113TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
113–33

CYBERSECURITY ENHANCEMENT ACT OF 2013

APRIL 11, 2013.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SMITH of Texas, from the Committee on Science, Space, and Technology, submitted the following

R E P O R T

[To accompany H.R. 756]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 756) 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.	Amendment	2
II.	Purpose and Summary	10
III.	Background and Need for the Legislation	10
IV.	Hearing Summary	12
V.	Committee Consideration	13
VI.	Committee Votes	13
VII.	Summary of Major Provisions of the Bill	15
VIII.	Committee Views	16
IX.	Committee Oversight Findings	18
X.	Statement on General Performance Goals and Objectives	18
XI.	New Budget Authority, Entitlement Authority, and Tax Expenditures	18
XII.	Advisory on Earmarks	18
XIII.	Committee Cost Estimate	18
XIV.	Congressional Budget Office Cost Estimate	19
XV.	Federal Mandates Statement	21
XVI.	Compliance with House Resolution 5	21
XVII.	Federal Advisory Committee Statement	21
XVIII.	Applicability to Legislative Branch	21
XIX.	Section-by-Section Analysis of the Legislation	21
XX.	Changes in Existing Law Made by the Bill, As Reported	24
XXI.	Proceedings of the Full Committee Markup	31

I. AMENDMENT

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 2013".

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'."; and

(4) by amending paragraph (6) to read as follows:

"(6) 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, and to protect consumer privacy;

(3) describe how the Program will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the

timely 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;

(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; and

(7) describe how the Program will help to recruit and prepare veterans for the Federal cybersecurity workforce.

(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 community colleges, National Laboratories, 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)).

(f) CYBERSECURITY RESEARCH DATABASE.—The agencies involved in developing and updating the strategic plan under subsection (a) shall establish, in coordination with the Office of Management and Budget, a mechanism to track ongoing and completed Federal cybersecurity research and development projects and associated funding, and shall make such information publically available.

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, and user motivations.".

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—

(1) in subparagraph (A) by inserting "identity management," after "cryptography,"; and

(2) in subparagraph (I), by inserting ", crimes against children, and organized crime" after "intellectual property".

(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) $119,000,000 for fiscal year 2014;

"(B) $119,000,000 for fiscal year 2015; and

"(C) $119,000,000 for fiscal year 2016.".

(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) in paragraph (7) by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $5,000,000 for fiscal year 2014;

"(B) $5,000,000 for fiscal year 2015; and

"(C) $5,000,000 for fiscal year 2016.".

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $25,000,000 for fiscal year 2014;

"(B) $25,000,000 for fiscal year 2015; and

"(C) $25,000,000 for fiscal year 2016.".

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $4,000,000 for fiscal year 2014;

"(B) $4,000,000 for fiscal year 2015; and

"(C) $4,000,000 for fiscal year 2016.".

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $32,000,000 for fiscal year 2014;

"(B) $32,000,000 for fiscal year 2015; and

"(C) $32,000,000 for fiscal year 2016.".

(g) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is repealed.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Scholarship for Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) 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, including community colleges, 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 community colleges;

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

(D) public-private partnerships that will integrate research experiences and hands-on learning into cybersecurity degree programs.

(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, to the goal of promoting the participation of females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b), and to veterans. For purposes of this paragraph, the term "veteran" means a person who—

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

(B) served on active duty (other than active duty for training) in the Armed Forces of the United States and was discharged or released from such service for a service-connected disability before serving 180 consecutive days.

For purposes of subparagraph (B), the term "service-connected" has the meaning given such term under section 101 of title 38, United States Code.

(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 as provided in paragraph (5). 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.

(5) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this subsection shall be 1 year more than the number of years for which the scholarship was received.

(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.—

(1) APPOINTMENT IN EXCEPTED SERVICE.—Notwithstanding any provision of chapter 33 of title 5, United States Code, governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the academic program for which a scholarship was awarded.

(2) NONCOMPETITIVE CONVERSION.—Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) TIMING OF CONVERSION.—An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) AUTHORITY TO DECLINE CONVERSION.—An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

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, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector, and a description of how successful programs are engaging the talents of females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b);

(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 as-

surance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise, including individuals from States or regions in which the unemployment rate exceeds the national average;

(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, development, education, and training 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) identify and prioritize at least three cybersecurity grand challenges, focused on nationally significant problems requiring collaborative and interdisciplinary solutions;

(3) propose a process for developing a research and development agenda for such entity to address the grand challenges identified under paragraph (2);

(4) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(5) propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector; and

(6) 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, including minority-serving institutions and community colleges, 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.

(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.

SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.

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

"(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security 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 standards, reference materials, and checklists under this subsection on the basis of—

"(A) the security risks associated with the use of the system;

"(B) the number of agencies that use a particular system or security tool;

"(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

"(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

"(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or 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 standard, reference material, or checklist for the system.

"(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

"(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

"(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or 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 information technology hardware or software systems for which no such standard, reference material, or 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;

"(4) carry out research associated with improving security of industrial control systems; and

"(5) carry out research associated with improving the security and integrity of the information technology supply chain.".

SEC. 111. RESEARCH ON THE SCIENCE OF CYBERSECURITY.

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall, through existing programs and activities, support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

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.

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

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a plan for ensuring such Federal agency coordination.

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

SEC. 203. CLOUD COMPUTING STRATEGY.

(a) IN GENERAL.—The Director, in collaboration with the Federal CIO Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(b) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(3) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(A) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(B) to ensure secure access to the data stored in cloud computing data centers;

(C) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3); and

(D) to support the development of the automation of continuous monitoring systems.

SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, National Laboratories, the National Coordination Office of the Networking and Information Technology Research and Development program, and other organizations, shall continue to coordinate a cybersecurity awareness and education program to increase knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through—

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

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

(3) improving the state of cybersecurity education at all educational levels;

(4) efforts to attract, recruit, and retain qualified professionals to the Federal cybersecurity workforce; and

(5) improving the skills, training, and professional development of the Federal cybersecurity workforce.

(b) STRATEGIC PLAN.—The Director shall, in cooperation with relevant Federal agencies and other stakeholders, develop and implement a strategic plan to guide Federal programs and activities in support of a comprehensive cybersecurity awareness and education program as described under subsection (a).

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

SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall continue 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.

SEC. 206. AUTHORIZATIONS.

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

II. PURPOSE AND SUMMARY

The purpose of H.R. 756 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 Federal agency engagement in international cybersecurity technical standards development; and the 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. Recent reports of cyber criminals and nation-states accessing sensitive information and disrupting services in both the public and private domains have risen steadily, heightening concerns over the adequacy of our cybersecurity measures. GAO found that the number of incidents reported by federal agencies has increased 782 percent from 2006 to 2012.[1] This dramatic increase is attributed in part to the proliferation and increased sophistication of hacking and cyber attack technology.

According to the Office of Management and Budget, Federal agencies spent $8.6 billion in fiscal year 2010 on cybersecurity and the Federal government has spent more than $600 billion on information technology in the last decade. In addition, the Federal government funds more than $400 million in cybersecurity research and development each year.

In January 2008, the Bush Administration established, through a series of classified executive directives, the Comprehensive National Cybersecurity Initiative (CNCI). The Obama Administration has continued this initiative, with the goal of securing Federal systems and fostering public-private cooperation.

On May 29, 2009, the Obama Administration released its *Cyberspace Policy Review.* The Review recommended an increased level of interagency cooperation among all departments and agencies, highlighted the need for information sharing concerning attacks and vulnerabilities, and highlighted the need for an exchange of re-

[1] GAO–13–187, Cybersecurity, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented; http://www.gao.gov/assets/660/652170.pdf, February 2013.

search and security strategies essential to the efficient and effective defense of Federal computer systems. Furthermore, it stressed the importance of advancing cybersecurity research and development, and the need for the Federal Government to partner with the private sector to guarantee a secure and reliable infrastructure. The Review also called for increased public awareness, improved education and expansion of the number of information technology professionals.

In June 2009, GAO found that the Federal agencies responsible for protecting the U.S. information technology (IT) infrastructure were not satisfying their responsibilities, leaving the Nation's IT infrastructure vulnerable to attack. In an effort to strengthen the work of those Federal agencies, the U.S. House of Representatives passed the *Cybersecurity Enhancement Act of 2010* (H.R. 4061) in the 111th Congress by a vote of 422–5. H.R. 4061 required increased coordination and prioritization of Federal cybersecurity research and development activities, and the development and advancement of cybersecurity technical standards. It also strengthened cybersecurity education and talent development and industry partnership initiatives. Similar legislation (H.R. 2096) was considered by the House in the 112th Congress and passed by a vote of 395–10. The Senate did not act on the legislation in the 111th or 112th Congress.

The task of coordinating unclassified cybersecurity research and development (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 15 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.

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), although the effort is increasingly interdisciplinary. CISE supports cybersecurity R&D through a targeted program, Secure and Trustworthy Cyberspace, 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 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 Standards [FIPS]), identifying methods for assessing effectiveness of security requirements, conducting tests to

validate security in information systems, and conducting outreach exercises. NIST's technical standards and best practices are sometimes 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. Recognizing that private sector standards development organizations also are engaged in international standards work, in some scenarios a nonfederal entity may be best equipped to represent United States interests, and coordination is necessary.

Experts have also noted that the identification of grand challenges for cybersecurity R&D could help prioritize activities across the federal government.

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

In the 111th Congress, the House Committee on Science and Technology held four subcommittee hearings to explore the state of Federal cybersecurity research and development, education, and workforce training programs; to review the findings and recommendations included in the Administration's *Cyberspace Policy Review*; to examine ways Federal cybersecurity efforts could enhance privately-owned critical infrastructure, better monitor Federal networks, and more clearly define performance metrics and success criteria; and to review the findings and recommendations of a report from the Government Accountability Office (GAO).[2] Both the review and the report called for an increase in effective public/private partnerships, and for clarification of agency roles and responsibilities. As a result of information gathered from the hearings, H.R. 4061, the *Cybersecurity Enhancement Act*, was introduced on a bipartisan basis on November 7, 2009. The Science and Technology Committee favorably reported the bill on January 27, 2010, and the House passed the measure on February 4, 2010 by a vote of 422–5. The Senate did not act on this measure prior to the adjournment of the 111th Congress.

In the 112th Congress, the Subcommittee on Technology and Innovation and the Subcommittee on Research and Science Education

[2] *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, Government Accountability Office, http://www.gao.gov/new.items/d09432t.pdf.

held a joint hearing on May 25, 2011, to examine Federal agency efforts to improve our national cybersecurity and prepare the future cybersecurity talent needed for national security. The hearing included updates from the agencies on how they are responding to and addressing objectives of the 2009 *Cyberspace Policy Review*, their efforts to educate and develop the necessary cybersecurity personnel, and how standards development is coordinated with other relevant agencies.

In the 113th Congress, the Subcommittee on Technology and the Subcommittee on Research held a joint hearing on February 26, 2013, to hear from industry and academic stakeholders about the R&D needs for cybersecurity and to receive comments on H.R. 756, the *Cybersecurity Enhancement Act of 2013.*

V. Committee Consideration

On February 15, 2013, Representative Mike McCaul (R–TX), for himself, and Representative Daniel Lipinski (D–IL), introduced H.R. 756, the *Cybersecurity Enhancement Act of 2013*, a bill to advance cybersecurity research, development, and technical standards, and for other purposes. H.R. 756 was referred to the Committee on Science, Space, and Technology.

On March 14, 2013, the Committee on Science, Space, and Technology met in open markup session and ordered H.R. 756 favorably reported to the House, as amended, by voice vote.

VI. Committee Votes

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. A motion to order H.R. 756 favorably reported to the House, as amended, was agreed to by voice vote.

