based on the concept that in order to improve the security of our networked systems, which are fundamentally both public and private in nature, the Federal Government must work in concert with the private sector. H.R. 4061 will further our efforts in this direction and I urge my colleagues to support it.

Additionally, endorsements so far, and I am sure that we are going to be getting several more as the bill goes forward, but so far the endorsements come from the Business Software Alliance, the Association of Computing Machinery, Computing Research Association and Sun Microsystems.

Now I recognize my partner, Mr. Hall, to present his opening remarks.

[The prepared statement of Chairman Gordon follows:]

PREPARED STATEMENT OF CHAIRMAN BART GORDON

As I mentioned, the Committee will consider H.R. 4061 today. This is a good bipartisan bill based on input we received in four hearings held on cybersecurity. I would like to thank my colleagues, Dr. Lipinski, Mr. Wu, Dr. Ehlers and Mr. Smith, for their leadership and bipartisan work on the bill.

As many of you know, October was Cybersecurity Awareness Month. I think it's timely that we are considering this legislation on the heels of that effort to encourage people to protect their computers and the Nation's critical cyberinfrastructure. The theme of the recent awareness campaign was "Our Shared Responsibility." I find the theme particularly fitting as it also reflects an overarching recommendation in this year's Administration review of cyberspace policy. The common thread through all of the recommendations of the review was the importance of partnerships between the Federal Government and the private sector in achieving a more secure cyberspace.

Specific recommendations of the Administration review included:

- Developing a skilled cybersecurity workforce.
- Coordinating and prioritizing the federal R&D portfolio.
- Improving technology transfer to make sure new technologies make it into the marketplace.
- Promoting cybersecurity education and awareness for the general public.
- And, coordinating U.S. representation in the development of international standards.

Today's bill addresses every one of these recommendations. H.R. 4061 is based on the concept that in order to improve the security of our networked systems, which are fundamentally both public and private in nature, the Federal Government must work in concert with the private sector. H.R. 4061 will further our efforts in this direction and I urge my colleagues to support it.

Mr. HALL. Mr. Chairman, thank you.

We are all aware of the importance of cybersecurity and how much that importance has grown dramatically in recent years as most of the critical systems upon which we depend from telecommunications to electricity to banking and commerce rely on secure and reliable computing.

This committee has a long record of leadership on these issues dating back to the 1980s and the agencies and programs we oversee are critical to the success of federal efforts to address cybersecurity vulnerabilities. This bill will help to support these efforts through authorization of activities of three general areas: first, basic research at the National Science Foundation, which we know is a key driver to increasing security over the long-term; second, expanded NSF scholarships to increase the size and skills of the cybersecurity workforce; and three, increased R&D standards development and coordination and public outreach at the National Institute of Standards and Technology related to cybersecurity. These are modest but important changes that will help us do a better job of protecting our communications networks, and I am pleased to join my fellow Texan, Mr. McCaul, as a co-sponsor along with our

Subcommittee Ranking Members, Dr. Ehlers and Representative Smith of Nebraska.

I also want to note my appreciation for what this bill does not do. It avoids calling for any activities that could amount to being regulatory in nature. I think this is important. The Committee heard from multiple outside witnesses that heavy federal involvement in private-sector cybersecurity processes would actually be counterproductive to security. I hope we can ensure this bill continues to restrain from such action as it moves through the legislative process.

This is a good bill and represents a small but important step in the government's overall efforts to address cybersecurity issues. I want to thank the Chairman for working closely with all of us on this legislation. I look forward to continued cooperative efforts as we move forward. I yield back my time, sir.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, thank you for calling the markup this morning for H.R. 4061, the *Cybersecurity Enhancement Act of 2009.*

We are all aware that the importance of cybersecurity has grown dramatically in recent years, as most of the critical systems upon which we depend—from telecommunications to electricity to banking and commerce—rely on secure and reliable computing.

This committee has a long record of leadership on these issues (dating back to the 1980s), and the agencies and programs we oversee are critical to the success of federal efforts to address cybersecurity vulnerabilities.

This bill will help to support these efforts through authorization of activities in three general areas: (1) basic research at the National Science Foundation (NSF), which we know is a key driver to increasing security over the long-term; (2) expanded NSF scholarships to increase the size and skills of the cybersecurity workforce; and (3) increased R&D, standards development and coordination, and public outreach at the National Institute of Standards and Technology (NIST) related to cybersecurity.

These are modest but important changes that will help us do a better job of protecting our communications networks, and I am pleased to join my fellow Texan, Mr. McCaul, as a co-sponsor, along with our Subcommittee Ranking Members, Dr. Ehlers and Representative Smith of Nebraska.

I also want to note my appreciation for what this bill *doesn't* do. It avoids calling for any activities that could amount to being regulatory in nature. I think this is important. The Committee heard from multiple outside witnesses that heavy federal involvement in private sector cybersecurity processes would actually be counterproductive to security.

I hope we can ensure this bill continues to restrain from such action as it moves through the legislative process.

This is a good bill, and it represents a small but important step in the government's overall efforts to address cybersecurity issues. I want to thank the Chairman for working closely with Republicans on this legislation, and I look forward to continued cooperative efforts as we move forward.

Chairman GORDON. Thank you, Mr. Hall.

Does anyone else wish to be recognized? Mr. Lipinski, would you like to be recognized on the bill?

Mr. LIPINSKI. Thank you, Mr. Chairman.

H.R. 4061 is a product of combined efforts of the Research and Science Education Subcommittee and those of my colleagues on the Technology and Innovation Subcommittee. I would like to especially thank Dr. Ehlers, Mr. Wu and Mr. Smith for their contributions to the bill we are considering today.

The two Subcommittees have held a series of hearings on various aspects of cybersecurity including the state of R&D, the agency's

response to the 60-day review and the specific role of NIST [National Institute of Standards and Technology] in cybersecurity. At these hearings, witnesses emphasized the need to better coordinate and prioritize the federal R&D portfolio, to improve partnerships between the Federal Government and the private sector, to coordinate U.S. representation in international standard-setting bodies, and to train an IT [International Technology] workforce that can meet the growing needs of both the public and private sectors.

The legislation we are considering today addresses these concerns. First, it requires federal agencies to develop and implement a strategic plan for the federal cybersecurity R&D portfolio. The plan must be based on assessment of cybersecurity risk to make sure that taxpayer dollars fund the R&D needed to meet the strategic needs of our country and to keep Internet users safe from cybercrime. The strategic plan will also contain a description of how the program will transfer technology for our national labs and universities to industry since technology transfer is perhaps the most important component of any successful R&D program.

For the same reason, the bill establishes a university-industry taskforce to explore mechanisms and models for carrying out collaborative research in cybersecurity and make sure that the federal strategic plan is informed by industry needs.

In addition, the legislation addresses cybersecurity workforce needs for the Federal Government and for the Nation as a whole by providing fellowships to students pursuing advanced degrees in cybersecurity-related fields. The bill reauthorizes and expands the NSF's [National Science Foundation] Trustworthy Computing program, placing new emphasis on research into the social and behavioral aspects of cybersecurity, an important area identified by our witnesses. H.R. 4061 also emphasizes research into identity management at both NSF and NIST.

