with me on modifying the report that accompanies H.R. 1163 to ensure the operational role the Department of Homeland Security plays in the protection of the Nation's Federal information systems is in no way diminished. I request that you urge the Speaker to appoint Members of this Committee to any conference committee for consideration of any provisions that fall within the jurisdiction of the Committee on Homeland Security in the House-Senate conference on this or similar legislation.

I also request that this letter and your response be included in the committee report on H.R. 1163 and into the Congressional Record during consideration of this measure on the House floor. Thank you for your consideration of this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, HOUSE OF REPRESENTATIVES,
Washington, DC, April 12, 2013.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for your letter regarding the Committee on Homeland Security's jurisdictional interest in H.R. 1163, the ''Federal Information Security Amendments.''

I agree that the Committee on Homeland Security has a valid jurisdictional interest in federal cybersecurity, and that the Committee's jurisdiction will not be adversely affected by your decision to forego consideration of H.R. 1163. As you have requested, I will support your request for an appropriate appointment of outside conferees from your Committee in the event of a House-Senate conference on this or similar legislation, should such a conference be convened.

Finally, I will include a copy of your letter and this response in the Committee Report and in the Congressional Record during the floor consideration of this bill. Thank you again for your cooperation.

Sincerely,

DARRELL ISSA,
Chairman.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY, HOUSE OF REPRESENTATIVES,
Washington, DC, April 12, 2013.

Hon. DARRELL ISSA,
Chairman, Committee on Oversight and Government Reform, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN ISSA: I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 1163. the Federal Information Security Amendments Act of 2013.

I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology. This waiver, of course, is conditional on our mutual understanding that agreeing to waive consideration of this bill should not be construed as waiving, reducing, or affecting the jurisdiction of the Committee on Science, Space, and Technology.

Additionally, the Committee on Science, Space, and Technology expressly reserves its authority to seek conferees on any provision within its jurisdiction during any House-Senate conference that may be convened on this, or any similar legislation. I ask for your commitment to support any request by the Committee for conferees on H.R. 1163, as well as any similar or related legislation.

I ask that a copy of this letter be placed in the Committee Report on H.R. 1163 and in the Congressional Record during consideration of this bill on the House floor.

I look forward to continuing to work with you on the legislation as you work towards enactment of H.R. 1163.

Sincerely,

LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology.

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, HOUSE OF REPRESENTATIVES,
Washington, DC, April 16, 2013.

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

DEAR MR. CHAIRMAN: Thank you for your letter regarding the Committee on Science, Space, and Technology's jurisdictional interest in H.R. 1163, the ''Federal Information Security Amendments Act of 2013,'' and your willingness to forego consideration of H.R. 1163 by your committee.

I agree that the Committee on Science, Space, and Technology has a valid jurisdictional interest in certain provisions of H.R. 1163 and that the Committee's jurisdiction will not be adversely affected by your decision to forego consideration of H.R. 1163. As you have requested, I will support your request for an appropriate appointment of outside conferees from your Committee in the event of a House-Senate conference on this or similar legislation should such a conference be convened.

Finally, I will include a copy of your letter and this response in the Committee Report and in the Congressional Record during the floor consideration of this bill. Thank you again for your cooperation.

Sincerely,

DARRELL ISSA,
Chairman.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. ISSA) that the House suspend the rules and pass the bill, H.R. 1163.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ISSA. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

CYBERSECURITY ENHANCEMENT ACT OF 2013

Mr. SMITH of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 756) to advance cybersecurity research, development, and technical standards, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 756

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;

(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 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) 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.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. SMITH) and the gentlewoman from Texas (Ms. EDDIE BERNICE JOHNSON) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. SMITH of Texas. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on H.R. 756, the bill now under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. SMITH of Texas. Mr. Speaker, I yield myself such time as I may consume.

I thank Representative MCCAUL and Representative LIPINSKI for introducing this commonsense, bipartisan legislation. I am pleased to be an original cosponsor of H.R. 756, the Cybersecurity Enhancement Act of 2013.

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 the National Science Foundation, which we know is important to increasing security over the long term;

Three, National Science Foundation scholarships to improve the quality of the cybersecurity workforce;

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. We must develop a rigorous scientific foundation for cybersecurity. This legislation helps foster such an effort, which will make our computer systems more secure.