During Full Committee consideration of H.R. 756, the following amendments were considered:

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
Full Committee Markup
March 14, 2013

AMENDMENT ROSTER

H.R. 756, "Cybersecurity Enhancement Act of 2013"

No.	Amendment	Summary	
1	Amendment offered by Mr. Smith (TX) (009)	Reauthorizes NSF research grants for three years to match current spending levels; Requires the university-industry task force to identify and prioritize grand challenges for cybersecurity R&D; Requires agencies to track R&D projects; Adds education programs and cybersecurity workforce development to NIST awareness and education program; Amends federal hiring authority for Scholarship for Service Program graduates	Agreed to by Voice Vote
2	Amendment offered by Mr. Bera (CA) (003)	Amends the Cybersecurity Strategic Research and Development Plan to add into the contents of the plan a description of how the Networking and Information Technology Research and Development Program prepares veterans for the Federal cybersecurity workforce.	Agreed to by Voice Vote
3	Amendment offered by Mr. Grayson (FL) (057)	Amends the Federal Cyber Scholarship for Service Program to include community colleges as eligible for Scholarship for Service grants.	Agreed to by Voice Vote
4	Amendment offered by Mr. Kilmer (WA) (002)	Amends the Federal Cyber Scholarship for Service Program, to allow support for course evaluation and public-private partnership activities conducted at institution of higher education.	Agreed to by Voice Vote
5	Amendment offered by Mr. Grayson (FL) (056)	Amends the Federal Cyber Scholarship for Service Program to add females to the individuals to be considered for the Scholarship for Service Program.	Agreed to by Voice Vote
6	Amendment offered by Mr. Grayson (FL) (054)	Directs NIST to conduct research into improving the security and integrity of the information technology supply chain.	Agreed to by Voice Vote
7	Amendment offered by Ms. Wilson (FL) (002)	Creates a new section which directs NSF and NIST to conduct research on the development of the scientific framework underlying cybersecurity.	Agreed to by Voice Vote

VII. Summary of Major Provisions of the Bill

H.R. 756, the *Cybersecurity Enhancement Act of 2013,* coordinates research and related activities conducted across the Federal agencies to better address evolving cyber threats. By strengthening agency coordination and cooperation on cybersecurity research and development efforts, the legislation addresses certain critical aspects of our nation's overall cybersecurity needs.

In addition to providing coordination of cybersecurity research across the federal government, the bill strengthens the efforts of the NSF and the NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development.

The bill is identical to legislation in the 112th Congress, H.R. 2096, which passed the House by a vote of 395–10.

The bill requires that the agencies participating in the National Information Technology Research and Development (NITRD) program develop a strategic plan to guide the overall direction of Federal cybersecurity and information assurance R&D. It requires the agencies to solicit recommendations and advice from the advisory committee and a wide range of stakeholders and that they develop an implementation roadmap for the strategic plan.

The bill 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. It also requires the President to conduct an assessment of cybersecurity workforce needs across the Federal government and formally codifies NSF to carry out the Scholarship for Service program.

Additionally, the bill reauthorizes cybersecurity research at NSF and it requires that the Director of the Office of Science and Technology Policy convene a university-industry task force to identify grand challenges and explore mechanisms for carrying out collaborative R&D.

The bill tasks both NSF and NIST with conducting research to improve the scientific foundations of cybersecurity.

The bill amends section 8(c) of the *Cybersecurity R&D Act* (15 U.S.C. 7406(c)) by requiring the Director of NIST to develop and revise as necessary, security automation standards, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each information technology hardware or software system used by the Federal government. The bill also amends section 20 of the *NIST Act* (15 U.S.C. 278g–3), by directing NIST to conduct a research program aimed at creating a standardized identity, privilege, and access control management framework that can be used to enforce a wide variety of resource protection policies. The framework should be usable in a wide variety of existing and emerging computing environments. The bill also directs NIST to conduct research on how to improve the security of information systems, networks, supply chains, and industrial control systems.

The bill directs NIST to coordinate with other Federal agencies and private sector stakeholders involved in international cybersecu-

rity technical standards development and to report to Congress on a plan to conduct this coordination within one year of enactment.

NIST is also required to deliver a plan to Congress, within one year of enactment, describing how it will continue to coordinate a cybersecurity awareness and education program. NIST is to collaborate with relevant Federal agencies, National Laboratories, industry and educational institutions in developing this program. The purpose of the program is to disseminate cybersecurity best practices and standards and improve cybersecurity education and federal workforce recruitment and retention. NIST is also directed to develop a strategic plan to implement the program.

The bill directs NIST to engage in research and development programs to improve identity management systems. The programs have the goals of improving interoperability among identity management technologies, strengthening authentication methods, and improving privacy protection.

The bill clarifies that no additional funds are authorized for programs in the bill.

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 dropped 35 percent from 2004 to 2008. 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, including community colleges, to produce cybersecurity professionals is an essential first step in ensuring an adequate, well-trained workforce.

As part of the Workforce Training Assessment, the Committee expects that any assessment of education and training activities also include activities considered to be outside the scope of a classroom such as simulations and competitions. 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)(3) of this section, 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.

The Committee recognizes that in order for the United States to adequately protect itself from cybersecurity threats a strong partnership between the Federal government and the private sector must be built and maintained. In particular, the Committee believes active and lasting engagement between the federal science agencies, academia, and the private sector will ensure that cybersecurity research and development, education, and training activities are relevant not only for the current cybersecurity landscape, but will ultimately result in a more secure future environment. The Committee expects that the university-industry taskforce will develop a model that that will allow for such long-term collaboration.

NIST's security automation and 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.

International cybersecurity technical standards

The Committee intends for NIST to coordinate Federal agency engagement in international cybersecurity technical standards development, in partnership with relevant Federal agencies. This pro-

vision is meant to recognize that coordinating cybersecurity standards efforts across different Federal agencies will ensure appropriate governmental representation at international standard dialogues. Furthermore, in some instances it may not be appropriate for Federal agencies to be directly involved in the development of international cybersecurity technical standards. Therefore, consultation with private stakeholders is also required to determine the appropriate level of engagement, if any, by Federal agencies in specific international cybersecurity technical standards matters. 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.

Cloud computing strategy

The Committee recognizes the economic potential of the public and private sector's utilization of cloud computing. However, stakeholders must be certain their information will be secure in the cloud. NIST, working in close conjunction with industry, is well-positioned to provide standards and protocols to ensure that the cloud is a safe system for the Federal government to utilize.

IX. Committee Oversight Findings

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held an oversight hearing and made findings that are reflected in the descriptive portions of this report.

X. Statement on General Performance Goals and Objectives

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the performance goals and objectives of the Committee are reflected in the descriptive portions of this report, including the goal to improve cybersecurity in the Federal, private, and public sectors and to protect the Nation's critical infrastructure.

XI. New Budget Authority, Entitlement Authority, and Tax Expenditures

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XII. Advisory on Earmarks

In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 756, the *Cybersecurity Enhancement Act of 2013*, contains no earmarks.

XIII. Committee Cost Estimate

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XIV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 1, 2013.

Hon. LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 756, the Cybersecurity Enhancement Act of 2013.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Martin von Gnechten.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 756—Cybersecurity Enhancement Act of 2013

Summary: H.R. 756 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 continue a cybersecurity awareness program and to develop standards for managing personal identifying information stored on computer systems. Finally, the bill would establish a task force to recommend actions to the Congress for improving research and development activities related to cybersecurity.

Based on information from NSF and NIST and assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 756 would cost $504 million over the 2014–2018 period and $52 million after 2018. Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

H.R. 756 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. 756 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—					
	2014	2015	2016	2017	2018	2014–2018
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
NSF Cybersecurity Research Grants:						
Authorization Level	119	119	119	0	0	357
Estimated Outlays	15	63	94	96	55	324
NSF Cybersecurity Research Centers:						
Authorization Level	5	5	5	0	0	15
Estimated Outlays	1	3	4	4	2	14

	By fiscal year, in millions of dollars—					
	2014	2015	2016	2017	2018	2014–2018
NSF Cybersecurity Capacity Building Grants:						
Authorization Level	25	25	25	0	0	75
Estimated Outlays	3	13	20	20	12	68
NSF Science and Advanced Technology Grants:						
Authorization Level	4	4	4	0	0	12
Estimated Outlays	1	2	3	3	2	11
NSF Cybersecurity Graduate Traineeships:						
Authorization Level	32	32	32	0	0	96
Estimated Outlays	4	17	25	26	15	87
Cybersecurity Task Force:						
Estimated Authorization Level	1	0	0	0	0	1
Estimated Outlays	1	0	0	0	0	1
Total Changes under H.R. 756:						
Estimated Authorization Level	186	185	185	0	0	556
Estimated Outlays	25	98	146	150	85	504

Notes: NSF = National Science Foundation.
Amounts may not sum to totals because of rounding.

Basis of estimate: For this estimate, CBO assumes that H.R. 756 will be enacted in fiscal year 2013 and that the authorized and necessary amounts will be appropriated each fiscal year beginning in 2014. Estimated outlays are based on historical spending patterns for NSF programs.

H.R. 756 would authorize appropriations for several NSF grant programs aimed at enhancing cybersecurity. The bill would authorize appropriations totaling $357 million over the 2014–2016 period to improve research on cybersecurity. In addition, H.R. 756 would authorize the appropriation of:

- $15 million for grants to establish centers of cybersecurity research;
- $75 million for grants to universities to improve cybersecurity programs and increase the number of students in fields related to cybersecurity. This includes a program to offer scholarships to students who pursue higher education related to cybersecurity and commit to public service after graduating;
- $12 million for grants to institutions that grant associate degrees to develop cybersecurity programs and establish centers of excellence; and
- $96 million for grants to higher education institutions to establish cybersecurity traineeship programs for graduate students.

H.R. 756 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 similar activities, CBO estimates that carrying out this provision would cost $1 million in 2014.

H.R. 756 also would direct NIST to establish standards and protocols to enhance cybersecurity, develop a strategy for the government to adopt cloud computing services (the use of servers and network storage to provide remote, on-demand access to shared computer applications and services), and promote cybersecurity awareness and education. Based on information from NIST, CBO estimates that these activities would have no significant impact on the federal budget because NIST currently performs similar activities under its existing authority.

Pay-As-You-Go consideration: None.

Intergovernmental and private-sector impact: H.R. 756 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments. Institutions of higher education, including those that are publicly owned, may benefit from grants that help expand the professional development of faculty in cybersecurity-related courses and curricula.

Estimate prepared by: Federal costs: Martin von Gnechten; Impact on state, local, and tribal governments: J'nell Blanco; Impact on the private sector: Amy Petz.

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

XV. Federal Mandates Statement

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

XVI. Compliance with H. Res. 5

A. Directed Rule Making. The Committee does not believe that this bill directs any executive branch official to conduct any specific rule-making proceedings.

B. Duplication of Existing Programs. The Committee is not aware of another established or authorized program of the Federal government which duplicates the program in the bill. H.R. 756 coordinates cyber security programs and eliminates duplications as recommended by the Government Accountability Office (GAO) in its report to Congress pursuant to section 21 of Public Law 111–139. Because of the interdisciplinary nature of NSF, the Catalog of Federal Domestic Assistance identifies all programs at NSF at the directorate level and views such programs as related; however, specific activities at NSF, such as those included in H.R. 756, are not identified in the CFDA. H.R. 756 directs certain organizational units of NSF listed in the CFDA to make grants for specific purposes, but does not create new units or duplicate the activities.

XVII. Federal Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

XVIII. Applicability to Legislative Branch

The Committee finds that the legislation 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.

XIX. 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.

Also requires agencies involved in the strategic plan to establish a mechanism to track ongoing and completed R&D projects and make that information available to the public.

Sec. 104. Social and behavioral research in cybersecurity

Adds research on the social and behavioral aspects of cybersecurity to the list of cybersecurity research areas that the National Science Foundation may support 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.

Repeals NSF cybersecurity faculty development traineeship program.

Sec. 106. Federal cybersecurity 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 additional year of service over the number of years for which the scholarship was received.

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

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 cybersecruity 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 focused on grand challenges for 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 for the federal government, 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 codify NIST cybersecurity research and development activities; NIST is authorized to conduct research on the development of a unifying and standardized identity, privilege, and access control management framework and to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.

Sec. 111. Research on the science of cybersecurity

Requires NSF and NIST to support research to develop scientific foundations for cybersecurity leading to better metrics and definitions.

