AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

111TH CONGRESS
1ST SESSION

H. R. 4061

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

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 7, 2009

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

---

A BILL

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

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

SECTION 1. SHORT TITLE.

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

TITLE I—RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

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

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

SEC. 102. FINDINGS.

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

(1) by amending paragraph (1) to read as follows:

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

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

(3) by amending paragraph (3) to read as follows:

''(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has 'suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information'.'';

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

(5) by inserting after paragraph (3) the following new paragraph:

''(4) In a series of hearings held before Congress in 2009, experts testified that the Federal cybersecurity research and development portfolio was too focused on short-term, incremental research and that it lacked the prioritization and coordination

necessary to address the long-term challenge of ensuring a secure and reliable information technology and communications infrastructure.''; and

(6) by amending paragraph (7), as so redesignated by paragraph (4) of this section, to read as follows:

''(7) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.''.

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of this Act, the agencies identified in subsection 101(a)(3)(B) (i) through (x) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B) (i) through (x)) or designated under section 101(a)(3)(B)(xi) of such Act, working through the National Science and Technology Council and with the assistance of the National Coordination Office, shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking sys-

tems. 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 event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

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

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

(2) specify the funding allocated to each major research objective of the strategic plan and the

source of funding by agency for the current fiscal year; and

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

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

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

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

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

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

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

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

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

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

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

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

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

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended in subparagraph (A) by inserting ''identity management,'' after ''cryptography,''.

(b) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—Section 4(a)(3) of such Act (15 U.S.C. 7403(a)(3)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

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

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

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

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

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

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

(1) in paragraph (4)—

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

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

(C) by striking subparagraph (D);

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

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

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

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are nec-

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

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended to read as follows:

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

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

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

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended to read as follows:

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are nec-

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

(g) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CYBERSECURITY.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is amended to read as follows:

''(e) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CYBERSECURITY.—

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

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

SEC. 106. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to ex-

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 and for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources.

(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force.

SEC. 107. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

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

''(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each

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 speci-

fications (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 any product developed under the National Checklist Program for any information system, including the Security Content Automation Protocol and other automated security specifications, is made available to Federal agencies.

''(6) AGENCY USE REQUIREMENTS.—Federal agencies shall use checklists developed or identified under paragraph (1) to secure computer hardware and software systems. This paragraph 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 hard-

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

SEC. 108. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

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

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

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

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

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

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

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

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

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

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

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

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

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the

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

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

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

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

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

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

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

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

SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

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

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems; and

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

○