Finally, the bill addresses public awareness by requiring NIST to develop a plan for disseminating best practices and technical standards to the general public in a user-friendly format that will improve their basic cybersecurity knowledge.

In conclusion, H.R. 4061 is a good bipartisan bill that will help to ensure an overall vision for the federal cybersecurity R&D portfolio. It will help train the next generation of cybersecurity professionals, improve cybersecurity technical standards and will strengthen public-private partnerships in cybersecurity. This bill addresses a very urgent need that is becoming even greater every day in our nation and I think we have a very good bill here to address the science and technology aspects of this issue.

With that, I will yield back.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF REPRESENTATIVE DANIEL LIPINSKI

Thank you, Mr. Chairman. H.R. 4061 is a product of the combined efforts of the Research and Science Education Subcommittee and those of my colleagues on the Technology and Innovation Subcommittee. I'd like to thank Dr. Ehlers, Mr. Wu and Mr. Smith for their contributions to the bill we are considering today. The two Subcommittees have held a series of hearings on various aspects of cybersecurity, including the state of R&D, the agencies' response to the 60-day review, and the specific role of NIST in cybersecurity.

At these hearings witnesses emphasized the need to better coordinate and prioritize the federal R&D portfolio, to improve partnerships between the Federal

Government and the private sector, to coordinate U.S. representation in international standard setting bodies, and to train an IT workforce that can meet the growing needs of both the public and private sectors.

The legislation we are considering today addresses these concerns. First, it requires federal agencies to develop and implement a strategic plan for the federal cybersecurity R&D portfolio. The plan must be based on an assessment of cybersecurity risk, to make sure that taxpayer dollars fund the R&D needed to meet the strategic needs of our country and to keep Internet users safe from cybercrime. The strategic plan will also contain a description of how the program will transfer technology from our national labs and universities to industry, since technology transfer is perhaps the most important component of any successful R&D plan.

For the same reason, the bill establishes a university-industry task force to explore mechanisms and models for carrying out collaborative research in cybersecurity and makes sure that federal strategic plan is informed by industry needs.

In addition, the legislation addresses cybersecurity workforce needs for the Federal Government, and for the Nation as a whole, by providing fellowships to students pursuing advanced degrees in cybersecurity-related fields.

The bill reauthorizes and expands the NSF's Trustworthy Computing program, placing a new emphasis on research into the social and behavioral aspects of cybersecurity, an important area identified by our witnesses. H.R. 4061 also emphasizes research into identity management at both NSF and NIST.

Finally, the bill addresses public awareness by requiring NIST to develop a plan for disseminating best practices and technical standards to the general public in a user-friendly format that will improve their basic cybersecurity knowledge.

In conclusion, H.R. 4061 is a good bipartisan bill that will help to ensure an overall vision for the federal cybersecurity R&D portfolio, will help train the next generation of cybersecurity professionals, improve cybersecurity technical standards and will strengthen public-private partnerships in cybersecurity.

Chairman GORDON. Thank you, Dr. Lipinski.

Does anyone else wish to—Mr. McCaul.

Mr. MCCAUL. Thank you, Mr. Chairman, and let me thank Mr. Lipinski for this bill. I was proud to be a lead co-sponsor on the bill, original co-sponsor.

The Internet provides great opportunities and advances but it also presents many challenges and many threats. Cybersecurity I think is one of the most important issues we face as a nation, and one of the key issues we face when dealing with cybersecurity is a lack of an adequately trained workforce, both in the government and in the private sector. This bill acts on the research recommendations of the CSIS Commission On Cybersecurity, which I co-chaired, and this is the report. Congressman Jim Langevin and I co-chaired this along with CSIS. Some of the top experts in the Nation developed this report, and I am very pleased to see this bill addressing two of those recommendations: one, to develop a federal cyber workforce. This bill does that by creating a scholarship program at the NSF that can be repaid with federal service.

In addition, it improves cybersecurity R&D and coordination, which was another recommendation from the Commission, and this bill does that by reauthorizing the cyber programs at NSF as well as expanding NIST efforts and encouraging cooperation between the academic and private sectors with the university and industry taskforce.

So just let me close by again commending the gentleman Mr. Lipinski for introducing the bill and I look forward to its final passage. Thank you.

Chairman GORDON. Thank you, Mr. McCaul, for your active involvement in putting this bill together.

Mr. Wu is recognized.

Mr. WU. Thank you very much, Mr. Chairman.

I want to recognize your leadership in bringing this bill together and Mr. Lipinski's very fine work. The NIST sections of the bill from my Technology and Innovation Subcommittee hearings resulted from some very valuable information that we collected and some efforts to add new approaches or strengthen new approaches. NIST is the only federal agency which is tasked with protecting the government's non-classified computer systems and it is therefore very important that we work together to continuously adapt to the current scope of cybersecurity concerns and also prepare for some of the concerns of the future, and it is also very important that we achieve these goals by maximizing the effectiveness of our programs and resources and continuously tuning them up and not just by spending more money, and today's legislation reflects this strategy.

The legislation calls for an increased coordination among federal agencies and also calls for enhanced education programs, and I would just like to add that the education programs I think have some of the best potential for enhancing cybersecurity at low cost. There are some very technically sophisticated ways of enhancing cybersecurity but there are some simple ways also. In my home state, some folks were backing up their computer system every night and taking the discs home and some of these discs were stolen out of the back of a car and a lot of records were lost. You know, some aspects of computer security are rocket science and others are fairly simple precautionary steps which most people can take. It is the analogy to our FIRE bill that we will have on the Floor later today is that while you may need sophisticated fire suppression systems, you don't have to be a rocket scientist to teach folks not to play with matches, and there is an analogy here about the sophisticated things that we need to do and the more straightforward education programs that will enhance computer security at relatively low cost.

Again, Mr. Chairman, thank you for your leadership in bringing the two halves of this legislation together, and I yield back the balance of my time.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

Good morning. The NIST sections of this bill result from valuable information received in Technology and Innovation Subcommittee hearings and in collaboration with NIST, other government agencies, private industry, and academia. Since NIST is the only federal agency tasked with protecting non-classified federal computer systems, it is important that we work together to continuously adapt to the current scope of cybersecurity concerns and prepare for those on the horizon. It is important that we achieve these goals in part by maximizing the effectiveness of programs and resources, not just by spending more money. Today's legislation reflects this strategy by calling for an increased coordination among federal agencies and educating the most vulnerable users of our cyber-infrastructure.

Chairman GORDON. Thank you, Mr. Wu. I had the easy part, you all had the hard part, and again, I want to thank Mc. McCaul and Mr. Smith, Dr. Ehlers, Dr. Lipinski, Mr. Wu and all the Members of your committee and the staff for your work, having all the hearings. You did the groundwork and that is why things turn out well, so thank you.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you, Mr. Chairman.

As the world becomes increasingly connected through the Internet, it is critical to ensure that cyberspace remains secure and reliable.