The bill was recently approved by the Science, Space, and Technology Committee with strong bipartisan support. I again thank my Science Committee colleagues, Representatives MCCAUL and LIPINSKI, for their initiative on this issue, and look forward to this bill becoming law.

Mr. Speaker, the following groups have written letters of support for H.R. 756, the Cybersecurity Enhancement Act: TechAmerica, the U.S. Chamber of Commerce, USTelecom, the Information Technology Industry Council, the National Association of Manufacturers, the Financial Services Roundtable, the Computing Research Association, the Institute of Electrical and Electronics Engineers, the Society for Industrial and Applied Mathematics, and the U.S. Public Policy Council of the Association for Computing Machinery.

Mr. Speaker, I reserve the balance of my time.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 756, the Cybersecurity Enhancement Act of 2013.

This is a good, bipartisan bill, and it is nearly identical to the legislation that passed the House by an overwhelming majority last Congress. I would like to thank my colleagues, Mr. LIPINSKI and Mr. MCCAUL, for their leadership and dedication to improving our Nation's cybersecurity.

Almost every one of us uses a computer, a cell phone, and the Internet every single day. These technologies have greatly increased our productivity and connectivity, and they have become a key component of our economy. Unfortunately, if you pick up the newspaper, you're likely to see another story about a hacker bringing down a Web site, stealing credit card numbers, or gaining access to a company's intellectual property. We need to do what we can to help ensure that these sorts of cyber intrusions are minimized, and I am pleased that H.R. 756 addresses a number of critical issues:

It strengthens public-private partnerships, guarantees a proactive and comprehensive research and development portfolio, ensures the development of robust cybersecurity standards, and trains the next generation of cybersecurity professionals.

Both of the agencies covered in H.R. 756, the National Science Foundation and the National Institute of Standards and Technology, play important and unique roles in the Federal Government's effort to secure cyberspace. I strongly believe that these agencies and the activities they support are vital to our Nation's future prosperity. We not only need to protect the security of our current information systems, but we need to build the next generation of systems—systems that are more secure from the first time they're turned on.

President Obama previously stated that cyber threats are ''one of the most serious economic and national security challenges we face as a Nation'' and that cutting-edge research and development and a commitment to science and math education are central to securing America's information and communication networks. I couldn't agree more.

Cybersecurity is a critical issue, and it becomes more important day by day. Addressing this issue will not be easy, but it is absolutely necessary. H.R. 756 will help build up our cybersecurity capabilities through research and education. This is a good, bipartisan bill that should be included in any comprehensive effort to keep our Nation, our businesses, and our citizens safe from malicious cybersecurity attacks.

Before I conclude, I would like to thank my staff and the majority's staff for their hard work on this bill. In particular, I would like to thank Marcy Gallo for her efforts on this bill in this Congress and in past Congresses as well. I look forward to working with my colleagues to make sure this bill makes it to the President's desk.

I urge my colleagues to support H.R. 756, and I reserve the balance of my time.

□ 1300

Mr. SMITH of Texas. Mr. Speaker, I yield 5 minutes to the gentleman from Texas (Mr. MCCAUL), a member of the Science, Space, and Technology Committee, the chairman of the Homeland Security Committee, and the sponsor of this legislation.

Mr. MCCAUL. Mr. Speaker, I'd like to thank my fellow Texan and friend, Chairman SMITH, for his support, Ranking Member JOHNSON, and DAN LIPINSKI, my cohort on this bill. We passed this in two prior Congresses, and this is our third attempt. Let's hope the third time will be a charm.

For most of us around the country, it is hard to think of anything else other than the terrorist attack in Boston yesterday. It is a solemn reminder of the threats that we face. While the attention of the American people is focused on the physical attack that occurred during the Boston Marathon, I think it is important that we as leader in this Chamber be frank with the American people about the virtual threat of a cyber attack against our national and economic security interests. We must be vigilant against both.

The United States faces several daunting challenges at this moment in history, including emerging threats that we must as a Nation be prepared to face head on. Congress is often blamed for not rising to the occasion by being too reactive to events or failing to act at all. I'm determined, as my colleagues are, that this Congress tackle head on the problem of our vulnerable cyber defenses and bolster our security in cyberspace.