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 consult with the private sector and others 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. Cloud computing strategy

Directs NIST, in collaboration with Federal agencies and other stakeholders, to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government. The strategy should consider activities that accelerate standards development, the development of processes to test standards conformance, and the security of data stored in the cloud.

Sec. 204. Promoting cybersecurity awareness and education

Requires NIST to continue a cybersecurity awareness and education program and to deliver a strategic plan to Congress within 1 year describing the implementation of this program. Requires the program to be aimed at disseminating cybersecurity best practices

and standards and improving cybersecurity education and federal workforce recruitment and retention.

Sec. 205. Identity management research and development

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

Sec. 206. Authorizations

States that no additional funds are authorized for the activities in the bill.

XX. 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 mil-

lions of dollars and nation-states and other entities to steal intellectual property and sensitive military information".

* * * * * * *

[(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.]

(6) 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*, crimes against children, and organized crime*[.]*; and*

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

* * * * * * *

(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) $119,000,000 for fiscal year 2014;
(B) $119,000,000 for fiscal year 2015; and
(C) $119,000,000 for fiscal year 2016.

(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.]
(A) $5,000,000 for fiscal year 2014;
(B) $5,000,000 for fiscal year 2015; and
(C) $5,000,000 for fiscal year 2016.

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.]
(A) $25,000,000 for fiscal year 2014;
(B) $25,000,000 for fiscal year 2015; and
(C) $25,000,000 for fiscal year 2016.

(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.]
(A) $4,000,000 for fiscal year 2014;
(B) $4,000,000 for fiscal year 2015; and
(C) $4,000,000 for fiscal year 2016.

(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.]
(A) $32,000,000 for fiscal year 2014;
(B) $32,000,000 for fiscal year 2015; and
(C) $32,000,000 for fiscal year 2016.

* * * * * * *

[(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 possible, 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.]

* * * * * * *

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) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security 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 standards, reference materials, and checklists under this subsection on the basis of—

(A) the security risks associated with the use of the system;

(B) the number of agencies that use a particular system or security tool;

(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or 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 standard, reference material, or checklist for the system.

(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or 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 information technology hardware or software systems for which no such standard, reference material, or 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;

(4) carry out research associated with improving security of industrial control systems; and

(5) carry out research associated with improving the security and integrity of the information technology supply chain.

[(e)] *(f)* As used in this section—

(1) * * *

* * * * * * *

XXI. PROCEEDINGS OF THE FULL COMMITTEE MARKUP ON H.R. 756, CYBERSECURITY ENHANCEMENT ACT OF 2013

THURSDAY, MARCH 14, 2012

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Committee met, pursuant to call, at 10:01 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Committee] presiding.

Chairman SMITH. The Science, Space, and Technology Committee will come to order. Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Before we start today, I would like to recognize our Clerk, Deborah Samantar. After 30 years of service in the House of Representatives, Deborah will retire at the end of this month. She has been a valuable member—and she is sitting in front of us in pink if you needed to be reminded. She has been a valuable member of the Science Committee staff for many years and has clerked under three different Science Committee chairmen beginning with Representative Bart Gordon in 2007. Deborah started her career in the House working for her home Representative from Pennsylvania, Congressman Joe Kolter. After a few years, she became an intern and fellowship coordinator for the Committee on Education and the Workforce. I think that was under John Boehner, wasn't it? She held many positions during her 20 years with the Education and Workforce Committee and worked under five different chairmen. This is an impressive record by anyone's standards, and not many people can claim such an achievement. Deborah's ability to communicate, her attention to detail and dedication to the Science Committee and the House of Representatives will be missed. We thank her for her contributions to this Committee and to our country. Deborah, we will miss you, and we wish you the best on your well-deserved retirement.

I will now recognize the Ranking Member, Ms. Johnson, for her comments.

I am glad this is a bipartisan effort, and look forward to this bill becoming law.

Ms. JOHNSON. Thank you very much, Mr. Chairman. I would like also to wholeheartedly congratulate Deborah for her 30 years of service in the House. I first met her seven years ago when she became the Clerk of the Committee under Chairman Gordon. I have always known her to be a consummate professional and dedicated

staff person to the Committee. Thirty years is quite some time. I would point out that Deborah has been working in the House longer than both myself or Chairman Smith have been here, and I hope that in retirement Deborah will be able to spend more time with her mother in Pennsylvania and traveling to her favorite vacation spots in the Bahamas. After 30 years of service to the House, I think you deserve a little fun in the sun. Thank you for all that you have done for the Committee and for the Nation.

Chairman SMITH. Thank you, Ms. Johnson.

We will now move on to the Committee's official business of the day, and the Clerk, Deborah, will call the roll to establish a quorum.

The CLERK. Good morning. Thank you all very much.
Chairman Smith?
Chairman SMITH. Present.
The CLERK. Chairman Smith is present.
Mr. Sensenbrenner?
Mr. Hall? Mr. Hall?
Mr. HALL. Present.
The CLERK. Mr. Hall is present.
Mr. Rohrabacher?
Mr. ROHRABACHER. Present.
The CLERK. Mr. Rohrabacher is present.
Mr. Lucas?
Mr. Neugebauer?
Mr. McCaul?
Mr. MCCAUL. Present.
The CLERK. Mr. McCaul is present.
Mr. Broun?
Mr. BROUN. Here.
The CLERK. Mr. Broun is present.
Mr. Palazzo?
Mr. Brooks?
Mr. BROOKS. Here.
The CLERK. Mr. Brooks is present.
Mr. Hultgren?
Mr. Bucshon?
Mr. BUCSHON. Here.
The CLERK. Mr. Bucshon is present.
Mr. Stockman?
Mr. STOCKMAN. Here.
The CLERK. Mr. Stockman is present.
Mr. Posey?
Mr. POSEY. Present.
The CLERK. Mr. Posey is present.
Ms. Lummis?
Mr. Schweikert?
Mr. Massie?
Mr. MASSIE. Present.
The CLERK. Mr. Massie is present.
Mr. Cramer?
Mr. Bridenstine?
Mr. BRIDENSTINE. Present.
The CLERK. Mr. Bridenstine is present.

Mr. Weber?
Mr. Stewart?
Ms. Johnson?
Ms. JOHNSON. Present.
The CLERK. Ms. Johnson is present.
Ms. Lofgren?
Ms. LOFGREN. Here.
The CLERK. Ms. Lofgren is present.
Mr. Lipinski?
Mr. LIPINSKI. Present.
The CLERK. Mr. Lipinski is present.
Ms. Edwards?
Ms. EDWARDS. Present.
The CLERK. Ms. Edwards is present.
Ms. Wilson?
Ms. WILSON. Present.
The CLERK. Ms. Wilson is present.
Ms. Bonamici?
Ms. BONAMICI. Present.
The CLERK. Ms. Bonamici is present.
Mr. Swalwell?
Mr. SWALWELL. Present.
The CLERK. Mr. Swalwell is present.
Mr. Maffei?
Mr. MAFFEI. Here, present.
The CLERK. Mr. Maffei is present.
Mr. Grayson?
Mr. GRAYSON. Present.
The CLERK. Mr. Grayson is present.
The CLERK. Mr. Kennedy?
Mr. KENNEDY. Present.
The CLERK. Mr. Kennedy is present.
Mr. Peters?
Mr. PETERS. Here.
The CLERK. Mr. Peters is present.
Mr. Kilmer?
Mr. KILMER. Present.
The CLERK. Mr. Kilmer is present.
Mr. Bera?
Mr. BERA. Present.
The CLERK. Mr. Bera is present.
Ms. Esty?
Ms. ESTY. Present.
The CLERK. Ms. Esty is present.
Mr. Veasey?
Mr. VEASEY. Present.
The CLERK. Mr. Veasey is present.
Ms. Brownley?
Ms. BROWNLEY. Present.
The CLERK. Ms. Brownley is present.
Mr. Takano?

Chairman SMITH. Are there any other Members who wish to record their presence? If not, the Clerk will report. The gentleman from Mississippi is——

The CLERK. Mr. Palazzo?
Mr. PALAZZO. Here.
The CLERK. Mr. Palazzo is present.
Mr. Chairman, there is 28 Members present.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
Quorum Call

Date: March 14, 2013 **Quorum: 13 to vote; 20 to report**

	MEMBER	PRESENT	NOT PRESENT
1	Mr. Smith, Texas, *Chair*	X	
2	Mr. Rohrabacher, California***	X	
3	Mr. Hall, Texas	X	
4	Mr. Sensenbrenner, Wisconsin		X
5	Mr. Lucas, Oklahoma		X
6	Mr. Neugebauer, Texas		X
7	Mr. McCaul, Texas	X	
8	Mr. Broun, Georgia	X	
9	Mr. Palazzo, Mississippi	X	
10	Mr. Brooks, Alabama	X	
11	Mr. Hultgren, Illinois		X
12	Mr. Bucshon, Indiana	X	
13	Mr. Stockman, Texas	X	
14	Mr. Posey, Florida	X	
15	Mrs. Lummis, Wyoming		X
16	Mr. Schweikert, Arizona		X
17	Mr. Massie, Kentucky	X	
18	Mr. Cramer, North Dakota		X
19	Mr. Bridenstine, Oklahoma	X	
20	Mr. Weber, Texas		X
21	Mr. Stewart, Utah		X
22	Vacancy		
1	*Ms. Johnson, Texas, Ranking Member*	X	
2	*Ms. Lofgren, California*	X	
3	*Mr. Lipinski, Illinois*	X	
4	*Ms. Edwards, Maryland*	X	
5	*Ms. Wilson, Florida*	X	
6	*Ms. Bonamici, Oregon*	X	
7	*Mr. Swalwell, California*	X	
8	*Mr. Maffei, New York*	X	
9	*Mr. Grayson, Florida*	X	
10	*Mr. Kennedy, Massachusetts*	X	
11	*Mr. Peters, California*	X	
12	*Mr. Kilmer, Washington*	X	
13	*Mr. Bera, California*	X	
14	*Ms. Esty, Connecticut*	X	
15	*Mr. Veasey, Texas*	X	
16	*Ms. Brownley, California*	X	
17	*Mr. Takano, California*		X
18	*Vacancy*		
	TOTALS	28	10

*** Vice Chair

Chairman SMITH. A working quorum is more than present, and pursuant to Committee Rule 2(f) and House Rule 11284, the Chair announces that he may postpone roll call votes on matters in which the yeas and nays are ordered until the end of the markup.

Pursuant to notice, I now call up H.R. 756, the *Cybersecurity Enhancement Act of 2013* for markup, and the Clerk will report the bill.

The CLERK. H.R. 756, a bill to advance cybersecurity research, development and technical standards, and for other purposes.

Chairman SMITH. Without objection, the bill will be considered as read.

Chairman SMITH. I will recognize myself for an opening statement and then the Ranking Member.

The first bill for today's markup is H.R. 756, the *Cybersecurity Enhancement Act of 2013*. I thank Representatives McCaul and Lipinski for introducing this bill, and I am pleased to be a cosponsor.

As our reliance on information technology expands, so do our vulnerabilities. Cyber attacks against U.S. government and private sector networks are on the rise. Protecting America's cyber systems is critical to our economic and national security. Keeping our cyber infrastructure secure is a responsibility shared by different federal agencies, including the National Science Foundation and the National Institute of Standards and Technology.

The Cybersecurity Enhancement Act coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create new technologies and standards that better protect America's information technology systems.

To improve America's cybersecurity abilities, this bill strengthens activities in four areas: one, strategic planning for cybersecurity research and development needs across the federal government; two, basic research at NSF, which we know is important to increasing security over the long-term; three, NSF scholarships to improve the quality of the cybersecurity workforce; and four, improved research, development and public outreach organized by NIST related to cybersecurity.

These are modest but important changes that will help us better protect our cyber networks. Cyber attacks threaten our national and economic security. To solve this problem, America needs a solution that involves the cooperation of many public and private sector entities. This legislation helps foster such an effort, which will make our computer systems more secure.

Many industry partners and stakeholders have written letters in support of this bill. They include the U.S. Chamber of Commerce, National Association of Manufacturers, TechAmerica, Computing Research Association, Institute of Electrical and Electronic Engineers-USA, Society for Industrial and Applied Mathematics; Financial Services Roundtable, and the U.S. Public Policy Council of the Association for Computing Machinery.