Today we will markup the *Cybersecurity Coordination and Awareness Act*, which would direct the National Institutes of Standards and Technology (NIST) to develop and implement a proactive plan to ensure coordinated engagement in international cybersecurity technical standards development.

Under this proposal, NIST would also be required to deliver a plan to Congress describing how it will develop and implement a cybersecurity awareness and education program. The *Cybersecurity Coordination and Awareness Act* would also direct NIST to engage in research and development programs to improve identity management systems.

I look forward to our discussion of this proposal today.

I yield back.

Chairman GORDON. So now I ask unanimous consent that the bill is considered as read and open to amendment at any point and that the Members proceed with the amendments in the order of the roster. Without objection, so ordered.

The first amendment on the roster is an amendment in the nature of a substitute offered by the gentleman from Illinois, Dr. Lipinski. Are you ready to proceed with your amendment?

Mr. LIPINSKI. Yes, I am, Mr. Chairman.

Chairman GORDON. The Clerk will report the amendment.

The CLERK. Amendment number 046, amendment in the nature of a substitute to H.R. 4061, offered by Mr. Lipinski of Illinois.

Chairman GORDON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman for five minutes to explain the amendment.

Mr. LIPINSKI. Thank you, Mr. Chairman.

This amendment makes some technical corrections in addition to reinstating two sections that were part of the bill passed out of the Research and Science Education Subcommittee. The sections specifically address cybersecurity workforce concerns.

First, the amendment requires the President to assess the cybersecurity skills needed by the Federal Government to compare them to the skills sought by industry and then to examine the capacity of our colleges and universities to produce those qualified cybersecurity professionals. It also requires an assessment of the effectiveness of federal programs such as the National Centers of Academic Excellence in information assurance education. They are aimed at promoting cybersecurity research and education at our colleges and universities.

Additionally, the amendment attempts to address the estimated shortfall in cybersecurity professionals by authorizing the Federal Cyber Scholarship for Service program at NSF. This program would provide scholarships to undergraduate and graduate students pursing degrees in cybersecurity. It requires them in return to serve an equal number of years in the federal IT workforce. The amendment clarifies that three-year scholarships are for students pursuing doctoral degrees and it specifies that students who are unable to meet their service obligation at a federal agency or federally funded R&D center can meet their obligation by serving as a cybersecurity professional in a State, local or tribal government agency.

And finally, the amendment ensures that cybersecurity researchers have access to data relevant to development, testing and evaluation of security technologies.

I urge my colleagues to support this amendment.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF REPRESENTATIVE DANIEL LIPINSKI

This amendment makes some technical corrections in addition to reinstating two sections that were part of the bill passed out of the Research and Science Education Subcommittee. The sections specifically address cybersecurity workforce concerns. First, the amendment requires the President to assess the cybersecurity skills needed by the Federal Government, to compare them to the skills sought by industry, and then to examine of the capacity of our colleges and universities to produce those qualified cybersecurity professionals. It also requires an assessment of the effectiveness of federal programs such as the National Centers of Academic Excellence in Information Assurance Education that are aimed at promoting cybersecurity research and education at our colleges and universities.

Additionally, the amendment attempts to address the estimated shortfall in cybersecurity professionals by authorizing the Federal Cyber Scholarship for Service program at the NSF. This program provides scholarships to undergraduate and graduate students pursuing degrees in cybersecurity. It requires them, in return, to serve an equal number of years in the federal IT workforce. The amendment clarifies that three-year scholarships are for students pursuing doctoral degrees and it specifies that students who are unable to meet their service obligation at a federal agency or federally funded R&D center can meet their obligation by serving as a cybersecurity professional in a State, local or tribal government agency.

And finally, the amendment ensures that cybersecurity researchers have access to data relevant to the development, testing and evaluation of security technologies.

I urge my colleagues to support this amendment.

Chairman GORDON. Is there further discussion on the amendment?

Mr. HALL. Mr. Chairman.

Chairman GORDON. Yes. Mr. Hall is recognized.

Mr. HALL. The Subcommittee Chairman's amendment in the nature of a substitute simply makes some good technical changes and incorporates some valuable feedback we received from several folks familiar with NSF's cybersecurity programs. I support the amendment and I urge its adoption. I yield back.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, the Subcommittee Chairman's amendment in the nature of a substitute simply makes some technical changes and incorporates some valuable feedback we received from several folks familiar with NSF's cybersecurity programs. I support this amendment and urge its adoption.

Chairman GORDON. Is there further discussion on the amendment? If not, the second amendment on the roster is an amendment offered by the gentleman from New Mexico, Mr. Lujan. Are you ready to proceed?

Mr. LUJAN. Mr. Chairman, I have an amendment at the desk.

Chairman GORDON. The Clerk will report the amendment.

The CLERK. Amendment number 032, amendment to the amendment in the nature of a substitute to H.R. 4061, offered by Mr. Lujan of New Mexico.

Chairman GORDON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman for five minutes to explain the amendment.

Mr. LUJAN. Thank you, Mr. Chairman.

My amendment today amends two sections of the *Cybersecurity Enhancement Act of 2009,* section 106 and section 203. Section 106 of the bill establishes the Federal Cyber Scholarship for Service program, which will help recruit and train the next generation of cybersecurity professionals. This will be done through grant awards that support the development of cybersecurity-related curricula, faculty, professional development and institutional partnerships within institutions of higher education. My amendment today specifies that this program increases the capacity of institutions of higher education throughout all regions of the United States to train cybersecurity professionals. The goal of this amendment is to address any potential regional disparities in this program by ensuring that the program increases the ability of colleges and universities from all parts of the country to train highly qualified cybersecurity professionals. New Mexico is home to excellent research universities like the University of New Mexico, New Mexico State University, New Mexico Technical College. It is important that our universities in the Southwest as well as other regions of the United States are training cybersecurity professionals to become part of a geographically diverse talent pool. This will also promote local economic growth as companies, organizations and government agencies like our national laboratories will have better opportunities to hire locally trained talent.

Section 203 of the bill establishes a program to promote cybersecurity awareness and education in order to increase public awareness of cybersecurity risks. The program seeks to make cybersecurity standards and practices usable by individuals, businesses and State and local governments. My amendment today adds tribal governments to the list of entities cybersecurity standards and best practices are designed to assist. My district in New Mexico is home to 18 different tribes and many of these tribes are currently in the early stages of information technology development. As our tribes increase their level of connectivity and dependence on IT, it is critically important that we educate tribal communities about the risks of cyber attacks and how to take necessary precautions to protect sensitive information from cyber criminals. Establishing cybersecurity standards and practices that our trial communities will benefit from will greatly achieve the objective of this section to promote cybersecurity awareness and education.

I am proud to be a co-sponsor of the *Cybersecurity Enhancement Act of 2009,* and I want to thank you, Mr. Chairman, Chairman Wu, Chairman Lipinski, Ranking Member McCaul and Ranking Member Smith for their hard work on this important bill and I urge my colleagues to support this amendment today. I yield back my time.

[The prepared statement of Mr. Lujan follows:]

PREPARED STATEMENT OF REPRESENTATIVE BEN R. LUJAN

Thank you Mr. Chairman.