Last month our country's top intelligence officials told Congress that the U.S. is vulnerable to cyber espionage, cyber crime, and outright destruction of computer networks, both from sophisticated government-sponsored assaults from countries like China and Iran, as well as criminal hacker groups and cyber terrorists. We know that foreign nations are conducting reconnaissance on our critical infrastructures and utilities, including our gas lines and water systems and energy grids. If the ability to send a silent attack through our digital networks falls into our enemies' hands, this country could be the victim of a devastating attack. Last December, Iran 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. And just last year, an al Qaeda operative issued a call for electronic jihad against the United States, comparing our technological vulnerabilities to that of our security before 9/11.

Yet while these threats are imminent, no major cybersecurity legislation that would help protect us has been enacted since 2002. Quite simply, we are not prepared to meet the threats of the 21st century.

This act improves coordination in government, providing for a strategic plan to assess the cybersecurity risk and guide the overall direction of Federal cyber R&D. It updates the National Institutes of Standards and Technology's responsibilities to develop security standards for Federal computer systems to ensure computer hygiene and processes for agencies to follow.

Our bill also establishes a Federal-university-private-sector task force to

coordinate research and development, improves training of cyber professionals, and continues the much-needed cybersecurity research and development programs at the National Science Foundation and NIST.

This bill has been endorsed, as the chairman stated, by leading industry groups, including the U.S. Chamber of Commerce and Tech America. Most importantly, this bill is fiscally responsible. It is not being paid for with any new money since it is intended to work within the boundaries of funds authorized and appropriated to NSF and NIST. I'm confident that this legislation will advance the work these agencies are doing to bolster our domestic cybersecurity, as much as I'm confident that this Congress will finally address in a meaningful way the urgent need to pass this bipartisan cybersecurity legislation at that time. So I urge my colleagues to support this legislation.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I yield 5 minutes to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. Mr. Speaker, I want to start by thanking the gentlelady for yielding and for her support on this bill, and thank Chairman SMITH for his support and for moving the bill early in this Congress. I also want to thank Mr. MCCAUL for working with me on this bill for the third straight Congress and for his broader leadership in Congress on cybersecurity issues.

Two Congresses ago when Democrats were in the majority, I was the lead sponsor of this bill. Last Congress, Mr. MCCAUL became the lead sponsor. Both times the bill passed with overwhelming bipartisan support, which is a testament to the importance of this bill and to the quality of the work that has gone into it. Hopefully in this Congress, as Mr. MCCAUL said, the House and the Senate will finally pass this vital piece of the puzzle in protecting America's cybersecurity.

When I began working on this bill in 2010, it was clear that our use of the Internet and other communication networks would continue to grow and evolve, and that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve, too. This has turned out to be all too true.

Just last month, the Director of National Intelligence testified before the Senate Intelligence Committee that the danger of cyber attacks and cyber espionage on crucial infrastructure tops the list of global threats to our Nation. I believe that we face the possibility of a cyber ''Pearl Harbor'' that could destroy America's military or economic security. We have already seen the loss of countless jobs through cyber espionage, and we face—and thankfully, so far, we have repelled—much worse attacks every day. It is now more important than ever that we get this legislation onto the President's desk.

H.R. 756 will increase the security of our networks and information systems by building strong public-private partnerships, improving the transfer of cybersecurity technologies to the marketplace, training a cybersecurity workforce for both the public and private sectors, and coordinating and prioritizing Federal cybersecurity R&D efforts.

In addition to requiring a strategic plan for Federal cybersecurity R&D among all of the relevant Federal agencies, this bill explicitly authorizes programs and activities at the National Science Foundation and the National Institute of Standards and Technology. Both of these agencies play an important and unique role in the Federal Government's efforts to secure cyberspace.

This bill also builds on recommendations of the administration's cyberspace policy review. The first step is education, including educating individuals, companies, and especially the next generation of IT professionals. This legislation works towards these goals by building on existing partnerships, such as the NSF-sponsored Center for System Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois. This college has trained hundreds of teachers and college faculty in cybersecurity-related areas since 2003, individuals who are now teaching at colleges and technical training programs nationwide.

H.R. 756 utilizes these existing programs across the country by providing scholarships to students pursuing cybersecurity degrees in exchange for their service in the Federal IT workforce. This approach not only provides for the immediate workforce needs of the Federal Government but also builds a pipeline for private industry.

Of course, research, standards, and education are only part of the cybersecurity solution, but they are critical pieces of the puzzle that Congress must complete to secure our Nation.