I am glad this is a bipartisan effort, and look forward to this bill becoming law.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF CHAIRMAN LAMAR SMITH

The first bill for today's markup is H.R. 756, the "Cybersecurity Enhancement Act of 2013." I thank Representatives McCaul and Lipinski for introducing this bill. And I am pleased to be a cosponsor.

As our reliance on information technology expands, so do our vulnerabilities. Cyber attacks against U.S. government and private sector networks are on the rise. Protecting America's cyber systems is critical to our economic and national security.

Keeping our cyber infrastructure secure is a responsibility shared by different Federal agencies, including the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST).

The "Cybersecurity Enhancement Act," coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create new technologies and standards that better protect America's information technology systems.

To improve America's cybersecurity abilities, this bill strengthens activities in four areas:

(1) strategic planning for cybersecurity research and development needs across the federal government;

(2) basic research at NSF, which we know is important to increasing security over the long-term;

(3) NSF scholarships to improve the quality of the cybersecurity workforce; and

(5) improved research, development and public outreach organized by NIST related to cybersecurity.

These are modest but important changes that will help us better protect our cyber networks.Cyber attacks threaten our national and economic security. To solve this problem, America needs a solution that involves the cooperation of many public and private sector entities. This legislation helps foster such an effort, which will make our computer systems more secure.

Many industry partners and stakeholders have written letters in support of this bill. They include: The U.S. Chamber of Commerce; National Association of Manufacturers; TechAmerica; Computing Research Association; Institute of Electrical and Electronic Engineers-USA; Society for Industrial and Applied Mathematics; Financial Services Roundtable; and the U.S. Public Policy Council of the Association for Computing Machinery.

Chairman SMITH. I will yield the remainder of my time to the gentleman from Texas, Mr. McCaul, the author of the bill along with Mr. Lipinski.

Mr. MCCAUL. I thank the Chairman and Ranking Member for allowing me to proceed with this bill one more time. Mr. Lipinski, I believe this is the third time we have introduced this legislation. I hope the third time is the charm.

But I do think it is important, and I appreciate how seriously the Committee is taking this issue. It is of paramount importance for our country and our Congress right now.

Earlier this week, our country's top intelligence official told a Senate panel that the United States is vulnerable to espionage, cyber crime and outright destruction of computer networks both from sophisticated and state-sponsored attacks as well as criminal hacker groups and cyber terrorists. Many of these attacks emanate out of China, Russia, and Iran. Yesterday in the Homeland Security Committee, which I chair, the DHS Deputy Secretary, Jane Lute, again affirmed the need for Congress to develop legislation to address this critical issue.

We know that foreign nations are conducting reconnaissance on our critical infrastructures and utilities including our gas lines and water systems and energy grids, and if the ability to send silent attacks through our digital networks falls into our enemies' hands, this country could be the victim of a devastating attack.

Last December, Iranians attacked the state-owned Saudi Aramco with the goal of stopping Saudi Arabia's oil production. Additionally this year, Iran conducted multiple denial-of-service attacks on major U.S. banks in the United States. Hackers have also attacked the servers of our air traffic control system. And just last year, an al-Qaeda operative issued a call for an electronic jihad against the United States, comparing our technological vulnerabilities to that of our security before 9/11.

Yet while threats are imminent, no major cybersecurity legislation that would help protect us has been enacted since 2002. Simply put, we are not prepared to meet the threats of the 21st century. Last month, the President issued an Executive Order with the intention of bolstering our cyber defenses because Congress has failed to take action. That is why Congressman Lipinski and I introduced the *Cybersecurity Enhancement Act of 2013* before this Committee today.

This Act improves coordination in the government, providing for a strategic plan to assess the cybersecurity risk and guide the overall direction of federal cyber research and development. Our federal networks are under cyber attack every day. This bill updates the National Institute of Standards and Technology's responsibilities to develop security and procurement standards for the .gov computer systems to harden these federal networks against attack. Our bill also establishes a federal university-private sector task force to coordinate research and development. It improves the training of cyber professionals and continues much-needed cybersecurity research and development programs at the National Science Foundation and the National Institute of Standards and Technology.

Additionally, this bill promotes cybersecurity awareness and education throughout the country, and when you talk to agencies like the NSA, they tell you that perhaps 80 percent of this could be prevented by proper computer hygiene.

Through a bipartisan effort, this bill passed last Congress 395 to 10. Most importantly, H.R. 756 is fiscally responsible. It is not being paid with any new money since it is intended to work within the boundaries of funds authorized and appropriated to NSF and NIST. This bill has been endorsed by leading industry groups including the U.S. Chamber of Commerce and the Computing Research Association.

We have also been working closely with NSF and NIST to ensure this bill suits their needs. I am confident this legislation will advance the work these agencies are doing to bolster our domestic cybersecurity, and I urge my colleagues to support the legislation. And with that, Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. McCaul. The gentlewoman from Texas, Ms. Johnson, the Ranking Member, is recognized for her opening statement.

Ms. JOHNSON. Thank you very much, Chairman Smith.

Today we are marking up two bipartisan pieces of legislation, H.R. 756, the *Cybersecurity Enhancement Act of 2013*, and H.R. 967, *Advancing America's Networking and Information Technology R&D Act*.

Advances in network and information technology, or NIT, are a key driver of our economy, increasing productivity and existing in-

dustries and opening the door for the formation of new ones. Small businesses use NIT to connect a wider consumer base, allowing them to grow. The military uses NIT to improve intelligence gathering and sharing as well to support many of its worldwide operations. NIT is improving health care by creating better treatment options through electronic health record keeping, advanced surgical tools, and the facilitation of medical research. And of course, Internet companies such as Google and Facebook are now worth billions of dollars and show how quickly NIT R&D can translate into real-world products.

NIT has truly revolutionized our modern way of life. However, our growing reliance on NIT to fuel our society leaves us vulnerable to cyber attacks. As the stakes have grown higher, individual hackers have given way to organized criminal groups and even foreign governments. It is not an overstatement to say that the increasing threat of cyber attack puts both our NIT-based economy and our national security at risk.

Today we consider bills to address both those good and bad aspects of our high-tech society's growing reliance on information technology. The first bill, H.R. 756, addresses the growing threat of cyber attack. I want to commend Mr. Lipinski and Mr. McCaul for their longstanding bipartisan leadership on this critical topic of cybersecurity research and development.

The bill they have reintroduced is identical to the legislation we moved through this Committee and passed overwhelmingly on the House Floor last Congress. This bipartisan bill is overall a very good bill that contributes in essential ways to any comprehensive effort to keep our Nation, our businesses and our citizens safe from malicious cyber attacks.

While H.R. 756 is a good bill, I think it is important that we consider the fact that the research accounts of both NSF and NIST would be flat-funded under this proposal and were cut under sequestration. The Federal Government is already suffering from a lack of adequately trained cybersecurity professionals, and the impact of sequestration on these key agencies will further erode the human capital we need to build up our cybersecurity capabilities. It will also slow down much-needed advances in research and development on potentially game-changing technologies.

Next, we will consider H.R. 967, which is another good bipartisan bill. It continues to strengthen and build upon the interagency initiative launched more than 20 years ago with the *High Performance Computing Act of 1991*. H.R. 967 is an updated version of a bipartisan bill that former Chairman Bart Gordon first introduced and the House passed in 2009. The bill was developed by Chairman Gordon to ensure that the Federal Government creates a coherent vision and strategy for federal investments in NIT R&D including all of the applications made possible by NIT. The bill also contains provisions that would help facilitate and strengthen public-private partnerships for the benefit of our economy, national security and overall quality of life.

I am proud to work closely with Chairman Hall—I was proud to work closely with Chairman Hall last year to update that legislation to appropriately reflect changes both to the NITRD program and to the network and information technology landscape since

2009. While it was not possible to get the NITRD legislation enacted into law in the 112th Congress, I want to thank Ms. Lummis for reintroducing our bipartisan bill once again in this new Congress, and I am happy again to be an original cosponsor for this measure.

With that, I will close by saying that I am looking forward to a productive markup today, and I yield back.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Thank you Chairman Smith.

Today, we are marking up two bipartisan pieces of legislation:

- H.R. 756, the Cybersecurity Enhancement Act of 2013, and
- H.R. 967, Advancing America's Networking and Information Technology R&D Act.

Advances in networking and information technology, or NIT, are a key driver of our economy, increasing productivity in existing industries and opening the door for the formation of new ones. Small businesses use NIT to connect to a wider consumer base, allowing them to grow. The military uses NIT to improve intelligence gathering and sharing as well as well as to support many of its worldwide operations. NIT is improving health care by creating better treatment options through electronic health recordkeeping, advanced surgical tools, and the facilitation of medical research.

And of course, internet companies such as Google and Facebook are now worth billions of dollars and show how quickly NIT R&D can translate into real world products. NIT has truly revolutionized our modern way of life.

However, our growing reliance on NIT to fuel our society leaves us vulnerable to cyber attacks. As the stakes have grown higher, individual hackers have given way to organized criminal groups and even foreign governments.

It is not an overstatement to say that the increasing threat of cyber attack puts both our NIT-based economy and our national security at risk.

Today we consider bills to address both the good and bad aspects of our hi-tech society's growing reliance on information technology.

The first bill, H.R. 756, addresses the growing threat of cyber attack. I want to commend Mr. Lipinski and Mr. McCaul for their longstanding, bipartisan leadership on this critical topic of cybersecurity research and development.

The bill they have reintroduced is identical to legislation we moved through this Committee and passed overwhelmingly on the House floor last Congress.

This bipartisan bill is overall a very good bill that contributes in essential ways to any comprehensive effort to keep our nation, our businesses, and our citizens safe from malicious cyber attacks.

While H.R. 756 is a good bill, I think it is important that we consider the fact that the research accounts of both NSF and NIST would be flat-funded under this proposal, and were cut under sequestration. The federal government is already suffering from a lack of adequately trained cybersecurity professionals and the impact of sequestration on these key agencies will further erode the human capital we need to build up our cybersecurity capabilities.It will also slow down much needed advances in research and development on potentially game-changing technologies.

Next we will consider H.R. 967, which is another good bipartisan bill. It continues to strengthen and build upon the interagency initiative launched more than 20 years ago with the High Performance Computing Act of 1991.

H.R. 967 is an updated version of a bipartisan bill that former Chairman Bart Gordon first introduced and the House passed in 2009.

The bill was developed by Chairman Gordon to ensure that the federal government creates a coherent vision and strategy for federal investments in NIT R&D, including all of the applications made possible by NIT. The bill also contained provisions that would help facilitate and strengthen public-private partnerships for the benefit of our economy, national security, and overall quality of life.

I was proud to work closely with Chairman Hall last year to update that legislation to appropriately reflect changes both to the NITR-D program and to the networking and information technology landscape since 2009.

While it was not possible to get the NITR-D legislation enacted into law in the 112th Congress, I want to thank Mrs. Lummis for re-introducing our bipartisan bill once again in the new Congress, and I'm happy to again be an original cosponsor

of this measure. With that, I will close by saying that I'm looking forward to a productive markup today, and I yield back.

Chairman SMITH. Thank you, Ms. Johnson.

If there is no further discussion on the bill, I will recognize myself to offer a Manager's Amendment, and the Clerk will report the amendment.

The CLERK. Amendment number 009, amendment to H.R. 756, offered by Mr. Smith of Texas.

[The amendment of Mr. Smith appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and I will recognize myself and then the Ranking Member.

This Manager's Amendment makes a number of modest changes to the programs authorized in H.R. 756. First, the amendment supports coordination of cybersecurity research and development. It assigns the university-industry task force the responsibility of identifying and prioritizing grand challenges for cybersecurity R&D. This will help the public sector become more aware of long-term industry needs and give more focus to public-private R&D efforts.

The amendment also requires the cybersecurity R&D agencies to track ongoing and completed federal cybersecurity R&D projects and make that information publicly available. For the last several years, the Government Accountability Office has recommended this requirement in order to make federal cyber R&D more transparent and ensure we do not duplicate efforts. The amendment also improves NIST's Cybersecurity Awareness and Education program. It directs NIST to include cybersecurity educational programs and federal workforce professional development in its activities, and I thank Ranking Member Johnson for her ideas that were included in this section.