My amendment today amends two sections of the *Cybersecurity Enhancement Act of 2009,* Section 106 and Section 203.

Section 106 of the bill establishes the Federal Cyber Scholarship for Service Program which will help recruit and train the next generation of cybersecurity professionals. This will be done through grant awards that support the development of

cybersecurity-related curricula, faculty professional development, and institutional partnerships within institutions of higher education. My amendment today specifies that this program increases the capacity of institutions of higher education throughout all regions of the United States to train cybersecurity professionals. The goal of this amendment is to address any potential regional disparities in this program by ensuring that the program increases the ability of colleges and universities from all parts of the country to train highly qualified cybersecurity professionals. New Mexico is home to excellent research universities like the University of New Mexico and the New Mexico State University. It is important that our universities in the Southwest as well as all other regions of the United States are training cybersecurity professionals to become part of a geographically diverse talent pool.

This will also promote local economic growth as companies, organizations and government agencies will have better opportunities to higher locally trained talent.

Section 203 of the bill establishes a program to promote cybersecurity awareness and education in order to increase public awareness of cybersecurity risks. The program seeks to make cybersecurity standards and practices usable by individuals, businesses and State and local governments. My amendment today adds tribal governments to the list of entities cybersecurity standards and best practices are designed to assist. My district in New Mexico is home to eighteen different tribes and many of these tribes are currently in the early stages of information technology infrastructure development. As our tribes increase their level of connectivity and dependence on IT, it is critically important that we educate tribal communities about the risks of cyber attacks and how to take necessary precautions to protect sensitive information from cyber criminals. Establishing cybersecurity standards and practices that our tribal communities will benefit from will greatly achieve the objective of this section to promote cybersecurity awareness and education.

I am proud to co-sponsor the *Cybersecurity Enhancement Act of 2009* and I want to thank Chairman Gordon, Chairman Wu, Chairman Lipinski, Ranking Member Hall, Ranking Member Smith, and Ranking Members Ehlers for their hard work on this important bill. I urge my colleagues to support my amendment today.

Chairman GORDON. Is there further discussion on the amendment?

Mr. HALL. Mr. Chairman.

Chairman GORDON. Mr. Hall is recognized.

Mr. HALL. This amendment is another good Lujan amendment and it simply adds language ensuring that the scholarship program authorized in this bill is geographically diverse. I support the amendment and I urge its adoption. I say another good amendment because he is a given family from a great state. Thank you.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, this amendment simply adds language ensuring that the scholarship program authorized in the bill is geographically diverse. I support this amendment and urge its adoption.

Chairman GORDON. Thank you, Mr. Hall.

Is there further discussion on the amendment? If no, the vote occurs on the amendment. All in favor, say aye. Opposed, no. The ayes have it. The amendment is agreed to.

The third amendment on the roster is an amendment offered by the gentleman from Texas, Mr. McCaul. Are you ready to proceed with your amendment?

Mr. MCCAUL. I am, Mr. Chairman.

Chairman GORDON. The Clerk will report the amendment.

The CLERK. Amendment number 027, amendment to the amendment in the nature of a substitute to H.R. 4061, offered by Mr. McCaul of Texas.

Chairman GORDON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman for five minutes to explain his amendment.

Mr. MCCAUL. Thank you, Mr. Chairman.

My amendment has to do with the NIST checklist provision in this bill. Basically the amendment would clarify that NIST inform agencies of the availability of cybersecurity products under the national checklist program and, two, that NIST checklists are not required to be used by agencies. This bill expands NIST's responsibility for updating and disseminating guidance to federal agencies on cybersecurity. There was some concern that the language in the bill would prevent NIST from including software developed outside of NIST on the checklist distributed to the federal agencies. This amendment clarifies that NIST can include software developed by an outside source or by the private sector. There is no reason that federal agencies should not be allowed to use software developed by the private sector if that software is superior and can do the job, and with that I yield back.

Chairman GORDON. Thank you, Mr. McCaul. I think that is the theme of the bill is coordination between public and private sector.

Is there further discussion on the amendment?

Mr. HALL. Mr. Chairman.

Chairman GORDON. Mr. Hall is recognized.

Mr. HALL. I am pleased to support my colleague from Texas and the lead Republican co-sponsor of the underlying bill with his amendment. I think it is good, sound policy and so does the Business Software Alliance. I ask unanimous consent that their letter of support be submitted for the record, Bob Holleyman, the President and CEO.

[The information follows:]

BSA®
BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

1150 18th Street, NW
Suite 700
Washington DC 20036

p. 202/872.5500
f. 202/872.5501

November 17, 2009

The Honorable Bart Gordon, Chairman
The Honorable Ralph M. Hall, Ranking Member
Committee on Science & Technology
United States House of Representatives
Washington, DC 20515

Dear Chairman Gordon and Ranking Member Hall:

On behalf of its members, the Business Software Alliance (BSA)* commends you for your leadership on cyber security policy. We have greatly appreciated your willingness to consider BSA members' views on HR 4061, the Cybersecurity Enhancement Act of 2009.

We are particularly grateful for the improvements you have been able to make to section 109(5) and (6), which will ensure that the implementation of NIST checklists remains flexible, and that agencies are adequately informed of the tools available to comply with the checklists. We strongly appreciate the cyber security research and development provisions of the bill, which will make a major contribution toward leveraging our Nation's innovation. We also appreciate the identity management provisions, which recognize the importance of more reliable identity and authentication as cornerstones of an inherently more secure cyber space.

Based on the improvements to section 109(5) and (6) and your commitment to continue to work with us on the bill as it moves through the process, we support its passage by the Committee on Science & Technology. We applaud you for your great efforts to improve the cyber security of our Nation, and its continued international leadership in cyber security.

Sincerely yours,

Robert W. Holleyman, II
President and CEO

*The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, AVG, Bentley Systems, CA, Cadence, Cisco Systems, Corel, CyberLink, Dassault Systemes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

WWW.BSA.ORG

Chairman GORDON. Without objection, so ordered.

Mr. HALL. I support the amendment and urge its adoption. I yield back my time.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, I am pleased to support my colleague from Texas—and the lead Republican co-sponsor of the underlying bill—with his amendment. I believe it is good, sound policy, and so does the Business Software Alliance. I ask unanimous consent that their letter of support be submitted for the record. I support this amendment and urge its adoption.

Chairman GORDON. Is there further discussion on the amendment? If no, all in favor say aye. Opposed, no. The ayes have it. The amendment is agreed to.

The fourth amendment on the roster is offered by the gentleman from Oregon, Mr. Wu. Are you ready to proceed with your amendment?

Mr. WU. I am, Mr. Chairman.

Chairman GORDON. The Clerk will report the amendment.

The CLERK. Amendment number 027, amendment to the amendment in the nature of a substitute to H.R. 4061, offered by Mr. Wu of Oregon.

Mr. WU. Mr. Chairman, I ask unanimous consent to dispense with the reading.

Chairman GORDON. Granted, and I recognize the gentleman for five minutes to explain the amendment.

Mr. WU. Thank you very much, Mr. Chairman.

