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.

FEDERAL INFORMATION SECURITY AMENDMENTS ACT OF 2013

Mr. ISSA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1163) to amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1163

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 ''Federal Information Security Amendments Act of 2013''.

SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are to—

''(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) recognize the highly networked nature of the current Federal computing environment and provide effective Governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities assets;

''(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

''(4) provide a mechanism for improved oversight of Federal agency information security programs and systems through a focus on automated and continuous monitoring of agency information systems and regular threat assessments;

''(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information systems important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and

''(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

''§ 3552. Definitions

''(a) SECTION 3502 DEFINITIONS.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AUTOMATED AND CONTINUOUS MONITORING.—The term 'automated and continuous monitoring' means monitoring, with minimal human involvement, through an uninterrupted, ongoing real time, or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat development.

''(3) INCIDENT.—The term 'incident' means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

''(4) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, which means ensuring timely and reliable access to and use of information.

''(5) INFORMATION SYSTEM.—The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information and includes—

''(A) computers and computer networks;

''(B) ancillary equipment;

''(C) software, firmware, and related procedures;

''(D) services, including support services; and

''(E) related resources.

''(6) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given that term in section 11101 of title 40.

''(7) NATIONAL SECURITY SYSTEM.—

''(A) DEFINITION.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) EXCEPTION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(8) THREAT ASSESSMENT.—The term 'threat assessment' means the formal description and evaluation of threat to an information system.

''§ 3553. Authority and functions of the Director

''(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

''(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

''(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(A) information collected or maintained by or on behalf of an agency; or

''(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

''(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3554(b);

''(6) coordinating information security policies and procedures with related information resources management policies and procedures;

''(7) overseeing the operation of the Federal information security incident center required under section 3555; and

''(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

''(A) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40;

''(B) significant deficiencies in agency information security practices;

''(C) planned remedial action to address such deficiencies; and

''(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(b) NATIONAL SECURITY SYSTEMS.—Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

''(c) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the

case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

''(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

''(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of the agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40 and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

''(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

''(iii) ensuring the standards implemented for information systems and national security systems of the agency are complementary and uniform, to the extent practicable;

''(C) ensuring that information security management processes are integrated with agency strategic and operational planning and budget processes, including policies, procedures, and practices described in subsection (c)(2);

''(D) as appropriate, maintaining secure facilities that have the capability of accessing, sending, receiving, and storing classified information;

''(E) maintaining a sufficient number of personnel with security clearances, at the appropriate levels, to access, send, receive and analyze classified information to carry out the responsibilities of this subchapter; and

''(F) ensuring that information security performance indicators and measures are included in the annual performance evaluations of all managers, senior managers, senior executive service personnel, and political appointees;

''(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

''(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information system;

''(B) determining the levels of information security appropriate to protect such information and information systems in accordance with policies, principles, standards, and guidelines promulgated under section 11331 of title 40 and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) for information security classifications and related requirements;

''(C) implementing policies and procedures to cost effectively reduce risks to an acceptable level;

''(D) with a frequency sufficient to support risk-based security decisions, testing and evaluating information security controls and techniques to ensure that such controls and techniques are effectively implemented and operated; and

''(E) with a frequency sufficient to support risk-based security decisions, conducting threat assessments by monitoring information systems, identifying potential system vulnerabilities, and reporting security incidents in accordance with paragraph (3)(A)(v);

''(3) delegate to the Chief Information Officer or equivalent (or a senior agency official who reports to the Chief Information Officer or equivalent), who is designated as the 'Chief Information Security Officer', the authority and primary responsibility to develop, implement, and oversee an agencywide information security program to ensure and enforce compliance with the requirements imposed on the agency under this subchapter, including—

''(A) overseeing the establishment and maintenance of a security operations capability that through automated and continuous monitoring, when possible, can—

''(i) detect, report, respond to, contain, and mitigate incidents that impair information security and agency information systems, in accordance with policy provided by the Director;

''(ii) commensurate with the risk to information security, monitor and mitigate the vulnerabilities of every information system within the agency;

''(iii) continually evaluate risks posed to information collected or maintained by or on behalf of the agency and information systems and hold senior agency officials accountable for ensuring information security;

''(iv) collaborate with the Director and appropriate public and private sector security operations centers to detect, report, respond to, contain, and mitigate incidents that impact the security of information and information systems that extend beyond the control of the agency; and

''(v) report any incident described under clauses (i) and (ii) to the Federal information security incident center, to other appropriate security operations centers, and to the Inspector General of the agency, to the extent practicable, within 24 hours after discovery of the incident, but no later than 48 hours after such discovery;

''(B) developing, maintaining, and overseeing an agencywide information security program as required by subsection (b);

''(C) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 11331 of title 40;

''(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

''(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

''(4) ensure that the agency has a sufficient number of trained and cleared personnel to assist the agency in complying with the requirements of this subchapter, other applicable laws, and related policies, procedures, standards, and guidelines;

''(5) ensure that the Chief Information Security Officer, in consultation with other senior agency officials, reports periodically, but not less than annually, to the agency head on—

''(A) the effectiveness of the agency information security program;

''(B) information derived from automated and continuous monitoring, when possible, and threat assessments; and

''(C) the progress of remedial actions;

''(6) ensure that the Chief Information Security Officer possesses the necessary qualifications, including education, training, experience, and the security clearance required to administer the functions described under this subchapter; and has information security duties as the primary duty of that official; and

''(7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Officer with responsibility for the entire agency, and all components thereof, to implement, monitor, and hold senior agency officers accountable for the implementation of appropriate security policies, procedures, and controls of agency components.

''(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director and consistent with components across and within agencies, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

''(1) automated and continuous monitoring, when possible, of the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of information and information systems that support the operations and assets of the agency;

''(2) consistent with guidance developed under section 11331 of title 40, vulnerability assessments and penetration tests commensurate with the risk posed to agency information systems;

''(3) policies and procedures that—

''(A) cost effectively reduce information security risks to an acceptable level;

''(B) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated pursuant to section 11331 of title 40;

''(iii) minimally acceptable system configuration requirements, as determined by the Director; and

''(iv) any other applicable requirements, including—

''(I) standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

''(II) the National Institute of Standards and Technology standards and guidance;

''(C) develop, maintain, and oversee information security policies, procedures, and control techniques to address all applicable requirements, including those promulgated pursuant section 11331 of title 40; and

''(D) ensure the oversight and training of personnel with significant responsibilities for information security with respect to such responsibilities;

''(4) with a frequency sufficient to support risk-based security decisions, automated and continuous monitoring, when possible, for testing and evaluation of the effectiveness and compliance of information security policies, procedures, and practices, including—

''(A) controls of every information system identified in the inventory required under section 3505(c); and

''(B) controls relied on for an evaluation under this section;

''(5) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

''(6) with a frequency sufficient to support risk-based security decisions, automated and continuous monitoring, when possible, for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued by the National Institute of Standards and Technology, including—

''(A) mitigating risks associated with such incidents before substantial damage is done;

''(B) notifying and consulting with the Federal information security incident center and other appropriate security operations response centers; and

''(C) notifying and consulting with, as appropriate—

''(i) law enforcement agencies and relevant Offices of Inspectors General; and

''(ii) any other agency, office, or entity, in accordance with law or as directed by the President; and

''(7) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

''(c) AGENCY REPORTING.—Each agency shall—

''(1) submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b) to—

''(A) the Director;

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(C) the Committee on Oversight and Government Reform of the House of Representatives;

''(D) other appropriate authorization and appropriations committees of Congress; and

''(E) the Comptroller General;

''(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

''(A) annual agency budgets;

''(B) information resources management of this subchapter;

''(C) information technology management under this chapter;

''(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

''(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576);

''(F) financial management systems under the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note); and

''(G) internal accounting and administrative controls under section 3512 of title 31; and

''(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

''(A) as a material weakness in reporting under section 3512 of title 31; and

''(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note).

''§ 3555. Federal information security incident center

''(a) IN GENERAL.—The Director shall ensure the operation of a central Federal information security incident center to—

''(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

''(2) compile and analyze information about incidents that threaten information security;

''(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

''(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

''(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

''(c) REVIEW AND APPROVAL.—The Director shall review and approve the policies, procedures, and guidance established in this subchapter to ensure that the incident center has the capability to effectively and efficiently detect, correlate, respond to, contain, mitigate, and remediate incidents that impair the adequate security of the information systems of more than one agency. To the extent practicable, the capability shall be continuous and technically automated.

''§ 3556. National security systems

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

''(3) complies with the requirements of this subchapter.''.

SEC. 3. TECHNICAL AND CONFORMING AMENDMENTS.

(a) TABLE OF SECTIONS IN TITLE 44.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the matter relating to subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''Sec.
''3551. Purposes.
''3552. Definitions.
''3553. Authority and functions of the Director.
''3554. Agency responsibilities.
''3555. Federal information security incident center.
''3556. National security systems.''.

(b) OTHER REFERENCES.—

(1) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552(b)''.

(2) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(3) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(4) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(5) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(A) in subsections (a)(2) and (e)(5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''; and

(B) in subsection (e)—

(i) in paragraph (2), by striking ''section 3532(1)'' and inserting ''section 3552(b)''; and

(ii) in paragraph (5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''.

(6) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)''.

SEC. 4. NO ADDITIONAL FUNDS AUTHORIZED.

No additional funds are authorized to carry out the requirements of section 3554 of title 44, United States Code, as amended by section 2 of this Act. Such requirements shall be carried out using amounts otherwise authorized or appropriated.

SEC. 5. EFFECTIVE DATE.

This Act (including the amendments made by this Act) shall take effect 30 days after the date of the enactment of this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. ISSA) and the gentleman from Maryland (Mr. CUMMINGS) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. ISSA. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous materials on the bill under consideration.

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

There was no objection.

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

Cybersecurity threats represent one of the most serious national security and economic challenges we face in our Nation. Whether it's criminal hackers, organized crime, terrorist networks, or nation-states, our Nation is under siege from dangerous cybersecurity threats that grow daily in frequency and sophistication.

It is critical that the Federal Government address cybersecurity threats in a manner that keeps pace with our Nation's growing dependence on technology, but current Federal law does not adequately address the nature of today's cybersecurity threats.

Since the enactment in 2002 of the Federal Information Security Management Act, or FISMA, it has become a ''check the box'' compliance activity that all too often has little to do with minimizing cyber threats. And yet the Government Accountability Office recently found that security incidents among 24 key agencies increased by 650 percent, or more than six-fold, in the last 5 years.

To address the rising challenge posed by cyber threats, Ranking Member CUMMINGS and I introduced last Congress a bill to reauthorize FISMA. That

bill was adopted by the House unanimously.

Recently, Mr. CUMMINGS and I reintroduced that legislation as H.R. 1163, the Federal Information Security Amendments Act of 2013. The bill was voted out of our committee by unanimous vote on March 20. This bill aims to harness the last decade of technological innovation in securing Federal information systems.

To enhance the current framework of securing Federal information technology systems, our bill calls for automated and continuous monitoring of government information systems—and I'm going to repeat—automated and continuous monitoring of government information systems. And it ensures that continuous monitoring finally incorporates regular threat assessments, not just ''check the box.''

The bill also reaffirms the role of the Office of Management and Budget with respect to FISMA, recognizing that the budgetary leverage of the Executive Office of the President is necessary to ensure agencies are focused on effective security IT systems. Mr. Speaker, that's particularly significant because IT is the backbone of every single large and small agency of the government; and only with the power of the President through the Office of Management and Budget can you, in fact, ensure that the President has transparency and his authority is respected throughout all these agencies.

We can no longer afford the ''check the box'' that came out of the first piece of legislation. It wasn't its intent, and the six-fold increase in the last 5 years says it has failed us.

While our bill does not include new requirements, restrictions, or mandates on private, non-Federal computer systems, H.R. 1163 does highlight the need for stronger public-private partnership. Again, as we interface over the public Internet, it is critical that the weakest link be prevented. To that extent, this bill has received strong support from cybersecurity experts and industry, including TechAmerica, the Information Technology Industry Council, and the Business Software Alliance.

I'd like to personally thank Ranking Member CUMMINGS for partnering, both personally and through his staff, to create a bill that is necessary, timely, and accurate to meet the growing threat of cybersecurity.

I encourage all Members to support this timely legislation, and I reserve the balance of my time.

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

I want to begin by thanking Chairman ISSA for sponsoring this legislation and for making this a truly bipartisan effort. I am pleased to join the chairman in sponsoring this bill again this Congress.

Also, I thank the other cosponsors of the bill, including the chairman and the ranking member of the Subcommittee on Government Operations, Representatives JOHN MICA and GERRY CONNOLLY, and the chairman and the ranking member of the Subcommittee on National Security, Representatives JASON CHAFFETZ and JOHN TIERNEY.

Last month, the Director of National Intelligence, James Clapper, placed cyber attacks at the top of his list of national security threats. This bill is an important step in Congress' response to the cyber threat. This legislation would ensure that Federal agencies use a risk-based approach to defend against cyber attacks and protect government information from being compromised by our adversaries.

It is important that the Federal Government set the example by ensuring that its own information is protected. The Department of Energy was hacked in January, and personal data for hundreds of employees was compromised. We are better than that, Mr. Speaker, and we can do better.

Personal data for more than 100,000 accounts in the Thrift Savings Plan was compromised last year when a contractor's computer was hacked. This bill would shift the Federal Government to a system of continuous monitoring of information systems. And just this morning, the chairman said in a hearing that we have to do more with less and we have to figure out ways to use technology so that we can efficiently and effectively do the things that we need to do.

This bill goes right in that direction, which is so important. It would also streamline reporting requirements and ensure that agencies take a smart, risk-based approach to securing networks.

This bill would continue to authorize the Office of Management and Budget to set Federal policy for information security. This is important because we need to hold all the agencies accountable for developing appropriate standards and living up to those very standards. OMB is the appropriate entity to be responsible for ensuring that that happens.

However, nothing in this bill will prevent the Department of Homeland Security from continuing the great work it is doing to protect our Nation against potential cyber attacks. The Department has expanded its cybersecurity workforce and is working with agencies to establish continuous monitoring. This bill supports that work by making clear that agencies must take action to protect their networks, rather than just doing routine ''check the box'' reports, as Chairman ISSA just talked about.

□ 1240

Today, we have a bipartisan effort. It is truly a bipartisan effort to address a problem that affects every single American and business, every entity of our Nation. That's why it's so good that we had all of our subcommittee rankings and chairmen working together and Mr. ISSA making sure that this legislation got out. As it is so very important, I urge my colleagues to vote in favor of this legislation.

With that, I reserve the balance of my time.

Mr. ISSA. Mr. Speaker, I yield myself 1½ minutes.

I want to associate myself with the ranking member's statements.

Mr. CUMMINGS does make the great point that Homeland Security is, in fact, doing a great deal. And if there is an active activity through NSA and other agencies, we applaud that.

A great deal of what this bill reauthorization is intended to do, in working with the subcommittee ranking member Mr. CONNOLLY, is to recognize that there needs to be a public-private partnership. We need our private entities to be as strong as they can be so they don't become conduits for espionage and for attacks. But also that, in fact, it's the smallest entity of government, the one that you don't think much of, the one that may not be high priority that, in fact, also has to be protected: commerce at our public parks; commerce occurring throughout the Federal Government; and, in fact, just the records that are so often collected and maintained in places like the Veterans Administration and so on.

Although they may not represent an immediate threat to national security, as a veteran, I must tell you the fact that those records sit there tells all of us, millions of veterans, that we want to have a robust maintenance of cybersecurity, something that under the current statute we believe the box is being checked, but not all that needs to be done is being done.

I reserve the balance of my time.

Mr. CUMMINGS. It gives me great pleasure, Mr. Speaker, to yield 3 minutes to a gentleman who has worked very hard on this issue night and day, and it's been at the forefront of his efforts, the gentleman from Virginia (Mr. CONNOLLY).

Mr. CONNOLLY. Mr. Speaker, I thank the distinguished ranking member, my friend from Maryland, and I also thank the distinguished chairman of the Oversight and Government Reform Committee.

I proudly join them in cosponsoring this legislation and rising in strong support of H.R. 1136, the Federal Information Security Amendments Act of 2013. The chairman and ranking member of the full committee have worked in a bipartisan fashion to advance this bill to the floor today, and they deserve great credit.

H.R. 1163 is desperately needed to address a looming and critical threat to our Nation's economic and national security. As the Government Accountability Office testified before our committee in its 2013 High Risk Report, the number of cyber incidents has grown exponentially among Federal agencies and, for that matter, in the private sector.

Specifically, in the year 2006, they reported 5,503 cyber incidents to the U.S. Computer Emergency Readiness Team.

Six years later, that same number was 48,562, which is an astounding 782 percent increase in just 6 years.

According to the Government Accountability Office, cyber attacks involving Federal systems and critical infrastructure, Mr. Speaker, could be devastating to the country. Yet, its audits have consistently revealed information security deficiencies in public and private, financial and nonfinancial systems.

More troubling, despite producing hundreds of recommendations over the past 2 fiscal years that would address security-control deficiencies, the majority of GAO's recommendations have, in fact, not been fully implemented. Unfortunately, vital Federal assets and missions will remain at high risk for fraud, misuse, and disruption unless agencies fully implement the literally hundreds of recommendations made by the GAO and various offices of the inspectors general aimed at strengthening the security of critical information systems.

The sophisticated and rapidly involving cybersecurity threat has outpaced the security framework established by the former Federal Information Security Management Act of 2002. FISMA's static, compliance-based framework, as noted by both the ranking member and the distinguished chairman of the committee, must be enhanced. It can't be used as a substitute for developing strategies to counter this threat.

I believe this bipartisan legislation will accomplish that goal by enhancing FISMA to promote a more dynamic, risk-based approach that leverages current technology to implement continuous monitoring of networks and systems.

Specifically, the Federal Information Security Amendments Act will direct agencies to test and evaluate information security controls and techniques and conduct threat assessments by monitoring information systems and identifying potential system vulnerabilities.

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

Mr. CUMMINGS. I yield the gentleman an additional 1½ minutes.

Mr. CONNOLLY. It will conduct vulnerability assessments and penetration tests commensurate with the risk posed to agency information systems and collaborate with OMB and appropriate public- and private-sector security operations centers on security incidents that extend beyond the control of the agency to require that security incidents be reported through an automated and continuous monitoring capability to the Federal Information Security Incident Center, appropriate security operations centers, and respective agency Offices of Inspector General.

Mr. Speaker, I join the distinguished chairman and ranking member of the Oversight and Government Reform Committee in urging all Members to support this critical bipartisan cybersecurity legislation that is urgently needed to provide Federal agencies with the necessary tools to effectively secure our Federal information systems.

With that, I thank them both for their leadership on this critical matter.

Mr. ISSA. I reserve the balance of my time.

Mr. CUMMINGS. I yield myself such time as I may consume.

As we have no other speakers, Mr. Speaker, I just want to make it clear that I think yesterday's incident in Boston should remind us of how fragile our society is and that there are so many people who want to do us harm.

A lot of times we concentrate on those kinds of attacks and don't spend the kind of time we really need to on the cyber attacks, which can be just as harmful, just as damaging. These cyber attacks can literally bring our country and our economy to a halt. That's why we are urging all Members to vote in favor of this.

And it is my hope, Mr. Speaker, that as we are addressing this issue today, that it will send the word out to the Nation that once again our committee and this Congress is putting a microscope on this issue and doing everything in our power to make sure that our efforts are effective and efficient because the threats are there, and they are real.

It is up to us. It is our watch. It is our watch, just like a watchman watching over a fort or watching over a city. We are the watchmen right now, and it's our watch, and we have to make sure we do everything in our power to make sure that we protect against this very clear threat.

With that, I urge all Members to vote in favor of this legislation, and I yield back the balance of my time and.

Mr. ISSA. Mr. Chairman, I yield myself the balance of my time.

Mr. Speaker, H.R. 1163 has many authors: Mr. CUMMINGS and myself, Mr. CONNOLLY, Mr. CHAFFETZ, Mr. TIERNEY. It also has every committee chairman and every ranking member here in the House. And I would like to take a moment to thank all the committee chairmen of Homeland Security, Foreign Affairs, and House Administration, because staffs from all of those committees, particularly with the acquiescence of the chairmen and ranking members, have contributed to our fact-finding to try to produce a good bill here today.

I think often our committee is viewed as, what is your authority and so on. This is an odd situation in which, in order for us to bring the bill here today, we really needed all the agencies and all the personnel here to be brought to bear so that we could try to fashion a piece of legislation that would allow the Federal Government to work better, that would allow the executive branch to execute better on behalf of the American people.

□ 1250

Lastly, I would like to thank the outside groups, many of which I mentioned in my opening statement, but even more who responded when this bill was posted for comment. They responded with constructive suggestions.

I know there is a lot of trepidation any time the government is, in fact, looking at data passing through the system, but this and other legislation is a balancing act. We cannot have the economy that we enjoy today if these systems are shut down by attacks. At the same time, I know I join with the ranking member and all of the authors of this legislation in that we are committed to making sure we maintain the personal freedom and the privacy that goes with what we are entrusted to here in the government.

So, in closing, Mr. Speaker, this is an update. It is not the last time we will have to update cybersecurity. It is not the last time we will be here concerned about America's economy so dependent on the Internet, but it is a good bill. It is ready.

I urge its approval, and I yield back the balance of my time.

COMMITTEE ON HOMELAND SECURITY,
HOUSE OF REPRESENTATIVES,
Washington, DC, April 11, 2013.

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

DEAR CHAIRMAN ISSA: On March 20, 2013, the Committee on Oversight and Government Reform ordered H.R. 1163, the ''Federal Information Security Amendments Act of 2013'', reported favorably to the House with certain provisions in the legislation that fall within the Rule X jurisdiction of the Committee on Homeland Security. Specifically, this legislation would require the Department of Homeland Security to share cyber threat information with an information security center, delegate the authority and primary responsibility of information security to a Chief Information Security Officer responsible for overseeing a Department-wide information security program, and recognize the existence of a Federal information security incident center, which in practice, is currently the National Cybersecurity and Communications Integration Center at the Department of Homeland Security.

The Office of Management and Budget (OMB) issued Memorandum M–10–28 on July 6, 2010, transferring many of OMB's Federal information security and responsibilities to the Department of Homeland Security. Since Memorandum M–10–28 was issued, the Department of Homeland Security has conducted the operational aspects of Federal information security through the functions of the National Cybersecurity and Communications Integration Center and the United States Computer Emergency Readiness Team. This legislation, through its accompanied report, preserves the operational capabilities of DHS pertaining to Federal information security while reaffirming OMB's supervisory role with respect to FISMA.

I understand the importance of advancing this legislation to the House floor in an expeditious manner. Therefore, the Committee on Homeland Security will not seek a sequential referral over provisions within our jurisdiction. This action is conditional on our mutual understanding and agreement that doing so will in no way diminish or alter the jurisdiction of the Committee on Homeland Security over the subject matter included in this or similar legislation. In addition, I would like to thank you for working

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