In addition, the amendment helps graduates with the Scholarship for Service program. It modifies the federal hiring authority available to these graduates to allow for expedited hiring and improved retention of these individuals in the federal workforce.

Finally, the Manager's Amendment updates the authorization levels providing to the National Science Foundation cybersecurity research and education grants. These programs have not been authorized since 2007. Since that time, the NSF has increased its activities to address cybersecurity. The authorizations proposed in this amendment are approximately equal to what NSF currently spends on these activities and sets that level for the next three years. The amendment also clarifies that this funding does not increase the total authorization for NSF research activities. These authorizations demonstrate strong Congressional support for prioritizing cybersecurity R&D activities that are important for America's security and competitiveness. This amendment improves an already strong bill, and I urge my colleagues to support it, and the Ranking Member, Ms. Johnson, is recognized for her comments.

Ms. JOHNSON. Thank you, Mr. Chairman, and thanks to Mr. McCaul for working with me to update and improve Section 204 to better reflect the goals and status of federal cybersecurity education and dissemination activities. The federal science agencies support important education and training efforts such as the Schol-

arship for Service program at NSF that are helping to create a cadre of skilled cybersecurity professionals for both federal workforce needs and critical sectors of our economy including energy and financial systems. The agencies also have a role to play in increasing the public's awareness of risk they may face in their everyday online activities and to help disseminate best practices for managing these risks.

The language in the Manager's Amendment appropriately reflects the full scope of these critical activities, and once again, I thank my colleagues for working with me on this language.

I do want to take a moment to express one concern that I have. Almost everyone in this room supports these programs. For the reasons that I outlined in my opening statement, I strongly support these programs. I think these programs are absolutely vital for our Nation's future prosperity, and I think many, if not most, of my colleagues on both sides of the aisle would agree with that. But I am very concerned that we are moving forward on this bill without recognizing the funding situation facing the agencies we are tasking to address this issue. NSF and NIST and all the agencies tasked with responsibilities in this bill were hit with sequester, and those cuts will affect the ability of these agencies to implement the very responsibilities we are assigning them in this legislation. Cybersecurity is a critical issue, and it becomes more important by the day. Addressing this issue will not be easy and it will not be cheap, but it is absolutely necessary. We need to recognize that and work towards finding resources to fix this problem.

Chairman Smith and Chairman McCaul have both worked with us in an amicable way on this bill, and I will not offer any amendments to address this. But I do think we need to acknowledge that we can't continually tell our agencies to do important work like this on the one hand and deprive them of the resources they need to do the job with the other hand.

I yield back. Thank you very much.

Chairman SMITH. Thank you, Ms. Johnson.

Is there any further discussion on this amendment?

Mr. LIPINSKI. Mr. Chairman.

Chairman SMITH. The gentleman from Illinois, Mr. Lipinski, is recognized.

Mr. LIPINSKI. Thank you, Mr. Chairman. I want to express my appreciation to you and to Mr. McCaul for your willingness to work with me on this legislation. I thank Ranking Member Johnson for working to bring this up. I think this Manager's Amendment incorporates a lot of feedback from both sides of the aisle, and I wholeheartedly support the amendment. I think this is the way that we should be working. I know that the House passed the legislation twice, once in the Democrat majority 111th Congress and once in the Republican majority 112th Congress, both times with broad bipartisan support. When we had a Democratic majority, this was the Lipinski-McCaul bill and it is now the McCaul-Lipinski bill, and I think that is the way this incredibly vital issue of cybersecurity should be handled, and I hope that this continues here today in the markup.

As Mr. McCaul stated, he did a good job of going through what this bill does. I think we should all take note, and it certainly bears

repeating that the Director of National Intelligence this week said the danger of cyber attacks and cyber espionage on crucial infrastructure tops the list of global threats, and I believe that we face the possibility of a cyber Pearl Harbor that could destroy America's military and economic security. I mean, we have already seen the loss of countless jobs in this country through cyber espionage, and we have thankfully so far repelled much worse attacks that are happening every day. So I think it is now more important than ever that we get this legislation across the finish line and on to the President's desk.

I just want to echo one of the points that Ranking Member Johnson mentioned. I would like to see higher authorization levels and recognition of the consequences if we fail in protecting our critical infrastructure. I understand what we have before us now is what we can do today but I think it is important that we make sure we keep our eyes on that and we do have enough support given to what is needed to protect our country.

Of course, cybersecurity research standards and education are only part of the solution. I look forward to working with my colleagues to make sure this bill is included in any comprehensive cybersecurity legislation passed by Congress.

So again, I want to thank Chairman Smith and Chairman McCaul for working with me on this legislation. I urge the adoption of the Manager's Amendment and adoption of the bill.

Chairman SMITH. Thank you, Mr. Lipinski, and appreciate your work on this bill, this being the third Congress you have done so.

Are there any other Members who wish to be recognized? The gentleman from California, Mr. Swalwell—I am sorry. The gentleman from New York, Mr. Maffei, then.

Mr. MAFFEI. Mr. Chairman, shouldn't it be done by seniority? That is the only question. Okay. All right.

Mr. Chairman, I move to strike the last word. I just—I totally agree and want to associate myself with the comments of Mr. Lipinski and the Ranking Member, and I also want to thank the Chairman, the Chairman Emeritus and Mr. McCaul, the Chairman of the Subcommittee.

As a new member of this Committee, this is one of the most important things that we can work on at all, and in both my Committee work here and on the Armed Services Committee, I will be trying to do that. There is broad bipartisan support. In fact, it was in October 2011 that then-presidential candidate Mitt Romney underlined the importance of cybersecurity when he made it one of the top eight actions that he would have dealt with in the first 100 days, and his plan was "a full interagency initiative to form a unified national strategy to deter and defend against the growing threats of these various cyber attacks."

Mr. Lipinski mentioned the testimony of the intelligence—our top intelligence personnel in saying that the cyber attacks pose a greater risk potential to the United States national security than al-Qaeda or other militants that we have focused on since 9/11, and of course, the President made news the other day when he mentioned that we have seen a steady ramping up of cybersecurity threats. Some are state sponsored and some are just sponsored by criminals.

I do also, though, believe that we might be being pennywise but pound foolish not to invest more in our cybersecurity. Normally, I would be the first person to say that this needs to be a very fiscally responsible bill, and of course, I do support it for being fiscally responsible, but there are some areas, and this is one of them, this poses extreme threats to our national security and our economy, and the threat, as Ranking Member Johnson said, to our future prosperity. So we should not be pennywise and pound foolish.

That said, I will not offer an amendment today and will fully support the bill and the Manager's Amendment because the most important thing is that we do move forward, and I am hoping that Mr. Swalwell, myself and the other new Members who certainly support this legislation will work to try to get through the logjams that you faced in the past couple of Congresses, because this is just so vital to everything that we do.

So again, I just want to thank the Chairman and the Ranking Member for working in a bipartisan way on this. This is the way we should be doing all these issues, and I appreciate the time.

Chairman SMITH. Thank you, Mr. Maffei, and thanks for reminding us about the President's and Governor Romney's support for this concept as well.

The gentleman from California, Mr. Rohrabacher, is recognized.

Mr. ROHRABACHER. Mr. Chairman, number one, I want to thank you for your leadership in this issue as well as the leadership that has been provided by several of the former chairmen, Chairman Hall and others in this room that are joining us today.

I have been trying to figure out what is being said here in the opening statements because we all seem to agree that this is vital—this is an issue that is vital to our national security and we all seem to agree on that, but what we don't seem to agree on, it seems this is quite often, is whether we need to—how much money we need to spend or whether we need to spend more money on it, and it sort of dawned on me that what we are really talking about now is whether or not we need to borrow more money from China in order to protect us from China, because every cent more than we spend now in increasing our deficit means we are going to have to borrow it from someone and the people who are out giving us those loans happen to be the Chinese government.

I would suggest that the threat that is posed to us by China will not be enhanced by us becoming even more indebted to China and that we should also, when we are looking at trying to find solutions, we should go beyond trying to give scholarships to our people to defend ourselves against the Chinese students that we are educating in our universities and providing them insights into our most secret information, which then they go back to China and utilize to develop these cyber attack threats. I would think that maybe that plus maybe the fact that we have permitted tech transfer and trade policies and investment policies that have built this enemy. So while I am totally supportive of this bill, I think we should start thinking about the fundamentals of how we get ourselves out of a predicament where we are actually in great debt now to a threat that we have created through our own policies in dealing with the world's worst human rights abuser, and that is the government of China.

Thank you very much, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Rohrabacher.

The gentlewoman from Maryland, Ms. Edwards, is recognized.

Ms. EDWARDS. Thank you, Mr. Chairman, and thank you to my good friends, Mr. McCaul and Mr. Lipinski, for bringing this forward. I do believe that this is one of the single-most important things that we will do during this Congress. Although I support our Ranking Member's concerns about the authorization levels because I do think that the security threat is just that great. But nonetheless, I plan to support the bill but I wanted to take a moment to acknowledge the efforts, Mr. McCaul and Mr. Lipinski, that you are doing to encourage cybersecurity education at all levels. It is vitally important that our universities and community colleges have the resources and expertise, and it is critical that we engage students at an earlier age to create the pipeline that we will need to develop a competent cybersecurity workforce in the decades to come, particularly as Mr. Rohrabacher has just expressed. The National Initiative for Cybersecurity Education plays an instrumental role in this, and I am glad that the Committee will be supporting NIST in its efforts to coordinate this cybersecurity education.

I also want to highlight the Maryland Cybersecurity Center, MC2, for a unique approach to educating the future generation of cybersecurity workforce to serve industry and government needs in Maryland and in the Washington metropolitan area. MC2 offers innovative, hands-on educational programs to pre-college students, undergraduates and graduate students. And I believe that by targeting as early as middle school and high school and not just waiting until the university level, that we can stimulate early interest in the field of cybersecurity and provide students with a knowledge base in preparation to be successful in their future post-secondary studies and eventual career, and I look forward to continuing to work with our Chairman and our Ranking Member on those issues. Thank you.

Chairman SMITH. Thank you, Ms. Edwards.

The gentleman from California, Mr. Swalwell, is recognized.

Mr. SWALWELL. Thank you, Mr. Chairman. I appreciate you holding this markup and I am also pleased that on the agenda of my first markup as a Member of Congress, as a startup Member of Congress, is a bill to address the critical issue of cybersecurity. I am proud and feel fortunate to represent northern Silicon Valley in California, the heart of innovation, technology, computers and the Internet for the Nation and the world.

Needless to say, protecting the integrity of computer systems and securing the information they contain is absolutely critical for our area. If we were to sneeze, the rest of the country could catch a cold. That is why it is so important to protect the infrastructure in Silicon Valley.

An attack against companies in Silicon Valley will ripple across the country and the globe. As we know, this threat is very real. Networks are being attacked constantly by a variety of different actors and for different reasons. For example, there is evidence that Iran has targeted our financial institutions, and China is out to steal one of the best drivers we have of economic growth, our intellectual property, and I would dispute that this is just one country

acting. I believe the evidence is clear, there are a number of countries, there are a number of nation-states and there are a number of individual criminal organizations from all over the globe who are seeking to attack our networks.

Yesterday in the other committee on which I sit, the Committee on Homeland Security, we discussed these and other issues at a hearing with Department of Homeland Security Deputy Secretary Janet Lute and other interested stakeholders. DHS acknowledges the need for federal legislation to enhance cybersecurity capabilities while still protecting privacy, and I am looking forward to passing legislation to do that out of the Homeland Security Committee.

Today, we are considering a piece of the cybersecurity puzzle, H.R. 756, the *Cybersecurity Enhancement Act of 2013*. This bill would help develop our capabilities for cyber defense by among other elements developing security standards and improving the collaboration among federal agencies for relevant research and development. I support this bill, and I encourage my colleagues to do so as well.