My amendment adds one task to NIST's work on identity management research and development. Today's bill directs NIST to improve the inter-operability, the authentication methods and privacy protection of identity management systems. This amendment would add usability to this list. The aim is to simplify how these systems are installed, set up and used and simply to make these methodologies more user-friendly. Improving usability is a key element in growing the widespread adoption of these important security systems, and I yield back the balance of my time, Mr. Chairman.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

This amendment adds one task to NIST's work on identity management research and development. Currently, today's bill directs NIST to improve the inter-operability, authentication methods, and privacy protection of identity management systems. By adding usability to this list, we aim to simplify how these systems are installed, set up, and used. Improving usability is a crucial element in growing the widespread adoption of these important security systems.

Chairman GORDON. Is there any further discussion on the amendment?

Mr. HALL. Mr. Chairman.

Chairman GORDON. Mr. Hall is recognized.

Mr. HALL. I am agreeable to not having to listen to his reading, but this amendment clarifies that NIST activities in the realm of identity management include research to improve the usability of identity management systems. Now, we all know that the information systems are only useful if people know how to use them effectively. This amendment ensures that as we research ways to improve the security of our cyber networks that we are mindful of the human element involved in that success. I support the amendment and urge its passage.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, this amendment clarifies that NIST's activities in the realm of identity management include research to improve the usability of identity management systems. We all know that information systems are only useful if people know how to use them effectively. This amendment ensures that as we research ways to

improve the security of our cyber-networks that we are mindful of the human element involved in that success. I support the amendment and urge its passage.

Chairman GORDON. Thank you, Mr. Hall.

Is there further discussion on the amendment? If no, the vote. In favor, say aye. Opposed, no. The ayes have it and the amendment is agreed to.

Are there other amendments? If not, then the vote occurs on the amendment in the nature of a substitute offered by the gentleman from Illinois as amended. All in favor, say aye. Opposed, no. The ayes have it. The amendment is agreed to.

The vote is now on the bill, H.R. 4061 as amended. All those in favor will say aye. All opposed, no. The ayes have it.

I now recognize Mr. Wu for a motion.

Mr. WU. Mr. Chairman, I move that the Committee favorably report H.R. 4061, as amended, to the House with the recommendation that the bill do pass. Furthermore, I move that staff be instructed to prepare the legislative report and make necessary technical and conforming changes and that the Chairman take all necessary steps to bring the bill before the House for consideration.

Chairman GORDON. The question is on the motion to report the bill favorably. Those in favor of the motion will signify by saying aye. Opposed, no. The ayes have it and the bill is favorably reported.

Without objection, the motion to reconsider is laid upon the table. Members will have two subsequent calendar days in which to submit supplemental Minority or additional views on this legislation.

And I want to thank everyone for coming today. I know that you have other things to do but we can't proceed if you are not here. I know you get here and you say well, that was easy. It wasn't so easy. These subcommittees put a lot of work on this and it is a good bill. Cybersecurity is important and this committee will play a major role now in our nation's cybersecurity. So I thank you, and this meeting is concluded.

[Whereupon, at 10:28 a.m., the Committee was adjourned.]

Appendix:

H.R. 4061, SECTION-BY-SECTION ANALYSIS, AMENDMENT ROSTER

I

111TH CONGRESS
1ST SESSION

H. R. 4061

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

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 7, 2009

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

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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 sys-

1 tems. Once every 3 years after the initial strategic plan
2 is transmitted to Congress under this section, such agen-
3 cies shall prepare and transmit to Congress an update of
4 such plan.

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

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

15 (2) describe how the Program will focus on in-
16 novative, transformational technologies with the po-
17 tential to enhance the security, reliability, resilience,
18 and trustworthiness of the digital infrastructure;

19 (3) describe how the Program will foster the
20 transfer of research and development results into
21 new cybersecurity technologies and applications for
22 the benefit of society and the national interest, in-
23 cluding through the dissemination of best practices
24 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 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) 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 inserting "and" after the semicolon;

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

(C) by striking subparagraph (D);

(2) 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

(3) 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 nec-

essary 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 nec-

essary 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. 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 ex-

1 plore mechanisms for carrying out collaborative research
2 and development activities for cybersecurity through a
3 consortium or other appropriate entity with participants
4 from institutions of higher education and industry.
5 (b) FUNCTIONS.—The task force shall—
6 (1) develop options for a collaborative model
7 and an organizational structure for such entity
8 under which the joint research and development ac-
9 tivities could be planned, managed, and conducted
10 effectively, including mechanisms for the allocation
11 of resources among the participants in such entity
12 for support of such activities;
13 (2) propose a process for developing a research
14 and development agenda for such entity, including
15 guidelines to ensure an appropriate scope of work fo-
16 cused on nationally significant challenges and requir-
17 ing collaboration;
18 (3) define the roles and responsibilities for the
19 participants from institutions of higher education
20 and industry in such entity;
21 (4) propose guidelines for assigning intellectual
22 property rights and for the transfer of research and
23 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. 107. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

Section 8(c) of the Cybersecurity 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

1 computer hardware or software system that is, or is
2 likely to become, widely used within the Federal
3 Government.

4 "(2) PRIORITIES FOR DEVELOPMENT.—The Di-
5 rector of the National Institute of Standards and
6 Technology shall establish priorities for the develop-
7 ment of checklists under this subsection. Such prior-
8 ities may be based on the security risks associated
9 with the use of each system, the number of agencies
10 that use a particular system, the usefulness of the
11 checklist to Federal agencies that are users or po-
12 tential users of the system, or such other factors as
13 the Director determines to be appropriate.

14 "(3) EXCLUDED SYSTEMS.—The Director of
15 the National Institute of Standards and Technology
16 may exclude from the requirements of paragraph (1)
17 any computer hardware or software system for
18 which the Director determines that the development
19 of a checklist is inappropriate because of the infre-
20 quency of use of the system, the obsolescence of the
21 system, or the inutility or impracticability of devel-
22 oping a checklist for the system.

23 "(4) AUTOMATION SPECIFICATIONS.—The Di-
24 rector of the National Institute of Standards and
25 Technology shall develop automated security speci-

1 fications (such as the Security Content Automation
2 Protocol) with respect to checklist content and asso-
3 ciated security related data.
4 "(5) DISSEMINATION OF CHECKLISTS.—The
5 Director of the National Institute of Standards and
6 Technology shall ensure that any product developed
7 under the National Checklist Program for any infor-
8 mation system, including the Security Content Auto-
9 mation Protocol and other automated security speci-
10 fications, is made available to Federal agencies.
11 "(6) AGENCY USE REQUIREMENTS.—Federal
12 agencies shall use checklists developed or identified
13 under paragraph (1) to secure computer hardware
14 and software systems. This paragraph does not—
15 "(A) require any Federal agency to select
16 the specific settings or options recommended by
17 the checklist for the system;
18 "(B) establish conditions or prerequisites
19 for Federal agency procurement or deployment
20 of any such system;
21 "(C) imply an endorsement of any such
22 system by the Director of the National Institute
23 of Standards and Technology; or
24 "(D) preclude any Federal agency from
25 procuring or deploying other computer hard-

ware or software systems for which no such checklist has been developed or identified under paragraph (1).''.