Mr. Speaker, I want to thank again Mr. MCCAUL for his work on this legislation. I urge Members to support it.

Mr. SMITH of Texas. Mr. Speaker, I yield 2 minutes to the gentleman from California (Mr. ROHRABACHER) who is the vice chairman of the Science, Space, and Technology Committee.

Mr. ROHRABACHER. Mr. Speaker, first of all I would like to thank LAMAR SMITH and Congressmen MCCAUL and LIPINSKI for the leadership that they've provided on this very significant issue.

First of all, I would like to say that I am completely supportive of this bill. This legislation will continue America's path toward greater capabilities on cybersecurity. This is critical to our national security and our future.

And while we are increasing the authorization levels in this legislation for these critical activities, we are aware that every new dollar that we spend is a dollar that we borrowed, probably from China.

□ 1310

The Communist Chinese regime, of course, is the greatest human rights abuser in the world and potential adversary of the United States.

Furthermore, there has been unequivocal evidence that the Chinese Government is a source of significant cyber attacks on targets within the United States, which leads me to the main point, being, we must take note that there are many students from China and students from other known cyber attack countries attending our universities, participating in our programs, and learning exactly how we are setting up our system and defenses.

We need to apply a little common sense here, which is so often missing from our government, of course; and we need to make certain that we are not funding, enabling, and training our potential enemies.

Section 106 of this legislation clearly limits the Scholarships for Service program to citizens or permanent residents of the United States. But that limitation is not extended to the Graduate Traineeships Program, which is also authorized; nor does it extend that limitation to the National Science Foundation Graduate Research Fellowship program, which has previously been expanded to include computer and network security specializations.

Other cybersecurity programs give funding to and rely upon universities that are now training both sides in a future cyber war.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. SMITH of Texas. Mr. Speaker, I yield the gentleman an additional 2 minutes.

Mr. ROHRABACHER. So here we might end up, if we're not careful on how we approach this battle that we're having for the security of our country, we could end up financing both sides of a potential cyber conflict. We don't need to do that.

The Chinese graduate students that head home, after being trained by the American taxpayers, and they're supposed to head home, by the way, after they go through education here, if they go home, they could end up becoming soldiers in China's cyber war against us.

We need to consider the fundamental questions of how we got ourselves into this predicament, and that was through our policies of technology transfer, trade, and investment that benefited and actually were structured in a way to transfer wealth to China.

We need solutions to get ourselves out of this problem and not be in jeopardy from this Communist Chinese dictatorship that still exists in Beijing. Well, turning off the funding spigot to those who threaten us and potentially could do us harm is the first step.

So I would hope that as this legislation works its way through the Senate and elsewhere, that we make sure that there are limitations placed on it so that no students from countries that

are possible enemies of the United States, but are currently engaged in cyber attacks, should be able to be funded by this program.

But with that said, the purpose of the program is terrific. We need to do it, and we need to do it right. And I congratulate my friends and my colleagues for the good job they've done.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I yield 5 minutes to the gentleman from Rhode Island (Mr. LANGEVIN).

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

Mr. LANGEVIN. I thank the gentlelady for yielding.

Before I begin, let me just say that my heart goes out to all those who lost their lives and were injured in the terrorist attack at the Boston Marathon yesterday. My thoughts and prayers are with them and their families, and we pray for a quick recovery for all of those who were hurt. And our thoughts and prayers are with everyone in Boston at this difficult time.

I also would like to take a minute just to comment on and to lend my support to the previous bill that was just debated, H.R. 1163, the FISMA reform bill that was before the House, vitally important for updating our reporting of cybersecurity incidents and other issues relating to enhancing our cybersecurity. And I commend Chairman ISSA for his leadership on that, as well as others on the committee who are supporting that bill.

But, Mr. Speaker, I am pleased today to rise as a supporter and cosponsor of the Cybersecurity Enhancement Act, offered by my good friend and colleague, the chairman of the Homeland Security Committee, as well as the co-chair, along with me, on the Cybersecurity Caucus, Chairman MCCAUL.

Mr. Speaker, it seems that every week we read about a new cyber attack taking place. Last month, the Mandiant Report detailed a campaign of espionage against hundreds of corporations around the world. The New York Times and other media companies have also been victims of recent attacks; and we saw in South Korea last month the financial and communications sectors can clearly be vulnerable to these pernicious attacks as well.