I want to make two quick points. First, Section 107 requires a report from the President relating to the needs of our federal cybersecurity workforce. Among other items, the bill requires that the report include an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent including barriers relating to the compensation, hiring process, job classification and hiring flexibilities. I want to be clear that any such discussion should encompass and explain the effects of the ongoing federal pay freeze and the sequester. Federal employee pay has been frozen since 2011, and that freeze is expected to continue this year.

This sequester, as has been alluded to by the Ranking Member and others, threatens to hurt our capabilities in fighting cybersecurity. I believe the problem with the sequester is that when it is so indiscriminate and across the board, you target and cut—you do not target but rather you cut some services that are very critical and in many cases there are services that should be cut more than what we are cutting them, for example, agricultural subsidies. If I had to weigh agricultural subsidies against protecting our cyber networks, I think it is clear based on what the national security threat is where we should be putting our money.

Second, I strongly believe that our best solutions come from collaboration between all interested stakeholders—government, industry, academia and so on. I ran for Congress with a deep desire to encourage public-private partnerships and collaboration, and I hope that we can do that with this bill. Section 103 requires a plan on how the networking and information technology research and development programs should best guide federal cybersecurity research and development. The plan already must include a variety of items like goals for federal research and a description of how the program will establish a research infrastructure. As part of this process, the agencies involved should also be required to consider and include in the report how the program will foster the establishment of public-private partnerships that will result in research, technologies and applications that will help us improve our cybersecurity defense. With such an important issue and in an era of

tight budgets, we need to make the best and most effective use of our taxpayer dollars. This can be accomplished in part by combining the talents of the private sector like the many technology companies in my district and the government.

Mr. Chairman, I hope you and the Ranking Member will consider adding such a provision to the bill when it passes the Committee today. I look forward to working with you both on strengthening this bill before it makes its way to the House Floor, and thank you again for holding this markup.

Chairman SMITH. Thank you, Mr. Swalwell.

Is there any further discussion? The gentleman from Georgia, Mr. Broun, is recognized.

Mr. BROUN. Thank you, Mr. Chairman, and I keep hearing my Democratic colleagues talking about the sequester and how devastating it is going to be, and I had a question for any one of you all, well, actually two questions. Number one is, who gave us the sequester, and number two is why? Can any of my colleagues—I will be glad to yield a moment to answer that question. Ms. Johnson? She is sitting there not paying any attention. You talked about the sequester. Who gave us that sequester? I will be glad to——

Ms. JOHNSON. You were one of them that gave it.

Mr. BROUN. No, ma'am, I did not vote for it. The sequester was given to us by our President, President Obama. He is the one who suggested it. He is the one who promoted it. And I keeping hearing from my Democratic colleagues blame placed on the Republican side, but the long and short of it is that we are spending money that we cannot afford. As Mr. Rohrabacher said, I keep hearing about wanting to plus up spending on many areas, and cybersecurity has been a big concern of mine for a long period of time, both in this Committee as well as in the Homeland Security Committee, where I serve under the able Chairmanship of my good friend, Mr. McCaul from Texas. And we need to be spending money on national defense. I agree with that. But to continue to harp about the sequester that you all's President that gave us the——

Ms. EDWARDS. Will the gentleman yield?

Mr. BROUN. Let me finish my point. To continue to hear my colleagues harp about the sequester when it was proposed by the President, it was promoted by the President. Nobody in the press seems to ask the President why he wanted to give us the sequester, and I think it was all about trying to raise taxes and it wasn't to solve the economic problems that we face. We have got to spend money on what it is important, and that is national security and things that the Constitution gives us authority to spend money on instead of spending money on things that we shouldn't be.

Cybersecurity is certainly something that we should be spending money on just because it is a national defense, national security issue. But I am just getting tired of hearing colleagues on the other side of the aisle continue to squawk about the sequester when it was our President, President Obama, who gave us the sequester and for whatever reason he has promoted that, for whatever reason that he suggested that, but it was his suggestion. Congress voted on approving the sequester. I did not. I voted against it because I thought it was terrible policy, and we have the sequester, so let us

just put our big boy pants on and go forward and do what we can to try to keep this country economically safe as well as militarily safe. Mr. Chairman, I yield back.

Ms. EDWARDS. Would the gentleman yield?

Mr. BROUN. Certainly.

Ms. EDWARDS. Thank you. I just want to just clarify, because in the interest of bipartisanship, and I think that the Chairman has really conducted this Committee and this markup in that way and I know the gentleman from Georgia, and I know that he actually did not mean to refer in that kind of disparaging way to the gentlewoman from Texas, the Ranking Member, and it would be great if you would on the record, you know, just make sure that we continue to express our points but not do it in a way that disparages our Committee leadership, either the Chairman or the Ranking Member, and I would appreciate it if you could just put that on the record.

Mr. BROUN. Well, I was not disparaging Ms. Johnson by any means. I asked her a question and she didn't answer it, and I just was trying to get her to pay attention. I know she was deep in thought, and if I offended her, I apologize, but the point is, continuing to harp about a sequester that is in place, it was given to us by the President, we have got to stop spending money we don't have, we have got to be financially responsible as a Congress, and we are not being, and I just wanted to make my point.

Thank you, Mr. Chairman. I yield back.

Ms. JOHNSON. Could the gentleman yield?

Chairman SMITH. Would the gentleman yield to the Ranking Member?

Mr. BROUN. Certainly. I would be glad to yield.

Ms. JOHNSON. Thank you, Mr. Chairman. I think that due to a personal relationship, I just really didn't pay Mr. Broun much attention. However, regardless of how we got here, we are here and I think we have to keep it before us. At the same time, I think that we should put our Nation's security ahead of that and continue to fund the areas that we need to fund for security and to make sure that the agencies we are giving this responsibility to have some way to carry out the responsibility.

Thank you, and I yield back.

Chairman SMITH. Thank you, Mr. Broun. Thank you, Ms. Johnson.

If there is no further discussion, the vote is on the Manager's Amendment.

All in favor, say aye.

All opposed, no.

The ayes have it and the Manager's Amendment is agreed to.

We will now go to other amendments, and does the gentleman from California, Mr. Bera, seek recognition?

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

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number 003, amendment to H.R. 756, offered by Mr. Bera of California.

[The amendment of Mr. Bera appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman from California is recognized to explain his amendment.

Mr. BERA. My amendment today is simple. It asks that we maximize the talent of our military veterans to continue to serve our country by recruiting and prepping veterans for the cybersecurity workforce.

Our military men and women are heroes at home and abroad, bravely defending our country overseas and in our backyard. We trust our veterans with our lives every day, and I applaud and thank them for their service and duty to America. When they retire or leave the service, some of our best network specialists can help us continue to keep our Nation secure. Who better than these men and women to protect our cyber and networking infrastructure? By finding ways to recruit and prepare veterans for the cybersecurity workforce, we can both protect ourselves and help our returning heroes.

I urge my colleagues to adopt my amendment, which adds preparing veterans for the cybersecurity workforce to the Networking and Information Technology Research and Development program. I yield back my time.

Chairman SMITH. Thank you, Mr. Bera. I will recognize myself in support of the amendment, and thank the gentleman for his addition to the Strategic Plan for the NITRD program. I do support this amendment.

Is there anyone else who wants to be recognized?

If not, all in favor of the amendment, say aye.

Opposed, nay.

The ayes have it and the amendment is agreed to.

Does the gentleman from Florida, Mr. Grayson, seek recognition?

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

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number 057, amendment to H.R. 756, offered by Mr. Grayson of Florida.

[The amendment of Mr. Grayson appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman from Florida, Mr. Grayson, is recognized to explain his amendment.

Mr. GRAYSON. Thank you, Mr. Chairman.

This amendment explicitly adds community colleges to the list of qualified institutions for the cyber scholarship program. There are two other parts of the bill that explicitly mention community colleges as part of academia and institutions of higher education. This is a conforming amendment to make this other section conform. I yield back.

Chairman SMITH. Thank you, Mr. Grayson.

I will recognize myself in support of the amendment, and I do want to thank the gentleman for the inclusion of community colleges in the Scholarship for Service program. As I say, I support the amendment.

Is there anyone else who seeks recognition?

If not, all in favor of the amendment, say aye.

Opposed, nay.

The ayes have it and the amendment is agreed to.

Does the gentleman from Washington, Mr. Kilmer, have an amendment?

Mr. KILMER. Yes. Thank you, Mr. Chairman. I have an amendment at the desk.

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number 002, amendment to H.R. 756, offered by Mr. Kilmer of Washington.

[The amendment of Mr. Kilmer appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman from Washington is recognized to explain his amendment.

Mr. KILMER. Thank you, Mr. Chairman.

To recruit and train the next generation of federal and private sector cybersecurity professionals, we need to leverage capabilities within higher education and create a pipeline that will produce the IT workforce that can help and enhance our Nation's communications and information infrastructure. We need to ensure that the cybersecurity courses and degree programs being developed are effective and that they are producing individuals with the skills necessary for employment as cybersecurity professionals.

To make sure that this is happening, my amendment calls for the NSF to support activities that evaluate the effectiveness of cybersecurity courses and degree programs. Additionally, it calls on NSF to support the establishment of public-private partnerships that will allow students to gain critical research experience on real-world problems as a component of their degree programs. Collaboration between academia, industry and our students will help ensure our future workforce has the qualifications and skills necessary to strengthen America's national security and economic prosperity. I believe this amendment would further encourage students to seek a cybersecurity education and will strengthen the ability of the institutions to produce highly effective cyber professionals to join America's future workforce.

Thank you for consideration of this amendment, and I yield back. Thank you.

Chairman SMITH. Thank you, Mr. Kilmer.

I will recognize myself in support of the amendment, and I thank the gentleman for offering it. It improves the ability of universities to produce cybersecurity professionals so I think it is a good amendment. Are there any others who wish to be recognized?

If not, all in favor of the amendment, say aye.

Opposed, nay.

The ayes have it. The amendment is agreed to.

The gentleman from Florida, Mr. Grayson, is recognized.

Mr. GRAYSON. Thank you, Mr. Chairman. I have an amendment at the desk.

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number——

Chairman SMITH. Is this amendment number 56 or——

Mr. GRAYSON. Yeah.

Chairman SMITH. —54.

The CLERK. It should be 056.

Chairman SMITH. Okay.

The CLERK. Is that correct?

Chairman SMITH. Correct.

Mr. GRAYSON. Yes.

The CLERK. Okay. Amendment 056, amendment to H.R. 756, offered by Mr. Grayson of Florida.

[The amendment of Mr. Grayson appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman is recognized to explain his amendment.

Mr. GRAYSON. Mr. Chairman, this amendment like the earlier amendment is meant to harmonize different sections of the bill. This amendment clarifies language in the bill to ensure that the participation of women is encouraged in the Federal Cyber Scholarship for Service portion of the bill. Women are called out specifically on page 5 of the bill and on page 20 of the bill, but not on page 12 of the bill. This corrects that dilemma. I yield back.

Chairman SMITH. Thank you, Mr. Kilmer—I mean Mr. Grayson. Sorry. I am one behind here.

I recognize myself in support of the amendment. I too would like to see more women pursue cybersecurity degrees so I support the gentleman's amendment.

Are there any other Members who wish to be recognized?

If not, all in favor of the amendment, say aye.

Opposed, nay.

The ayes have it and the amendment is agreed to.

Does the gentleman have another amendment?

Mr. GRAYSON. Yes, Mr. Chairman, I have another amendment at the desk.

Chairman SMITH. The Clerk will report the amendment. And what number is this, Mr. Grayson?

Mr. GRAYSON. I believe this is 58 or 54. There appears to be a discrepancy. On the list of amendments that I see, Mr. Chairman, I see the next one being 058. That is an amendment—well, in any event, not the amendment that you and I discussed but a different one.

Chairman SMITH. Okay. The Clerk will report amendment 54. Is that correct, Mr. Grayson?

Mr. GRAYSON. If we are talking about amendment 54, Mr. Chairman, I am going to withdraw that amendment. No, sorry. It is the other way around. Yes, Mr. Chairman, I have an amendment at the desk.

Chairman SMITH. The Clerk will report the amendment, and it is number 54.

Mr. GRAYSON. Thank you. This amendment adds language to require—sorry.

The CLERK. Amendment number 054, amendment to H.R. 756, offered by Mr. Grayson of Florida.

[The amendment of Mr. Grayson appears in the Appendix]

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman from Florida is recognized to explain the amendment.

Mr. GRAYSON. Thank you very much, Mr. Chairman. Sorry for the confusion on my part.

What this amendment does is to add language to require NIST to carry out research associated with improving the security and integrity of the information technology supply chain as part of its intramural security research program on cybersecurity.

Just by way of background, former U.S. counterterrorism Chief Richard Clark has said that all electronics made in China may have built-in trapdoors allowing Chinese malware to infect American systems on demand. The Fukushima experience has demonstrated to us the fragility of our supply chains, both technological and otherwise. It is an obvious potential target for cyber terrorism. Therefore, I respectfully ask that NIST be engaged in this regard and charged with the responsibility to carry out research to improve the security and integrity of the information technology supply chain. I yield back.

Chairman SMITH. Thank you, Mr. Grayson.

I will recognize myself in support of the amendment, and I appreciate the gentleman's addition of supply chain security and integrity management to NIST research activities.

Is there anyone else who seeks recognition on this amendment?

If not, all in favor, say aye.

Opposed, nay.

In the opinion of the Chair, the ayes have it and the amendment is agreed to.

We will now go to the gentlewoman from Florida, Ms. Wilson, for her amendment.

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

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number 002, amendment to H.R. 756, offered by Ms. Wilson of Florida.

[The amendment of Ms. Wilson appears in the Appendix]

Chairman SMITH. And without objection, the amendment will be considered as read, and the gentlewoman from Florida is recognized to explain her amendment.

Ms. WILSON. Mr. Chairman, this amendment will do exactly what the bipartisan witnesses at our recent cybersecurity hearing argued is necessary for our Nation's cyber defense. It will advance scientific understanding of emerging threats to ensure that American businesses, government agencies and citizens can take action for their own protection.

As Dr. Frederick Chang argued before the Subcommittees on Technology and Research, the discipline of cybersecurity today is too reactive and after the fact. To detect new attacks and vulnerabilities and develop solutions to defend against the identified risk, we need to develop what Dr. Chang and the other esteemed witness, Ms. Terry Benzel, have termed "the science of technology."

The amendment at the desk calls on the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to support research that will lead to the development of a scientific foundation for the field of cybersecurity. This includes research to increase understanding of the underlying principles of securing complex network systems, to enable repeatable experimentation and to create quantifiable security metrics. This research, which will draw on existing programs and activities,

will go a long way toward developing a science of cybersecurity. This in turn will do a great deal to keep our businesses profitable and our citizens safe.

I yield back the balance of my time.

Chairman SMITH. Thank you, Ms. Wilson. I will recognize myself in support of the amendment.

The gentlewoman's amendment supports research at NSF and NIST that establishes a stronger scientific foundation for cybersecurity. A firm science and engineering foundation providing metrics and repeatable testing methods, for example, will improve confidence in cybersecurity technologies and promote innovation. I support the amendment and encourage my colleagues to do the same.

Is there any other member who seeks recognition?

If not, all in favor of the amendment, say aye.

Opposed, nay.

The ayes have it and the amendment is agreed to.

I believe now we will go to our last amendment, and that is being offered by the gentleman from California, Mr. Peters.

Mr. PETERS. Thank you very much, Mr. Chairman. I have an amendment at the desk.

Chairman SMITH. The Clerk will report the amendment.

The CLERK. Amendment number 003, amendment to H.R. 756, offered by Mr. Peters of California.

Chairman SMITH. Without objection, the amendment will be considered as read, and the gentleman from California is recognized to explain his amendment.

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

The economic and national security of the United States depend on the reliable functioning of our critical infrastructure in the face of ever-changing cybersecurity threats. I am offering an amendment today that takes steps to protect this infrastructure by creating a critical infrastructure cybersecurity framework, and I thank the Chairman for bringing this bill and my colleagues from Texas and Illinois for leading this legislation.

It is important that we work to enhance the Nation's cybersecurity and improve our critical infrastructure. If our communications systems or power grid were to be hijacked and controlled by an enemy, it would be debilitating to our national security, our government and the people we serve.

This amendment directs the Director of NIST to collaborate with the private sector to develop a voluntary framework that includes standards, guidelines and best practices for reducing cybersecurity risk to critical infrastructure. The Director would solicit input from not only the private sector but also the federal agencies, state, local and tribal governments and the Director of NIST would publish the framework 18 months after the enactment of the legislation.

I want to emphasize that this framework is non-binding and not prescriptive. In fact, it is an opportunity not only to highlight and learn from the best practices of the private sector but also for government information to augment the ability of private sector to defend its own networks. Cybersecurity and protecting our infrastructure is not a Democratic or Republican issue, it is a national one,

so I am approaching this need for such a framework with viewpoints from both sides of the aisle.

In October 2011, the House Republican Cybersecurity Task Force put forth recommendations, which I have here, one of which was to create this voluntary critical infrastructure cybersecurity network framework led by NIST. The President's recent Executive Order on Cybersecurity also directs the development of a cybersecurity framework. The framework is something therefore that both sides agree on and both sides agree needs to be done, and I want to emphasize that it needs to be done here in Congress too so that we have oversight through this committee, particularly through the Oversight Committee chaired by Mr. Broun from Georgia.

There is an urgency to seek such a framework, to see such a framework is accomplished, and I agree with the majority task force that NIST is the ideal federal agency to carry out such an important task. It is a non-regulatory agency and it is well respected in the private sector. We can't make progress on cybersecurity without the vital input of the private sector, which is integral to our critical infrastructure.

Mr. Chairman, I urge my colleagues to adopt this amendment to improve our cybersecurity and protect our assets, and I yield back my remaining time.

Chairman SMITH. Thank you, Mr. Peters.

The gentleman from Texas, Mr. McCaul, is recognized in opposition to the amendment.

Mr. MCCAUL. Thank you, Mr. Chairman.

While I am sure Mr. Peters' intentions are good, this amendment directs NIST to seek input from the private sector when developing the critical infrastructure framework without ensuring that the director will use this input wisely. This has been a bipartisan process over the last several Congresses, but I am concerned this amendment lacks specificity, which is why the U.S. Chamber of Commerce opposes this amendment, and they represent the private sector. Inclusion of this amendment would hurt the progress that has already been made and reduce the likelihood of finally getting this bill through the Senate and signed into law by the President. I think the private sector is dealing with this issue every day and has a great stake in the development of any guidelines or framework. Its role must be clearly defined so we do not risk losing the knowledge that these experts would bring to the table. We are currently exploring this also in the Homeland Security Committee in terms of voluntary standards being produced by the private sector with respect to critical infrastructures, and with that, Mr. Chairman, I stand in opposition and I yield back.

Chairman SMITH. Okay. Thank you, Mr. McCaul.

Are there any other Members who wish to be heard on this amendment? The gentlewoman from Maryland, Ms. Edwards, is recognized.

Ms. EDWARDS. Thank you, Mr. Chairman.

I just want to express my support for the amendment. It requires NIST to develop, in collaboration with the private sector, including the owners and operators of our critical infrastructure, a framework that will promote the adoption of voluntary standards and best practices to lower cybersecurity risks across all sectors and in-

dustries. The amendment implements Section 7 of the President's Executive Order on Cybersecurity. I know there are concerns that have been expressed that the framework will open the door for regulatory action by sector-specific agencies but I want to reiterate that NIST does not intend to do so. Rather, this amendment would allow NIST to continue promoting the wide adoption of practices to increase cybersecurity across all sectors and industry types. The framework will seek to provide owners and operators a flexible, repeatable and cost-effective risk-based approach to implementing security practices while allowing organizations to express requirements to multiple authorities and regulators.

And with that, I yield and express support for the amendment.

Chairman SMITH. Thank you, Ms. Edwards.

Does anyone else seek recognition? The Ranking Member, the gentlewoman from Texas, Ms. Johnson, is recognized.

Ms. JOHNSON. Thank you very much, Mr. Chairman, and I want to thank the gentleman from California for this amendment.

The national and economic security of the United States depends on a reliably functioning critical infrastructure. Tasking NIST with accelerating development of voluntary consensus-based standards through a public-private partnership is a common sense approach to increasing the security and reliability of our critical infrastructure. In fact, the Republican Cybersecurity Task Force Report stated that Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies such as the National Institute of Standards and Technology to help the private sector improve security.

The common sense amendment implements the task force recommendation by requiring NIST to establish a public-private partnership that will bring all of the stakeholders together in the development of best practices and standards. This amendment will accelerate the adoption of voluntary cybersecurity practices, and I urge its adoption.

Chairman SMITH. Thank you, Ms. Johnson.

The question is on the Peters—the gentleman from Florida, Mr. Grayson, is recognized.

Mr. GRAYSON. Thank you, Mr. Chairman.

I am reading the amendment, and I heard what the gentleman from Texas said, and I just don't see anything in this amendment that seems to require anybody to do anything or to impose any burden on the private sector. I don't mean to impose on the gentleman from Texas, but if the gentleman would be so kind, I will yield the time to you. Can you point to anything in the amendment that actually does what was described?

Mr. MCCAUL. I believe that—I would be happy to take that. I believe that it lacks specificity in terms of what collaboration is supposed to take place, how the Director is to use this input, and again, I think this poses a problem for the private sector. They do view this as a slope down the road to regulatory standards, which is why the U.S. Chamber of Commerce opposes this amendment.

Having said that, I would be happy to work with the gentleman, Mr. Peters, on language if he would be willing to withdraw the amendment.

Mr. GRAYSON. I yield to Mr. Peters.

Mr. PETERS. You know, I had not intended to do that, but I am going to accept the gentleman's offer in the interest of bipartisanship. Mr. Chairman, if I might just add——

Chairman SMITH. Without objection, the amendment will be withdrawn. Thank you, Mr. Peters, and I know you and Mr. McCaul will be able to try to work something out in that regard.

Mr. GRAYSON. Mr. Chairman, I am so happy that I could bring the two parties together. It is something I am famous for.

Chairman SMITH. Thank you, Mr. Grayson.

Mr. MCCAUL. That could be a first.

Chairman SMITH. But we hope not the last, Mr. Grayson. Thank you.

Let us see. Are there any other amendments? The gentleman from California, Mr. Rohrabacher.

Mr. ROHRABACHER. I just would like to announce that I will be offering the following amendment to the Rules Committee to see if we can offer this on the Floor, mainly because I did not offer this amendment 24 hours in advance of this hearing, which I think is par for the course and I would need unanimous consent, and I doubt if I would get unanimous consent, so I will be offering this at the Rules Committee, the following amendment: No money provided by this legislation shall be used to finance scholarships to be used in education programs that are open to foreign students who are citizens of a country that is recognized as a base of cyber attacks on targets within the United States. That will be an amendment that I will offer to the Rules Committee for their consideration, and I thank you very much for allowing me to suggest that today.

Chairman SMITH. Thank you, Mr. Rohrabacher.

If there are no further amendments, a reporting quorum being present, the question is on reporting the bill as amended favorably to the House.

Those in favor, say aye.

Opposed, no.

The ayes have it, and the bill is amended is ordered reported favorably.

Without objection, the motion to reconsider is laid on the table, and we will now go to our second bill of the day—H.R. 967

Chairman SMITH. Pursuant to notice, I now call up H.R. 756—I am sorry—967, the *Advancing America's Networking and Information Technology Research and Development Act of 2013*, and the Clerk will report the bill.

The CLERK. H.R. 967, a bill to amend the *High Performance Computing Act of 1991* to authorize activities for support of networking and information technology research, and for other purposes.

Chairman SMITH. Without objection, the bill is considered as read.

Appendix:

H.R. 756, CYBERSECURITY ENHANCEMENT ACT OF 2013,

SECTION–BY–SECTION ANALYSIS, AMENDMENTS,

AMENDMENT ROSTER

U.S. GOVERNMENT INFORMATION GPO

I

113TH CONGRESS
1ST SESSION

H. R. 756

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

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 15, 2013

Mr. MCCAUL (for himself, Mr. LIPINSKI, Mr. SMITH of Texas, Mr. LANGEVIN, Mr. MEEHAN, Ms. MATSUI, Mr. HALL, and Mr. BEN RAY LUJÁN of New Mexico) introduced the following bill; which was referred to the Committee on Science, Space, 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 2013".

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'."; and

(4) by amending paragraph (6) to read as follows:

"(6) 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, and to protect consumer privacy;

(3) describe how the Program will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely 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 community colleges, National Laboratories, 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, and user motivations.".

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—

(1) in subparagraph (A) by inserting "identity management," after "cryptography,"; and

(2) in subparagraph (I), by inserting ", crimes against children, and organized crime" after "intellectual property".

(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) $90,000,000 for fiscal year 2014;

"(B) $90,000,000 for fiscal year 2015; and

"(C) $90,000,000 for fiscal year 2016.".

(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) in paragraph (7) by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $4,500,000 for fiscal year 2014;

"(B) $4,500,000 for fiscal year 2015; and

"(C) $4,500,000 for fiscal year 2016.".

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $19,000,000 for fiscal year 2014;

"(B) $19,000,000 for fiscal year 2015; and

"(C) $19,000,000 for fiscal year 2016.".

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended by striking subparagraphs (A)

through (E) and inserting the following new subparagraphs:

"(A) $2,500,000 for fiscal year 2014;

"(B) $2,500,000 for fiscal year 2015; and

"(C) $2,500,000 for fiscal year 2016.".

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $24,000,000 for fiscal year 2014;

"(B) $24,000,000 for fiscal year 2015; and

"(C) $24,000,000 for fiscal year 2016.".

(g) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is repealed.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Scholarship for Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) 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 devel-

opment opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions and community colleges; 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, 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), and to veterans. For purposes of this paragraph, the term "veteran" means a person who—

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

(B) served on active duty (other than active duty for training) in the Armed Forces of the United States and was discharged or released from such service for a service-connected disability before serving 180 consecutive days.

For purposes of subparagraph (B), the term "service-connected" has the meaning given such term under section 101 of title 38, United States Code.

(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 as provided in paragraph (5). 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.

(5) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this subsection shall be 1 year more than the number of years for which the scholarship was received.

(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 (e)(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 Edu-

cation 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 para-

graph, 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 con-

verted to a competitive service position without competition if the individual meets the requirements for that position.

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, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector, and a description of how successful programs are engaging the

talents of females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b);

(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, including individuals from States or regions in which the unemployment rate exceeds the national average;

(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, development, education, and training 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, including minority-serving institutions and community colleges, 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.

(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.

SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.

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

"(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

"(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the develop-

ment of standards, reference materials, and checklists under this subsection on the basis of—

"(A) the security risks associated with the use of the system;

"(B) the number of agencies that use a particular system or security tool;

"(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

"(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

"(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsoles-

cence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

"(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

"(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

"(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or 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 information technology hardware or software systems for which no such standard, reference material, or 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.

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

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of inter-

national technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a plan for ensuring such Federal agency coordination.

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

SEC. 203. CLOUD COMPUTING STRATEGY.

(a) IN GENERAL.—The Director, in collaboration with the Federal CIO Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(b) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(3) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(A) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(B) to ensure secure access to the data stored in cloud computing data centers;

(C) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3); and

(D) to support the development of the automation of continuous monitoring systems.

SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institu-

tions, National Laboratories, the National Coordination Office of the Networking and Information Technology Research and Development program, and other organizations, shall continue to coordinate a cybersecurity awareness and education program to increase knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through—

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

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

(3) efforts to attract, recruit, and retain qualified professionals to the Federal cybersecurity workforce.

(b) STRATEGIC PLAN.—The Director shall, in cooperation with relevant Federal agencies and other stakeholders, develop and implement a strategic plan to guide Federal programs and activities in support of a comprehensive cybersecurity awareness and education program as described under subsection (a).

(c) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act and every 5 years

thereafter, the Director shall transmit the strategic plan required under subsection (b) to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall continue 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.

SEC. 206. AUTHORIZATIONS.

No additional funds are authorized to carry out this title and the amendments made by this title or to carry out the amendments made by sections 109 and 110 of this

Act. This title and the amendments made by this title and the amendments made by sections 109 and 110 of this Act shall be carried out using amounts otherwise authorized or appropriated.

○

SECTION–BY–SECTION ANALYSIS OF

H.R. 756, CYBERSECURITY ENHANCEMENT ACT OF 2013

TITLE I – RESEARCH AND DEVELOPMENT

SECTION101. DEFINITIONS

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

SECTION102. FINDINGS

Describes the findings of this title.

SECTION 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.

SECTION 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY

Adds research on the social and behavioral aspects of cybersecurity to the list of cybersecurity research areas that the National Science Foundation may support as part of its total cybersecurity research portfolio.

SECTION 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.

Repeals NSF cybersecurity faculty development traineeship program.

SECTION 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 additional year of service over the number of years for which the scholarship was received.

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 107. CYBERSCURITY 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 cybersecruity professionals; and the identification of any barriers to the recruitment and hiring of cybersecurity professionals.

SECTION 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.

SECTION 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 for the federal government, and requires NIST to develop automated security specifications with respect to checklist content.

SECTION 110. NIST CYBERSECURITY R&D

Amends the National Institute of Standards and Technology Act to codify NIST cybersecurity research and development activities; NIST is authorized to conduct research on the development of a unifying and standardized identity, privilege, and access control management framework and 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

SECTION 201. DEFINITIONS

Defines the terms Director and Institute in the title.

SECTION 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS

Requires NIST to consult with the private sector and others 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.

SECTION 203. CLOUD COMPUTING STRATEGY

Directs NIST, in collaboration with Federal agencies and other stakeholders, to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government. The strategy should consider activities that accelerate standards development, the development of processes to test standards conformance, and the security of data stored in the cloud.

SECTION 204. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION

Requires NIST to maintain a cybersecurity awareness and education program and to deliver a strategic plan to Congress within 1 year describing the implementation of this program. Requires the program to be aimed at disseminating cybersecurity best practices and standards and include how NIST will make these usable by individuals, small business, state and local governments, and educational institutions.

SECTION 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT

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

SECTION 206.

States that no additional funds are authorized for the NIST activities in the bill.

AMENDMENT TO H.R. 756

OFFERED BY MR. SMITH OF TEXAS

Page 7, after line 10, insert the following new subsection:

(f) CYBERSECURITY RESEARCH DATABASE.—The agencies involved in developing and updating the strategic plan under subsection (a) shall establish, in coordination with the Office of Management and Budget, a mechanism to track ongoing and completed Federal cybersecurity research and development projects and associated funding, and shall make such information publically available.

Page 8, lines 18 through 20, strike "$90,000,000" each place it appears and insert "$119,000,000".

Page 9, lines 12 through 14, strike "$4,500,000" each place it appears and insert "$5,000,000".

Page 9, lines 20 through 22, strike "$19,000,000" each place it appears and insert "$25,000,000".

Page 10, lines 3 through 5, strike "$2,500,000" each place it appears and insert "$4,000,000".

Page 10, lines 11 through 13, strike "$24,000,000" each place it appears and insert "$32,000,000".

Page 18, line 18, through page 19, line 3, amend subsection (e) to read as follows:

(e) HIRING AUTHORITY.—

(1) APPOINTMENT IN EXCEPTED SERVICE.—Notwithstanding any provision of chapter 33 of title 5, United States Code, governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the academic program for which a scholarship was awarded.

(2) NONCOMPETITIVE CONVERSION.—Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) TIMING OF CONVERSION.—An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) AUTHORITY TO DECLINE CONVERSION.—An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

Page 21, line 20, and page 22, lines 1, 4, and 7, redesignate paragraphs (2) through (5) as paragraphs (3) through (6), respectively.

Page 21, after line 19, insert the following new paragraph:

(2) identify and prioritize at least three cybersecurity grand challenges, focused on nationally significant problems requiring collaborative and interdisciplinary solutions;

Page 21, lines 21 through 24, strike ", including" and all that follows through "collaboration" and insert "to address the grand challenges identified under paragraph (2)".

Page 30, line 14, strike "and".

Page 30, after line 14, insert the following new paragraph:

(3) improving the state of cybersecurity education at all educational levels;

Page 30, line 15, redesignate paragraph (3) as paragraph (4).

Page 30, line 17, strike the period and insert "; and".

Page 30, after line 17, insert the following new paragraph:

(5) improving the skills, training, and professional development of the Federal cybersecurity workforce.

Page 31, line 22, through page 32, line 4, amend section 206 to read as follows:

SEC. 206. AUTHORIZATIONS.

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

☒

AMENDMENT TO H.R. 756

OFFERED BY MR. BERA OF CALIFORNIA

Page 5, line 22, strike "and".

Page 6, line 2, strike the period and insert "; and".

Page 6, after line 2, insert the following new paragraph:

(7) describe how the Program will help to recruit and prepare veterans for the Federal cybersecurity workforce.

☒

AMENDMENT TO H.R. 756

OFFERED BY MR. GRAYSON OF FLORIDA

Page 11, line 7, insert ", including community colleges" after "higher education".

☒

AMENDMENT TO H.R. 756

OFFERED BY MR. KILMER OF WASHINGTON

Page 12, line 5, strike "and".

Page 12, line 6, insert "and evaluation" after "development".

Page 12, line 7, strike the period and insert "; and".

Page 12, after line 7, insert the following new subparagraph:

(D) public-private partnerships that will integrate research experiences and hands-on learning into cybersecurity degree programs.

☒

AMENDMENT TO H.R. 756

OFFERED BY MR. GRAYSON OF FLORIDA

Page 12, line 23, insert "females and" after "participation of".

☒

AMENDMENT TO H.R. 756

OFFERED BY MR. GRAYSON OF FLORIDA

Page 27, line 6, strike "; and" and insert a semicolon.

Page 27, line 8, strike "systems." and insert "systems; and".

Page 27, line 8, after paragraph (4) insert the following new paragraph:

"(5) carry out research associated with improving the security and integrity of the information technology supply chain.".

☒

AMENDMENT TO H.R. 756

OFFERED BY Congresswoman Frederica S. Wilson

Page 27, after line 8, insert the following new section:

SEC. 111. RESEARCH ON THE SCIENCE OF CYBERSECURITY.

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall, through existing programs and activities, support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

☒

AMENDMENT ROSTER

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
Full Committee Markup
March 14, 2013

AMENDMENT ROSTER

H.R. 756, "Cybersecurity Enhancement Act of 2013"

No.	Amendment	Summary	
1	Amendment offered by Mr. Smith (TX) (009)	Reauthorizes NSF research grants for three years to match current spending levels; Requires the university-industry task force to identify and prioritize grand challenges for cybersecurity R&D; Requires agencies to track R&D projects; Adds education programs and cybersecurity workforce development to NIST awareness and education program; Amends federal hiring authority for Scholarship for Service Program graduates	Agreed to by Voice Vote
2	Amendment offered by Mr. Bera (CA) (003)	Amends the Cybersecurity Strategic Research and Development Plan to add into the contents of the plan a description of how the Networking and Information Technology Research and Development Program prepares veterans for the Federal cybersecurity workforce.	Agreed to by Voice Vote
3	Amendment offered by Mr. Grayson (FL) (057)	Amends the Federal Cyber Scholarship for Service Program to include community colleges as eligible for Scholarship for Service grants.	Agreed to by Voice Vote
4	Amendment offered by Mr. Kilmer (WA) (002)	Amends the Federal Cyber Scholarship for Service Program, to allow support for course evaluation and public-private partnership activities conducted at institution of higher education.	Agreed to by Voice Vote
5	Amendment offered by Mr. Grayson (FL) (056)	Amends the Federal Cyber Scholarship for Service Program to add females to the individuals to be considered for the Scholarship for Service Program.	Agreed to by Voice Vote
6	Amendment offered by Mr. Grayson (FL) (054)	Directs NIST to conduct research into improving the security and integrity of the information technology supply chain.	Agreed to by Voice Vote
7	Amendment offered by Ms. Wilson (FL) (002)	Creates a new section which directs NSF and NIST to conduct research on the development of the scientific framework underlying cybersecurity.	Agreed to by Voice Vote