SEC. 108. 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 and local 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

1 transmit to the Congress a report containing a strategy
2 for implementation of this section.

3 **SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
4 **OPMENT.**

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

9 (1) improve interoperability among identity
10 management technologies;

11 (2) strengthen authentication methods of iden-
12 tity management systems; and

13 (3) improve privacy protection in identity man-
14 agement systems, including health information tech-
15 nology systems, through authentication and security
16 protocols.

○

SECTION-BY-SECTION ANALYSIS OF THE
AMENDMENT IN THE NATURE OF A SUBSTITUTE TO
H.R. 4061, WHICH CONTAINS THE CONTENTS OF BOTH CYBERSECURITY PRINTS IN THEIR ENTIRETY.

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, it 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 their 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 needed by each federal agency, the supply of cybersecurity talent, and 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 their in-house research program, 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

NIST shall 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

NIST shall deliver a plan to Congress within 90 days describing how it will develop and implement a cybersecurity awareness and education program. The program shall 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. This plan will 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

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

COMMITTEE ON SCIENCE AND TECHNOLOGY
FULL COMMITTEE MARKUP
November 18, 2009

AMENDMENT ROSTER

H. R. 4061, the *Cybersecurity Enhancement Act of 2009*

No.	Amendment	Summary	Results
1	Mr. Lipinski (Amendment in the Nature of a Substitute)	Makes several technical and clarifying changes to the bill. Amends the bill to add items included in the Committee Prints reported by the Technology and Innovation Subcommittee and Research and Science Education Subcommittee.	Agreed to by voice vote.
2	Mr. Luján	Amends Section 106 ("Federal Cyber Scholarships for Service Program") to specify that the Program characteristic related to increasing the capacity of institutions of higher education to produce highly qualified cybersecurity professionals shall apply to higher education institutions "throughout all regions of the United States." Amends Section 203 ("Promoting Cybersecurity Awareness and Education") to add tribal governments to the list of governments at which the certain aspects of the cybersecurity awareness and education program are directed.	Agreed to by voice vote.
3	Mr. McCaul	Amends the manner by which checklists are disseminated under Section 109 ("Cybersecurity Checklist Development and Dissemination"). Also amends the agency use requirements for checklists developed in accordance with Section 109.	Agreed to by voice vote.
4	Mr. Wu	Amends Section 204 ("Identity Management Research and Development") to require that the program established under the Section also be directed toward improving the "usability of identity management systems."	Agreed to by voice vote.

AMENDMENT IN THE NATURE OF A SUBSTITUTE

TO H.R. 4061

OFFERED BY MR. LIPINSKI OF ILLINOIS

Strike all after the enacting clause and insert the following:

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the ''Cybersecurity En-
3 hancement Act of 2009''.

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).

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.".

1 **SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DE-**
2 **VELOPMENT PLAN.**

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

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

21 (1) specify and prioritize near-term, mid-term
22 and long-term research objectives, including objec-
23 tives associated with the research areas identified in
24 section 4(a)(1) of the Cyber Security Research and
25 Development Act (15 U.S.C. 7403(a)(1)) and how
26 the near-term objectives complement research and

1 development areas in which the private sector is ac-
2 tively engaged;
3 (2) describe how the Program will focus on in-
4 novative, transformational technologies with the po-
5 tential to enhance the security, reliability, resilience,
6 and trustworthiness of the digital infrastructure;
7 (3) describe how the Program will foster the
8 transfer of research and development results into
9 new cybersecurity technologies and applications for
10 the benefit of society and the national interest, in-
11 cluding through the dissemination of best practices
12 and other outreach activities;
13 (4) describe how the Program will establish and
14 maintain a national research infrastructure for cre-
15 ating, testing, and evaluating the next generation of
16 secure networking and information technology sys-
17 tems;
18 (5) describe how the Program will facilitate ac-
19 cess by academic researchers to the infrastructure
20 described in paragraph (4), as well as to relevant
21 data, including event data; and
22 (6) describe how the Program will engage fe-
23 males and individuals identified in section 33 or 34
24 of the Science and Engineering Equal Opportunities

1 Act (42 U.S.C. 1885a or 1885b) to foster a more di-
2 verse workforce in this area.
3 (c) DEVELOPMENT OF ROADMAP.—The agencies de-
4 scribed in subsection (a) shall develop and annually update
5 an implementation roadmap for the strategic plan re-
6 quired in this section. Such roadmap shall—
7 (1) specify the role of each Federal agency in
8 carrying out or sponsoring research and development
9 to meet the research objectives of the strategic plan,
10 including a description of how progress toward the
11 research objectives will be evaluated;
12 (2) specify the funding allocated to each major
13 research objective of the strategic plan and the
14 source of funding by agency for the current fiscal
15 year; and
16 (3) estimate the funding required for each
17 major research objective of the strategic plan for the
18 following 3 fiscal years.
19 (d) RECOMMENDATIONS.—In developing and updat-
20 ing the strategic plan under subsection (a), the agencies
21 involved shall solicit recommendations and advice from—
22 (1) the advisory committee established under
23 section 101(b)(1) of the High-Performance Com-
24 puting 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) 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 inserting "and" after the semicolon;

1 (B) in subparagraph (D), by striking the
2 period and inserting "; and"; and
3 (C) by striking subparagraph (D);
4 (2) by adding at the end the following new sub-
5 paragraph:
6 "(E) how the center will partner with gov-
7 ernment laboratories, for-profit entities, other
8 institutions of higher education, or nonprofit re-
9 search institutions."; and
10 (3) by amending paragraph (7) to read as fol-
11 lows:
12 "(7) 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 (d) COMPUTER AND NETWORK SECURITY CAPACITY
18 BUILDING GRANTS.—Section 5(a)(6) of such Act (15
19 U.S.C. 7404(a)(6)) is amended to read as follows:
20 "(6) 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 (e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
2 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
3 7404(b)(2)) is amended to read as follows:
4 "(2) 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 (f) GRADUATE TRAINEESHIPS IN COMPUTER AND
10 NETWORK SECURITY.—Section 5(c)(7) of such Act (15
11 U.S.C. 7404(c)(7)) is amended to read as follows:
12 "(7) 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 (g) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CY-
18 BERSECURITY.—Section 5(e) of such Act (15 U.S.C.
19 7404(e)) is amended to read as follows:
20 "(e) POSTDOCTORAL RESEARCH FELLOWSHIPS IN
21 CYBERSECURITY.—
22 "(1) IN GENERAL.—The Director shall carry
23 out a program to encourage young scientists and en-
24 gineers to conduct postdoctoral research in the fields
25 of cybersecurity and information assurance, includ-

1 ing the research areas described in section 4(a)(1),
2 through the award of competitive, merit-based fel-
3 lowships.
4 "(2) 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 **SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE**
10 **PROGRAM.**

11 (a) IN GENERAL.—The Director of the National
12 Science Foundation shall carry out a Scholarship for Serv-
13 ice program to recruit and train the next generation of
14 Federal cybersecurity professionals and to increase the ca-
15 pacity of the higher education system to produce an infor-
16 mation technology workforce with the skills necessary to
17 enhance the security of the Nation's communications and
18 information infrastructure.
19 (b) CHARACTERISTICS OF PROGRAM.—The program
20 under this section shall—
21 (1) provide, through qualified institutions of
22 higher education, scholarships that provide tuition,
23 fees, and a competitive stipend for up to 2 years to
24 students pursing a bachelor's or master's degree and

1 up to 3 years to students pursuing a doctoral degree
2 in a cybersecurity field;
3 (2) provide the scholarship recipients with sum-
4 mer internship opportunities or other meaningful
5 temporary appointments in the Federal information
6 technology workforce; and
7 (3) increase the capacity of institutions of high-
8 er education to produce highly qualified cybersecu-
9 rity professionals, through the award of competitive,
10 merit-reviewed grants that support such activities
11 as—
12 (A) faculty professional development, in-
13 cluding technical, hands-on experiences in the
14 private sector or government, workshops, semi-
15 nars, conferences, and other professional devel-
16 opment opportunities that will result in im-
17 proved instructional capabilities;
18 (B) institutional partnerships, including
19 minority serving institutions; and
20 (C) development of cybersecurity-related
21 courses and curricula.
22 (c) SCHOLARSHIP REQUIREMENTS.—
23 (1) ELIGIBILITY.—Scholarships under this sec-
24 tion shall be available only to students who—

1 (A) are citizens or permanent residents of
2 the United States;
3 (B) are full-time students in an eligible de-
4 gree program, as determined by the Director,
5 that is focused on computer security or infor-
6 mation assurance at an awardee institution;
7 and
8 (C) accept the terms of a scholarship pur-
9 suant to this section.
10 (2) SELECTION.—Individuals shall be selected
11 to receive scholarships primarily on the basis of aca-
12 demic merit, with consideration given to financial
13 need and to the goal of promoting the participation
14 of individuals identified in section 33 or 34 of the
15 Science and Engineering Equal Opportunities Act
16 (42 U.S.C. 1885a or 1885b).
17 (3) SERVICE OBLIGATION.—If an individual re-
18 ceives a scholarship under this section, as a condi-
19 tion of receiving such scholarship, the individual
20 upon completion of their degree must serve as a cy-
21 bersecurity professional within the Federal workforce
22 for a period of time equal to the length of the schol-
23 arship. If a scholarship recipient is not offered em-
24 ployment by a Federal agency or a federally funded
25 research and development center, the service require-

1 ment can be satisfied at the Director's discretion
2 by—
3 (A) serving as a cybersecurity professional
4 in a State, local, or tribal government agency;
5 or
6 (B) teaching cybersecurity courses at an
7 institution of higher education.
8 (4) CONDITIONS OF SUPPORT.—As a condition
9 of acceptance of a scholarship under this section, a
10 recipient shall agree to provide the awardee institu-
11 tion with annual verifiable documentation of employ-
12 ment and up-to-date contact information.
13 (d) FAILURE TO COMPLETE SERVICE OBLIGATION.—
14 (1) GENERAL RULE.—If an individual who has
15 received a scholarship under this section—
16 (A) fails to maintain an acceptable level of
17 academic standing in the educational institution
18 in which the individual is enrolled, as deter-
19 mined by the Director;
20 (B) is dismissed from such educational in-
21 stitution for disciplinary reasons;
22 (C) withdraws from the program for which
23 the award was made before the completion of
24 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

1 amount of awards received by the individual
2 under this section shall be repaid or such
3 amount shall be treated as a loan to be repaid
4 in accordance with subparagraph (C).
5 (B) MORE THAN ONE YEAR OF SERVICE.—
6 If a circumstance described in subparagraph
7 (D) or (E) of paragraph (1) occurs after the
8 completion of 1 year of a service obligation
9 under this section, the total amount of scholar-
10 ship awards received by the individual under
11 this section, reduced by the ratio of the number
12 of years of service completed divided by the
13 number of years of service required, shall be re-
14 paid or such amount shall be treated as a loan
15 to be repaid in accordance with subparagraph
16 (C).
17 (C) REPAYMENTS.—A loan described in
18 subparagraph (A) or (B) shall be treated as a
19 Federal Direct Unsubsidized Stafford Loan
20 under part D of title IV of the Higher Edu-
21 cation Act of 1965 (20 U.S.C. 1087a and fol-
22 lowing), and shall be subject to repayment, to-
23 gether with interest thereon accruing from the
24 date of the scholarship award, in accordance
25 with terms and conditions specified by the Di-

1 rector (in consultation with the Secretary of
2 Education) in regulations promulgated to carry
3 out this paragraph.
4 (4) COLLECTION OF REPAYMENT.—
5 (A) IN GENERAL.—In the event that a
6 scholarship recipient is required to repay the
7 scholarship under this subsection, the institu-
8 tion providing the scholarship shall—
9 (i) be responsible for determining the
10 repayment amounts and for notifying the
11 recipient and the Director of the amount
12 owed; and
13 (ii) collect such repayment amount
14 within a period of time as determined
15 under the agreement described in para-
16 graph (2), or the repayment amount shall
17 be treated as a loan in accordance with
18 paragraph (3)(C).
19 (B) RETURNED TO TREASURY.—Except as
20 provided in subparagraph (C) of this para-
21 graph, any such repayment shall be returned to
22 the Treasury of the United States.
23 (C) RETAIN PERCENTAGE.—An institution
24 of higher education may retain a percentage of
25 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.

1 (f) AUTHORIZATION OF APPROPRIATIONS.—There
2 are authorized to appropriated to the National Science
3 Foundation to carry out this section—
4 (1) $18,700,000 for fiscal year 2010;
5 (2) $20,100,000 for fiscal year 2011;
6 (3) $21,600,000 for fiscal year 2012;
7 (4) $23,300,000 for fiscal year 2013; and
8 (5) $25,000,000 for fiscal year 2014.

9 **SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.**

10 Not later than 180 days after the date of enactment
11 of this Act the President shall transmit to the Congress
12 a report addressing the cybersecurity workforce needs of
13 the Federal Government. The report shall include—
14 (1) an examination of the current state of and
15 the projected needs of the Federal cybersecurity
16 workforce, including a comparison of the different
17 agencies and departments, and an analysis of the ca-
18 pacity of such agencies and departments to meet
19 those needs;
20 (2) an analysis of the sources and availability of
21 cybersecurity talent, a comparison of the skills and
22 expertise sought by the Federal Government and the
23 private sector, and an examination of the current
24 and future capacity of United States institutions of
25 higher education to provide cybersecurity profes-