Mr. Speaker, the cyber threat is real. Protecting our networks is a complex task that we, in Congress, need to focus more on and address. Chairman MCCAUL and I served together on the CSIS Commission on Cybersecurity for the 44th Presidency, and I am happy to report that the Cybersecurity Enhancement Act builds on the important work that we did there.

As we are constantly reminded, today's threat may not be tomorrow's, due to the prodigious rate of technological innovation. This bill before us today encourages coordination between Federal agencies tasked with cyber research and development and requires them to develop a strategic plan for R&D activities.

Success in this area demands a skilled cyber workforce, something that we currently lack. This bill takes an important first step in correcting our course by reauthorizing NSF graduate fellowships in cybersecurity and requiring the President to issue a report addressing our critical cyber workforce shortage.

So, Mr. Speaker, with that, let me again thank the gentleman from Texas for his outstanding leadership on this issue. He's been a visionary on working to protect our Nation's cybersecurity, and I greatly appreciate his efforts and that of many others. I look forward to continuing to work with him, and I'm pleased to support this bipartisan piece of legislation.

I also recognize Mr. LIPINSKI and his leadership on this issue as well.

Mr. SMITH of Texas. Mr. Speaker, we have no more requests for time on this side, so we'll be prepared to yield back at the right time.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I yield 1 minute to the gentlewoman from Texas (Ms. JACKSON LEE).

Ms. JACKSON LEE. Let me thank the chairman and the ranking member for their leadership on the Science Committee, and thank the proponents of this legislation, my chairman on the Homeland Security Committee, Mr. MCCAUL, and Mr. LIPINSKI, for their bipartisanship on something that is enormously crucial; and it is certainly crucial for those of us who serve on both Judiciary and Homeland Security and probably a number of others.

What I want to applaud most of all is the R&D and expanded training. We will need to have a cadre, an army of civilians, who understand the protection of America's cyber landscape, if you will. And it is a domestic issue, as well as a security issue, because America's energy and utilities and medical care all are tied into the cybersphere.

Whether or not it is a youngster who wants to hack, or whether or not it is an aggressive foreign country, it is valuable and important for us to be trained. I'd like to offer the importance of Historically Black Colleges and Hispanic-serving Colleges as well, being part of this very important effort and, as well, to educate the private sector, which has 85 to 80 to 90 percent, in essence, of the private sector dealing with cybersecurity.

Let me complete, Mr. Speaker, by saying as we move forward, I think it is important for Homeland Security to be a lead on some of these issues, particularly the bill coming forward. But I applaud this legislation. I congratulate the proponents and sponsors and ask my colleagues to support this legislation.

The SPEAKER pro tempore. Members are reminded to please heed the gavel.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I have no further requests for time. I'd like to just urge that we support the bill, and I thank the chairman.

I yield back the balance of my time.

□ 1320

Mr. SMITH of Texas. I yield back the balance of my time.

Ms. ESTY. Mr. Speaker, I rise today in support of H.R. 756, the Cybersecurity Enhancement Act of 2013—legislation that I'm proud to cosponsor, which will both enhance our national security and help boost our economy.

Cybersecurity is increasingly essential to our national defense and to our economic security in the 21st century.

As the Internet and other communication networks have grown and become more sophisticated, so have the threats from individual hackers, criminal syndicates, and even other governments.

It's critical that we take steps today to encourage and better coordinate the research and development of cybersecurity technology on a national scale.

The Cybersecurity Enhancement Act will help ensure that our country is prepared to face the security threats of the 21st century, that our businesses have the IT protections they need to compete on a global scale. I am proud that we're making critical investments in science and IT education for our young people and our educational institutions.

By authorizing grants and prioritizing research areas with the National Science Foundation and the National Institute of Standards and Technology, this legislation will help boost workforce development. In Connecticut, home to high-tech manufacturing and top-quality universities and technical schools, these workforce investments are essential to our economic future.

Mr. Speaker, for the sake of our nation's security, for the sake of our businesses, for the sake of our economy, I urge a yes vote on this bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. SMITH) that the House suspend the rules and pass the bill, H.R. 756, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. SMITH of Texas. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

ADVANCING AMERICA'S NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT OF 2013

Mr. SMITH of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 967) to amend the High-Performance Computing Act of 1991 to authorize activities for support of networking and information technology research, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows: