never will be forgotten. All of us have a responsibility to give voice to the challenges crime victims face, not just this week, but for every week of the year.

IN RECOGNITION OF LOCKHEED MARTIN'S F–22 PROGRAM

(Mr. GINGREY of Georgia asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. GINGREY of Georgia. Mr. Speaker, I rise today with a heavy heart as the delivery ceremony of the last F–22 Raptor will take place next Wednesday in Marietta, Georgia, my hometown, tail No. 195—far short of what our Air Force needs.

Over the last three decades, the Cobb County community has watched the F–22 grace our skies as thousands of our citizens have worked steadfastly to make the Marietta production a model line. Many of our neighbors have indeed had a direct hand in producing the most capable fighter jet in history. The program has been a critical component of America's industrial base and a source of economic strength, creating 25,000 American jobs in 44 States and representing more than $12 billion in annual economic activity. The F–22 protects our citizens and our soldiers, and it deters America's enemies. Its legacy will be a credit to our community for years to come.

Mr. Speaker, I ask my colleagues to join me in recognizing Lockheed Martin and the F–22 program.

WORKERS' MEMORIAL DAY

(Mr. HIMES asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. HIMES. Mr. Speaker, I rise today on Workers' Memorial Day because 25 years ago in Bridgeport, Connecticut at L'Ambience Plaza, 28 construction workers lost their lives building a building using the controversial lift-slab construction technique, which even at the time was subject to controversy and is now subject to very significant regulation. This sad accident could easily have been avoided, but because the proper safety regulations were not in place, 28 men did not go home that day. When I attended a ceremony earlier this week to commemorate L'Ambience, I met with some of the families. The men were husbands, fathers, brothers, and neighbors.

Day in and day in out in this Chamber we hear about job-killing regulations from the other side. And yes, we must make sure that our regulations are finally balanced, but it has become religious in this Chamber that all regulations, whether they are there to preserve the lives of construction workers or to keep children from dying of asthma, are ''job-killing regulations.'' If this stays this ideological and this religious, we will see more killing of the real kind.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (Mr. WOODALL). Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote incurs objection under clause 6 of rule XX.

Record votes on postponed questions will be taken later today.

CYBERSECURITY ENHANCEMENT ACT OF 2012

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2096) 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. 2096

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 2012''.

TITLE I—RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

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

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

SEC. 102. FINDINGS.

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

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

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

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

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

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

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

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

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

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

(b) CONTENTS OF PLAN.—The strategic plan required under subsection (a) shall—

(1) specify and prioritize near-term, mid-term and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) and how the near-term objectives complement research and development areas in which the private sector is actively engaged;

(2) describe how the Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

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

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

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

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

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

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

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

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

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

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

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

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

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

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

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

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

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

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

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

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

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

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

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

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

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

''(B) $90,000,000 for fiscal year 2014; and

''(C) $90,000,000 for fiscal year 2015.''.

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

(1) in paragraph (4)—

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

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

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

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

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

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

''(B) $4,500,000 for fiscal year 2014; and

''(C) $4,500,000 for fiscal year 2015.''.

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

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

''(B) $19,000,000 for fiscal year 2014; and

''(C) $19,000,000 for fiscal year 2015.''.

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

''(A) $2,500,000 for fiscal year 2013;

''(B) $2,500,000 for fiscal year 2014; and

''(C) $2,500,000 for fiscal year 2015.''.

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

''(A) $24,000,000 for fiscal year 2013;

''(B) $24,000,000 for fiscal year 2014; and

''(C) $24,000,000 for fiscal year 2015.''.

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

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Scholarship for Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure.

(b) CHARACTERISTICS OF PROGRAM.—The program under this section shall—

(1) provide, through qualified institutions of higher education, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as—

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional development opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions and community colleges; and

(C) development of cybersecurity-related courses and curricula.

(c) SCHOLARSHIP REQUIREMENTS.—

(1) ELIGIBILITY.—Scholarships under this section shall be available only to students who—

(A) are citizens or permanent residents of the United States;

(B) are full-time students in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution; and

(C) accept the terms of a scholarship pursuant to this section.

(2) SELECTION.—Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need, to the goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b), and to veterans. For purposes of this paragraph, the term ''veteran'' means a person who—

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

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

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

(3) SERVICE OBLIGATION.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time as provided in paragraph (5). If a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by—

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

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

(4) CONDITIONS OF SUPPORT.—As a condition of acceptance of a scholarship under this section, a recipient shall agree to provide the awardee institution with annual verifiable documentation of employment and up-to-date contact information.

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

(d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) GENERAL RULE.—If an individual who has received a scholarship under this section—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section; or

(E) fails to fulfill the service obligation of the individual under this section,

such individual shall be liable to the United States as provided in paragraph (3).

(2) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall—

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligation; and

(B) provide to the Director, on an annual basis, post-award employment information required under subsection (c)(4) for scholarship recipients through the completion of their service obligation.

(3) AMOUNT OF REPAYMENT.—

(A) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(B) MORE THAN ONE YEAR OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship

awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS.—A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher 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.

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.

Not later than 180 days after the date of enactment of this Act the President shall transmit to the Congress a report addressing the cybersecurity workforce needs of the Federal Government. The report shall include—

(1) an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs;

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

(3) an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise, including individuals from States or regions in which the unemployment rate exceeds the national average;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities; and

(5) recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

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

(b) FUNCTIONS.—The task force shall—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

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

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

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

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

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of 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; and

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

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

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

SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

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

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

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

(4) improve the usability of identity management systems.

SEC. 206. AUTHORIZATIONS.

No additional funds are authorized to carry out this title and the amendments made by this title or to carry out the amendments made by sections 109 and 110 of this Act. This title and the amendments made by this title and the amendments made by sections 109 and 110 of this Act shall be carried out using amounts otherwise authorized or appropriated.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentleman from Illinois (Mr. LIPINSKI) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include extraneous material on this bill, as amended, now under consideration.

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

There was no objection.

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

Mr. Speaker, today Congress has a historic opportunity to lay the groundwork to defend our Nation against cyberattacks. We're not just talking about mischievous online activity, but actions that could bring America to its knees.

Unfortunately, this is not science fiction. America is under attack, not by armies advancing on our beaches or planes overhead, but in the virtual world, where those who intend to do us harm have already penetrated our Federal and private computer networks and continue to plot relentlessly to bring down our critical infrastructure. Our water supply, nuclear facilities, air traffic control systems, electrical grid, and defense and banking systems are all vulnerable to a crippling attack.

General Keith Alexander, Director of the National Security Agency, said it is not a matter of if, but when a cyber Pearl Harbor occurs. We are just simply fortunate that a computer-based attack has not brought physical harm to Americans, but that is not for a lack of trying.

China has already successfully stolen some of our biggest military secrets, such as information about the F–35 Joint Strike Fighter, the Department of Defense's biggest weapons program ever. Now they know the program well enough not only to copy it, but to guard against it. Similar attacks continue unabated on our military's computer systems. Hackers trick soldiers into downloading viruses onto their computers, after which every keystroke is recorded. Mr. Speaker, our military secrets are being stolen every day.

Imagine if agents of a foreign government were breaking into the Pentagon and stealing top secret documents, paper files. It would not be tolerated. It would be all over the front page of The Washington Post. And yet in the virtual world, that is occurring. In fact, the October 2011 Report to Congress on Foreign Economic Collection and Industrial Espionage states it is part of China and Russia's national policy to try to identify and take sensitive technology which they need for their own development. In fact, they train and have a cyberwarfare college.

The degradation of our national security and intellectual property from cybertheft threatens to weaken us where we have historically been strong. The NSA calculates that Russia and China have stolen $1 trillion in American intellectual property, the biggest

transfer of wealth in history. Their philosophy is: Why invent when you can steal it?

Besides nation-states, there are groups such as Anonymous, LulzSec, and AntiSec who indulge in nonstate ''hacktivism.'' Their agenda is to bully, embarrass, and steal from those that they disagree with philosophically or politically. They think nothing of closing down Web sites, hacking into email and voice mail, and taking sensitive information from those who don't do their bidding.

There has been a lot of hard work going into this Cyberweek and a lot of thought to find solutions. As cochair of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th President, I helped draft recommendations for securing the country's government networks and critical infrastructures.

□ 0920

As a member of the Speaker's Cyber Task Force and chairman of the House Cybersecurity Caucus, I helped present those recommendations to Congress in the legislation we have seen this week. The historic legislation the House votes on this week incorporates many of these recommendations.

This bill, the Cybersecurity Enhancement Act, gives the National Institute of Standards and Technology the authority to set security standards for Federal computer systems and develop checklists for agencies to follow.

Why is that important?

It hardens our Federal networks. Every Federal agency has been hacked into by agents of a foreign power, by activists. Every Federal agency, including the Pentagon, has been hacked into. This bill will harden those Federal networks and make them less vulnerable to such an attack.

It also creates a Federal/university/private sector task force to coordinate research and development. It establishes cybersecurity research and development grant programs and improves the quality of our cyber workforce by creating a scholarship program.

Importantly, it creates an education and awareness program for computer hygiene. When you talk to the NSA, they tell you that computer hygiene accounts for the majority of cyberattacks. This would remedy the majority of vulnerabilities that we face.

And finally, it sets forth procurement standards for hardware and software that will minimize security risks. This will also have a ripple effect in the private sector so that they will also adopt such procurement standards.

Other legislation we saw that passed yesterday facilitates the sharing of threat information between the public and private sector, which controls most of our critical infrastructure. While it's not part of this bill, I think it's important to make the analogy that what we did yesterday was simply allow the Federal Government to share signature threat information with the private sector, similar to a police officer sharing with a homeowner a threat that they see of someone breaking into their house and then telling them how they can better protect their house and lock the door without the door being opened.

These commonsense reforms are a baseline of what we need to secure our infrastructure. We must take action before life is lost and our economy and defenses have been weakened to the point of damaging our country.

One of the biggest failures after 9/11 was the knowledge that the attacks could have possibly been prevented with better intelligence information-sharing and protective measures. There was also a lack of imagination.

And while we can't change the past, we can use it as a lesson, as we go forward in our modern cyberworld, a world in which our water supply, defense systems, nuclear power plants, electrical grid, banking systems, FAA, and other critical infrastructures are vulnerable to cyberthieves, -attacks, and -terrorists.

We know what has to be done. Mr. Speaker, the time to act is now.

With that, I reserve the balance of my time.

Mr. LIPINSKI. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 2096, the Cybersecurity Enhancement Act. I'd like to first thank my colleague, Mr. MCCAUL, for his hard work on this critical piece of national cybersecurity policy.

As cofounder of the House Cybersecurity Caucus, Mr. MCCAUL has played a key role in this policy area that is becoming increasingly important to our Nation. Our work together on this legislation, which began last Congress, demonstrates that this bill is good, bipartisan public policy that should once again receive overwhelming support in this House.

In 2009, the President called for a comprehensive 60-day review of U.S. cyberspace policy. That call and the subsequent expert recommendations contained in the report led to a series of hearings on cybersecurity R&D and resulted in the Cybersecurity Enhancement Act of 2010, which I sponsored and worked on with Mr. MCCAUL in the Science and Technology Committee in the last Congress. That bill passed this Chamber by a vote of 422–5. Unfortunately, it was not taken up by the Senate.

Since that time, cyberthreats have only increased. So last May, Mr. MCCAUL and I introduced this bill once again to address the pressing education, research, and development and standards and practices aspects of cybersecurity.

In America, every individual and every organization, including the Federal Government, is vulnerable to cybercrime. Our most sensitive data are stored on computers, and around the world there are countless individuals, groups, and nations relentlessly focused on exploiting gaps in our cybersecurity system.

The Federal Trade Commission estimates that identity theft costs consumers about $50 billion annually. The Department of Commerce was targeted this month in a cyberattack that required the Economic Development Administration to completely unplug from the network. And just yesterday, the Homeland Security Committee heard from witnesses about Iran's development of a cyberarmy.

Cybercrime evolves as quickly as technology itself. Thus, it will take a collective effort by the Federal Government, the private sector, our scientists and engineers, and every American to defeat it. And H.R. 2096 will help to do this.

The first step is education. This bill builds on existing partnerships, such as the NSF-sponsored Center for Systems Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois. This community 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. 2096 also provides scholarships for students pursuing degrees in cybersecurity 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 it also builds a pipeline for private industry.

Now, in addition to a skilled IT workforce, our Nation also needs advances in basic R&D. Cyberthreats are constantly evolving, and cybersecurity must reflect the comprehensive efforts that build towards a more secure foundation in the short and long terms.

So this legislation requires relevant Federal agencies to work with the National Science and Technology Council to develop a national strategic plan for cybersecurity R&D that sets priorities based on risk assessments, focuses on transformational technology, and strengthens technology transfer programs. It will build on infrastructure that we need to get the best ideas out of the lab and into the marketplace. And because people are perhaps the weakest link in many IT systems, the research strategy will include the social sciences to help us better understand how humans interact with technology.

Promoting public awareness of good computer hygiene can go a long way to protecting our systems. The dissemination of simple concepts, such as installing antivirus software and not opening emails from unknown sources, can go a long way in reducing the threat of cybercrime.

The legislation also calls on the National Institute of Standards and Technology to be a leader in both domestic

and international cybersecurity standards. As Mr. MCCAUL said, H.R. 2096 tasks NIST with developing a comprehensive international cybersecurity strategy that defines what working and IT technical standards we need, determines where they're being developed, and ensures the United States is represented.

Finally, in recognition of the Federal Government's increasing effort to utilize remote data centers, known as cloud computing, in this Congress, I worked to add language so that the bill now directs NIST to work with other agencies and with experts in the private sector to ensure the consistent and secure standards on cloud computing are put in place across the Federal Government. As cloud computing is used more and more by the Federal Government, we must make sure that this data is safe.

Mr. Speaker, this bill is a necessary and vitally important step toward securing our public, private, and personal IT systems. It is a good bipartisan bill, and I urge my colleagues to support it.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield 3 minutes to the gentleman from Texas (Mr. HALL), my good friend and colleague, the chairman of the Science and Technology Committee.

□ 0930

Mr. HALL. I want to thank my fellow Texas Representative, MICHAEL MCCAUL, for his very capable leadership, for his wonderful opening statement. It allows me to spend less time. He has knowledge of cybersecurity issues that is a very important asset to this Congress and is a benefit to the Nation, and I'm pleased to join him as a cosponsor of H.R. 2096, the Cybersecurity Enhancement Act of 2012. As he stated so eloquently, as our reliance on information technology expands, so do our vulnerabilities.

Protecting the Nation's cyber-infrastructure is a responsibility shared by a number of different Federal agencies, including the National Science Foundation and the National Institute of Standards and Technology.

H.R. 2096 primarily addresses important cybersecurity research and development efforts conducted at or led by these agencies. It reauthorizes existing but expired research and education programs at NSF while eliminating two unnecessary programs and enhances scholarships to increase the size and skills of the Federal cybersecurity workforce.

It strengthens the cybersecurity R&D standards, development and coordination, and education and awareness at NIST; and it provides for strategic planning for cybersecurity R&D across the Federal Government. This is a good, fiscally responsible bill that enjoys broad bipartisan support.

It represents a modest but critical piece of Congress' overall efforts to address the comprehensive cybersecurity needs of the United States.

This bill has the support of numerous organizations, including the U.S. Chamber of Commerce, which calls H.R. 2096

an important step toward improving Federal cybersecurity R&D activities to improve the security, reliability, and resilience of America's digital infrastructure in partnership with industry.

I support the passage of H.R. 2096 and encourage my colleagues to do the same.

Mr. LIPINSKI. I'd like to yield to the gentleman from Rhode Island (Mr. LANGEVIN) 5 minutes.

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

Mr. LANGEVIN. I thank the gentleman for yielding.

Mr. Speaker, I'm pleased to rise today in strong support of the Cybersecurity Enhancement Act offered by my good friend and colleague, the cochair of the Cybersecurity Caucus, Mr. MCCAUL. The gentleman and I have been at this issue for several years now; and when we first began the effort back in '06 or '07, I think for the most part most people, when we talked about cybersecurity, it was, cyber what? Oh, how things have changed.

I think we certainly, collectively, between him and I and many others, have raised the awareness of this issue, its importance, and the challenges that we face in securing our Nation in cyberspace, and I deeply am grateful for his efforts.

It is impossible to overstate the importance of the cyberdomain to our national security, our infrastructure, and our economic competitiveness. Clearly, we all recognize how much we use the Internet every day in our daily lives, whether it's for commerce or communication, social networking, or national security issues. It really has become a part of our daily lives. But in securing the cyberdomain, we also face immense challenges.

Cyberthreats are clearly growing more numerous, sophisticated, and successful. We all know of someone who perhaps has had their bank accounts hacked and had money stolen or their identity stolen or their credit card number or Social Security number stolen because of a cyberattack on a company or government institution. We also have heard of numerous attacks, and we see them daily in the area of cyber-espionage, and the gentleman from Texas did a great job in outlining some of the specific challenges.

The F–35 is one case in particular that comes to mind. There are billions of dollars in R&D that is stolen on a daily or weekly basis by our adversaries; and, of course, we have heard and have documented numerous issues of cyberattacks. Thankfully, nothing major yet in this country. But as General Alexander, the Director of the NSA, has outlined, these days perhaps would come and we need to do all we can to avoid them.

Well-intentioned technological changes that create great efficiencies through automation and advanced management techniques, of course, can leave us even more vulnerable to cyber-exploitation.

Clearly, these efficiencies that have been brought through automation have helped us to be much more efficient; but as the test from Idaho National Labs, which showed how easy it would be to conduct a ''skater attack'' that penetrated systems that are government safety systems. Pumps and valves and generators could easily be penetrated and cause that generator to blow itself up. So these things can happen, and we need to do all we can to avoid them. Make sure that that day never comes.

Now, obviously, we have to tap into our creative and innovative spirit to address today's challenges and position ourselves to be agile in the face of tomorrow's threats.

I'm pleased that this bill helps us to make this need a reality by strengthening the coordination and cooperation among the various cyber-research and development efforts across the Federal Government.

The fruits of that research will be critical to our Nation's future defense and the cyberdomain.

Additionally, I'm pleased to highlight that this bill enhances programs that increase the size and skills of our Nation's cybersecurity workforce. Now, we have obviously a critical shortage of qualified cyber-experts, and we need to address that need. The director of the CIA's Clandestine Information Technology Office estimates that we only have about a thousand people that can operate in the country at world-class levels in cyberspace, and what he says is we need somewhere between 20,000 and 30,000 people.

We all heard about the skills gap that we face in this country where, in particular, high-tech companies are having a real difficult time finding qualified workers to fill those jobs of the 21st century. We need to do better in closing our skills gap.

To this end, last year the National Defense Authorization Act commissioned a study that the Pentagon had to conduct to determine its cyberworkforce needs and give them a better situation awareness about who they have with those capabilities and what their needs will be both now and in the future. It was a successful study, and the Pentagon is putting that plan and that information into action to close that gap.

And at the high school level in Rhode Island and in several of the other States, we, working with the Sands Institute, created the cyberchallenge. We need to focus on our young people and get them focused on a potential career in cybersecurity, and that program has been incredibly successful.

So in closing that gap and developing a cyberworkforce, this legislation is an important step in that effort. So I want to thank the gentleman from Texas for his leadership on this issue, and I'm

pleased to support this bipartisan legislation.

Mr. MCCAUL. Let me just as a point of personal privilege say and give my thanks to the gentleman from Rhode Island (Mr. LANGEVIN), my good friend, colleague, cochair of the Cybersecurity Caucus, for your vision, your leadership on this very, very important issue. As you know and I know, we were very into this issue of cybersecurity 6 years ago, before it was really cool to be into cybersecurity. So thank you so much for your leadership.

With that, Mr. Speaker, I yield 2 minutes to the gentleman from Texas (Mr. THORNBERRY), my good friend and colleague and also the chairman of the Speaker's Cybersecurity Caucus.

Mr. THORNBERRY. I thank the gentleman for yielding, and I appreciate the chairman of the Science Committee, Mr. HALL, and the ranking member, Ms. JOHNSON, for bringing this bill and the next bill to the floor. This will mean the House will have passed four bills this week related to cybersecurity, taking important steps in the right direction.

I particularly appreciate the work of the gentleman from Texas, Mr. MCCAUL, and Mr. LIPINSKI for bringing this bill to the floor. As they have said, they've been working on it for a while, and I appreciate their persistence and also the substance of the bill.

Of course, the gentleman from Texas, Mr. MCCAUL, as you've heard, has been working in this area for a number of years, and the study that he cochaired with Mr. LANGEVIN with the CSIS Commission on Cybersecurity remains one of the leading studies in this field.

Mr. Speaker, this bill is important. You've heard about the education and awareness. It also helps make sure that the research and development is coordinated so that we don't duplicate within the Federal Government, but also that it is complementary to what the private sector is doing.

□ 0940

I think it's important to emphasize that the answer to cybersecurity is not a government program; it is our people and innovation. That is really the key. So others may steal information from us—they may even copy some of the things they steal—but what they can't do is produce the sort of innovation and new approaches that are absolutely essential to our future. That's part of the reason this bill is important. It's part of the reason we have to be careful about new regulations and other things that some people want to do because nurturing the innovation that comes from this country, from the private sector and the government, is absolutely essential to our future.

So I appreciate all of the work that the gentleman from Texas and others have done, not only on this bill but in the larger scheme of things, as it cuts across a number of committees, and it takes our country a few steps in the right direction. But it's important that we take those steps for our future security.

Mr. LIPINSKI. Mr. Speaker, I yield such time as she may consume to the gentlelady from Texas, the ranking member of the committee, Ms. JOHNSON.

Ms. EDDIE BERNICE JOHNSON of Texas. Let me express my appreciation to the leaders of this bill. This is a good bipartisan bill, and it is nearly identical to the legislation that passed the House by an overwhelming majority in the last Congress. I would like to certainly cite Mr. LIPINSKI and Mr. MCCAUL for their leadership and work on this bill.

The Internet—and our access to the Internet through computers, tablets, smartphones, et cetera—has greatly increased our productivity and connectivity. Unfortunately, this connectivity and the dependence of our infrastructure, our commerce, and a great deal of our day-to-day lives on information technologies have increased our vulnerability to cyberattack. For example, you may recall last year, the networks of 48 companies were penetrated for at least 6 months by a hacker who was looking for intellectual property to steal, and it was reported that the personal information of nearly 80 million video game users was compromised.

So we need to do what we can to help ensure that these sorts of intrusions are minimized. To do this, we need to build strong partnerships between our Federal agencies, businesses, nongovernmental organizations, and educational institutions.

I am pleased that H.R. 2096 strengthens the public-private partnerships, guarantees a proactive and comprehensive Federal cybersecurity R&D portfolio, trains the next generation of cybersecurity professionals, and ensures the development of robust cybersecurity technical standards. These activities are essential to our efforts to advance the security of our current information and communication systems and to build future systems that are more secure from the outset.

I would simply close by saying thank you to Mr. MCCAUL and to Mr. LIPINSKI. I hope that we get this bill passed.

Both of the agencies covered in H.R. 2096, the National Science Foundation and the National Institute of Standards and Technology, play an important and unique role in the Federal effort to secure cyberspace.

While I support the passage of H.R. 2096, I would be remiss if I did not take this opportunity to express some disappointment over the language in H.R. 2096 that authorizes a cybersecuity awareness and education program at NIST.

During Committee consideration of H.R. 2096, I offered an amendment to ensure that the education and awareness activities authorized by the bill accurately represent NIST's current role as the coordinator of the National Initiative for Cybersecurity Education, or NICE.

I was pleased that my Republican colleagues offered to work with me to address this concern. However, the language in the bill we are considering today still falls short and fails to accurately reflect these activities.

NICE, under NIST's leadership, is playing an important and critical role in improving cybersecurity education in this country. Unfortunately, my Republican colleagues were resistant to language that specifically addressed NICE's role in formal cybersecurity education.

I believe that this is a regrettable omission and that we missed an opportunity to ensure that the initiative focuses sufficient attention on developing the next generation of cybersecurity professionals. I hope that this shortcoming can be addressed as the bill moves to the Senate.

President Obama has 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.

H.R. 2096 will help to advance these important goals and improve the Nation's resiliency to cyber attack.

I'd like to take a moment to thank both the Majority and Minority staff for their work on this bill, and in particular thank Marcy Gallo on my staff for her hard work. I urge my colleagues to support this important legislation.

Mr. MCCAUL. Mr. Speaker, does the gentleman from Illinois have any additional speakers?

Mr. LIPINSKI. Just myself. I am ready to close.

Mr. MCCAUL. Then I reserve the balance of my time.

Mr. LIPINSKI. Mr. Speaker, I want to thank Mr. LANGEVIN, the other cochair of the Cybersecurity Caucus, for all of his work. I want to thank Ranking Member JOHNSON for her work, Chairman HALL, and especially Mr. MCCAUL for coming together on this bill.

We started this in the last Congress. Hopefully, we will get it finished in this Congress. We know that cyberthreats are everywhere—from cyberarmies that are threatening our Nation to cybercrime that threatens the financial security of all Americans. This bill addresses three key pieces of protecting our Nation: improving education, R&D, and the development of standards. All of these are key pieces we have to continue to develop as the threats develop, and this will help us to do that.

So I want to urge my colleagues to vote for this bill, and I yield back the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield myself such time as I may consume.

Let me first recognize Mr. LIPINSKI for his excellent leadership. We've been pushing this bill. It's the second Congress in which we've pushed it. I certainly hope that this time it goes to the Senate and gets signed into law.

Mr. LIPINSKI, you've been a real leader on cybersecurity. It has been an honor to serve with you on the Science and Technology Committee together. Let me, again, thank you for all of your great efforts.

At a time of intense partisanship, when there is so much acrimony on

both sides of the aisle, it is refreshing to see a moment when we can come together as Americans first, regardless of party affiliation, and do something that's right. Cybersecurity is in the best interest of the Nation. Defending the United States is a fundamental element under the Constitution. So, for me, personally, to see us come together like we have today is a very refreshing thing.

My father flew in a B–17 over Europe in 35 bombing missions. He was a bombardier. At that time, the state of warfare was very kinetic. They handed down a better country to this generation, but we're faced with a new threat. They're not bombs of his era, of his day, but, rather, digital bombs that can be dropped at any time and that have dropped on this government—on the Federal Government—and on our private sector. Bombs that have stolen trillions of dollars of intellectual property. Bombs that have committed espionage and stolen our military secrets. And bombs that could be conducted in a cyberwarfare attack.

I think the thing that keeps me up most at night is the idea of cyberwarfare, because we know what our offensive capability is. We know what we can do and conduct as a Nation against another nation. That technology in the wrong hands, in a country's like Iran, can cause great devastation against the interests of the United States, can bring down power grids, can bring down financial institutions. Every critical infrastructure tied to the Internet is vulnerable to this type of attack. So I believe that this legislation will protect this Nation from such attacks.

We all came up here to serve, not for ego, not for title but, at the end of the day, to make a difference, to make a fundamental difference in the lives of Americans. So I believe a moment like this is a great moment in which we can reflect back on later in our lives and think, you know, I made a difference. This bill protects Americans and future generations.

Let me thank all of those who have been involved in this critical legislation and, particularly, Mr. LIPINSKI for your patriotism to this country and for what you've done in getting this to move forward.

With that, Mr. Speaker, I yield back the balance of my time.

Ms. JACKSON LEE of Texas. Mr. Speaker, I rise today in support of H.R. 2096, the ''Cybersecurity Enhancement Act.'' The bill would reauthorize several National Science Foundation (NSF) programs that aim to enhance cybersecurity. In addition, it would require the National Institute of Standards and Technology (NIST) to continue a cybersecurity awareness program and to develop standards for managing personal identifying information stored on computer systems. Further, it would establish a task force which would recommend actions to improve our Nation's cybersecurity.

Cyberspace can easily be considered the nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

This issue is not new to me nor to any other Member of Congress. As a senior Member of the Judiciary Committee I have faced the problems which arise when there are breaches and how best to protect our system in both the Crime and Intellectual Property Subcommittees.

As a senior Member of the Homeland Security Committee, I am deeply concerned about vulnerabilities in our cyber security protection. For the last few years, threats originating in cyberspace have risen dramatically. The policy of the United States has been to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States.

I realize that we must act in advance to reduce all of our vulnerabilities to these types of threats, in order to prevent any damage to the cyber systems supporting our Nation's critical infrastructures.

According to the Government Accountability Office (GAO) the threat posed by cyber attacks is heightened by vulnerabilities in federal systems and systems supporting critical infrastructure. Specifically, significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems supporting the operations, assets, and personnel of Federal Government agencies.

For example, 18 of 24 major Federal agencies have reported inadequate information security controls for financial reporting for fiscal year 2011, and inspectors general at 22 of these agencies identified information security as a major management challenge for their agency.

Moreover, GAO, agency, and inspector general assessments of information security controls during fiscal year 2011 revealed that most major agencies had weaknesses in most major categories of information system controls. These and similar weaknesses can be exploited by threat actors, with potentially severe effects.

In addition, the number of cybersecurity incidents reported by Federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past 6 years, the number of incidents reported by Federal agencies to the Federal information security incident center has increased by nearly 680 percent.

These incidents include unauthorized access to systems; improper use of computing resources; and the installation of malicious software, among others.

Reported attacks and unintentional incidents involving Federal, private, and infrastructure systems demonstrate that the impact of a serious attack could be significant, including loss of personal or sensitive information, disruption or destruction of critical infrastructure, and damage to national and economic security.

Federal agencies are facing a set of emerging cybersecurity threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms. Examples of these threats include spam (unsolicited commercial e-mail), phishing (fraudulent messages to obtain personal or sensitive data), and spyware (software that monitors user activity without user knowledge or consent).

Cyber attacks are analogous to guerilla warfare. Attribution of an attack to a specific source or entity is a significant challenge in cyberspace because the Internet was built on an open, anonymous platform. This architecture permits the original source of an attack to be easily masked. While an attack may be traced to a specific country, this does not necessarily mean that the government of that country is behind the attacks. Moreover, because of the near universal access to the Internet, disruptive activity can come from individual actors located in any corner of the globe.

In February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyberattacks as a means to target the United States.

The Federal Bureau of Investigation has identified multiple sources of threats to our Nation's critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization.

For these reasons and more, I support this bipartisan legislation. We must continue to support the research and development of technology that will help to combat threats to our cybersecurity. It is also essential to train and develop the professionals who are able to continue with the implementation of countermeasures and are the future of R&D.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 2096, 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. MCCAUL. 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 question will be postponed.

□ 0950

ADVANCING AMERICA'S NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT OF 2012

Mr. HALL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3834) 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.