[DISCUSSION DRAFT]

SEPTEMBER 18, 2009

111TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

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

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

SECTION 1. SHORT TITLE.

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

SEC. 2. DEFINITIONS.

In this Act:

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

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

SEC. 3. FINDINGS.

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

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

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

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

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

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

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

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

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

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. 4. 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; and

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

(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, and other relevant organizations and institutions.

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

SEC. 5. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

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

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

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

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

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

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

SEC. 6. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

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

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

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

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

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

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

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

(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); and

(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.''.

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

(d) 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.—The 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) 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.—The 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) 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, includ-

ing the research areas described in section 4(a)(1), through the award of competitive, merit-reviewed fellowships.

''(2) AUTHORIZATION OF APPROPRIATIONS.—The 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. 7. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall carry out a Scholarship for Service program to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce a 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 3 years to students pursuing undergraduate and graduate degrees in cybersecurity fields;

(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 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; 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; and

(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.

(2) SELECTION.—Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need.

(3) SERVICE OBLIGATION.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time equal to the length of the scholarship. If a scholarship recipient is not offered employment by a Federal agency, the service requirement can be satisfied by —

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

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

(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.—A qualified institution of higher education receiving a grant under this section shall, as a condition of participating in the program, enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their respective service requirements.

(3) AMOUNT OF REPAYMENT.—

(A) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in paragraph (1) occurs before the completion of 1 year of a

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

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

(C) REPAYMENTS.—A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a and following), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance

with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT.—

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

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

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

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

(C) RETAIN PERCENTAGE.—An institution of higher education may retain a percentage of

any repayment the institution collects under this paragraph to defray administrative costs associated with the collection. The Director shall establish a single, fixed percentage that will apply to all eligible entities.

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

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

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to appropriated to the National Science Foundation to carry out this section—

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

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

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

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

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

SEC. 8. 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, including a comparison of the Federal Government's needs with the cybersecurity skills and expertise sought by the private sector; and

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity tal-

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

SEC. 9. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force shall—

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

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work fo-

cused 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.