1 sionals with those skills sought by the Federal Gov-
2 ernment and the private sector;
3 (3) an examination of the effectiveness of the
4 National Centers of Academic Excellence in Infor-
5 mation Assurance Education, the Centers of Aca-
6 demic Excellence in Research, and the Federal
7 Cyber Scholarship for Service programs in pro-
8 moting higher education and research in cybersecu-
9 rity and information assurance and in producing a
10 growing number of professionals with the necessary
11 cybersecurity and information assurance expertise;
12 (4) an analysis of any barriers to the Federal
13 Government recruiting and hiring cybersecurity tal-
14 ent, including barriers relating to compensation, the
15 hiring process, job classification, and hiring flexibili-
16 ties; and
17 (5) recommendations for Federal policies to en-
18 sure an adequate, well-trained Federal cybersecurity
19 workforce.
20 **SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK**
21 **FORCE.**
22 (a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY
23 TASK FORCE.—Not later than 180 days after the date of
24 enactment of this Act, the Director of the Office of Science
25 and Technology Policy shall convene a task force to ex-

1 plore mechanisms for carrying out collaborative research
2 and development activities for cybersecurity through a
3 consortium or other appropriate entity with participants
4 from institutions of higher education and industry.
5 (b) FUNCTIONS.—The task force shall—
6 (1) develop options for a collaborative model
7 and an organizational structure for such entity
8 under which the joint research and development ac-
9 tivities could be planned, managed, and conducted
10 effectively, including mechanisms for the allocation
11 of resources among the participants in such entity
12 for support of such activities;
13 (2) propose a process for developing a research
14 and development agenda for such entity, including
15 guidelines to ensure an appropriate scope of work fo-
16 cused on nationally significant challenges and requir-
17 ing collaboration;
18 (3) define the roles and responsibilities for the
19 participants from institutions of higher education
20 and industry in such entity;
21 (4) propose guidelines for assigning intellectual
22 property rights and for the transfer of research and
23 development results to the private sector; and

1 (5) make recommendations for how such entity
2 could be funded from Federal, State, and nongovern-
3 mental sources.
4 (c) COMPOSITION.—In establishing the task force
5 under subsection (a), the Director of the Office of Science
6 and Technology Policy shall appoint an equal number of
7 individuals from institutions of higher education and from
8 industry with knowledge and expertise in cybersecurity.
9 (d) REPORT.—Not later than 12 months after the
10 date of enactment of this Act, the Director of the Office
11 of Science and Technology Policy shall transmit to the
12 Congress a report describing the findings and rec-
13 ommendations of the task force.

14 **SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND**
15 **DISSEMINATION.**

16 Section 8(c) of the Cybersecurity Research and De-
17 velopment Act (15 U.S.C. 7406(c)) is amended to read
18 as follows:
19 ''(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—
20 ''(1) IN GENERAL.—The Director of the Na-
21 tional Institute of Standards and Technology shall
22 develop or identify and revise or adapt as necessary,
23 checklists, configuration profiles, and deployment
24 recommendations for products and protocols that
25 minimize the security risks associated with each

1 computer hardware or software system that is, or is
2 likely to become, widely used within the Federal
3 Government.
4 "(2) PRIORITIES FOR DEVELOPMENT.—The Di-
5 rector of the National Institute of Standards and
6 Technology shall establish priorities for the develop-
7 ment of checklists under this subsection. Such prior-
8 ities may be based on the security risks associated
9 with the use of each system, the number of agencies
10 that use a particular system, the usefulness of the
11 checklist to Federal agencies that are users or po-
12 tential users of the system, or such other factors as
13 the Director determines to be appropriate.
14 "(3) EXCLUDED SYSTEMS.—The Director of
15 the National Institute of Standards and Technology
16 may exclude from the requirements of paragraph (1)
17 any computer hardware or software system for
18 which the Director determines that the development
19 of a checklist is inappropriate because of the infre-
20 quency of use of the system, the obsolescence of the
21 system, or the inutility or impracticability of devel-
22 oping a checklist for the system.
23 "(4) AUTOMATION SPECIFICATIONS.—The Di-
24 rector of the National Institute of Standards and
25 Technology shall develop automated security speci-

1 fications (such as the Security Content Automation
2 Protocol) with respect to checklist content and asso-
3 ciated security related data.
4 "(5) DISSEMINATION OF CHECKLISTS.—The
5 Director of the National Institute of Standards and
6 Technology shall ensure that any product developed
7 under the National Checklist Program for any infor-
8 mation system, including the Security Content Auto-
9 mation Protocol and other automated security speci-
10 fications, is made available to Federal agencies.
11 "(6) AGENCY USE REQUIREMENTS.—Federal
12 agencies shall use checklists developed or identified
13 under paragraph (1) to secure computer hardware
14 and software systems. This paragraph does not—
15 "(A) require any Federal agency to select
16 the specific settings or options recommended by
17 the checklist for the system;
18 "(B) establish conditions or prerequisites
19 for Federal agency procurement or deployment
20 of any such system;
21 "(C) imply an endorsement of any such
22 system by the Director of the National Institute
23 of Standards and Technology; or
24 "(D) preclude any Federal agency from
25 procuring or deploying other computer hard-

1 ware or software systems for which no such
2 checklist has been developed or identified under
3 paragraph (1).''.

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

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

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

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

21 ''(2) carry out research associated with improv-
22 ing the security of information systems and net-
23 works;

"(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

1 Congress a proactive plan to engage international
2 standards bodies with respect to the development of
3 technical standards related to cybersecurity.

4 **SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND**
5 **EDUCATION.**

6 (a) PROGRAM.—The Director, in collaboration with
7 relevant Federal agencies, industry, educational institu-
8 tions, and other organizations, shall develop and imple-
9 ment a cybersecurity awareness and education program to
10 increase public awareness of cybersecurity risks, con-
11 sequences, and best practices through—

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

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

19 (b) MANUFACTURING EXTENSION PARTNERSHIP.—
20 The Director shall, to the extent appropriate, implement
21 subsection (a) through the Manufacturing Extension Part-
22 nership program under section 25 of the National Insti-
23 tute of Standards and Technology Act (15 U.S.C. 278k).

24 (c) REPORT TO CONGRESS.—Not later than 90 days
25 after the date of enactment of this Act, the Director shall

1 transmit to the Congress a report containing a strategy
2 for implementation of this section.

3 **SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
4 **OPMENT.**

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

9 (1) improve interoperability among identity
10 management technologies;

11 (2) strengthen authentication methods of iden-
12 tity management systems; and

13 (3) improve privacy protection in identity man-
14 agement systems, including health information tech-
15 nology systems, through authentication and security
16 protocols.

AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 4061 OFFERED BY MR. LUJÁN OF NEW MEXICO

Page 12, line 8, insert "throughout all regions of the United States" after "higher education".

Page 27, line 17, strike "State and local" and insert "State, local, and tribal".

☒

AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 4061 OFFERED BY MR. MCCAUL OF TEXAS

Page 24, line 6, strike ''any product developed'' and insert ''Federal agencies are informed of the availability of any product developed or identified''.

Page 24, line 10, strike '', is made available to Federal agencies''.

Page 24, lines 11 through 14, strike ''Federal agencies'' and all that follows through ''paragraph does not'' and insert ''The development of a checklist under paragraph (1) for a computer hardware or software system does not''

AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 4061 OFFERED BY MR. WU OF OREGON

Page 28, line 12, strike "and".

Page 28, line 16, strike the period and insert "; and".

Page 28, after line 16, insert the following new paragraph:

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

☒