112TH CONGRESS
1ST SESSION

S. 1152

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

IN THE SENATE OF THE UNITED STATES

JUNE 7, 2011

Mr. MENENDEZ introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

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 2011''.

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;

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

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;

(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities

Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

(c) DEVELOPMENT OF ROADMAP.—The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan required in this section. Such roadmap shall—

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

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

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

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

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

(2) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, and other relevant organizations and institutions.

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

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

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

(1) by inserting ''and usability'' after ''to the structure'';

(2) in subparagraph (H), by striking ''and'' after the semicolon;

(3) in subparagraph (I), by striking the period at the end and inserting ''; and''; and

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

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

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

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(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 2012;

''(B) $90,000,000 for fiscal year 2013; and

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

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

(1) in paragraph (4)—

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

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

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

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

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

''(A) $4,500,000 for fiscal year 2012;

''(B) $4,500,000 for fiscal year 2013; and

''(C) $4,500,000 for fiscal year 2014.''.

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

''(A) $19,000,000 for fiscal year 2012;

''(B) $19,000,000 for fiscal year 2013; and

''(C) $19,000,000 for fiscal year 2014.''.

(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 2012;

"(B) $2,500,000 for fiscal year 2013; and

"(C) $2,500,000 for fiscal year 2014.".

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

"(A) $24,000,000 for fiscal year 2012;

"(B) $24,000,000 for fiscal year 2013; and

"(C) $24,000,000 for fiscal year 2014.".

(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 (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 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 cybersecurity professionals with those skills sought by the Federal Government 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 Engineer-

ing 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;

(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 ex-

plore mechanisms for carrying out collaborative research and development activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force shall—

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

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;

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

(4) propose guidelines for assigning intellectual property rights, 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.

SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

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

''(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment

recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

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

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

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

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

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

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

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

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

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

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

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

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

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

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

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

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

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

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

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

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

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

(1) ensure coordination of United States Government representation in the international develop-

ment of technical standards related to cybersecurity; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a proactive plan to engage international standards bodies with respect to the development of technical standards related to cybersecurity.

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

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

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

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

(b) MANUFACTURING EXTENSION PARTNERSHIP.—The Director shall, to the extent appropriate, implement subsection (a) through the Manufacturing Extension Part-

nership program under section 25 of the National Institute of Standards and Technology Act (15 U.S.C. 278k).

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

SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall 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.

○