ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on the motion 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.

Any record vote on the postponed question will be taken later.

FEDERAL INFORMATION SECURITY AMENDMENTS ACT OF 2012

Mr. ISSA. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4257) to amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4257

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 2012''.

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)(2), by striking ''section 3532(1)'' 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. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material 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. Madam Speaker, I yield myself such time as I may consume.

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

□ 1840

It is critical that the Federal Government address cybersecurity threats in a manner that keeps pace with the Nation's growing dependence on technology. The President himself recently stated: ''Cybersecurity is a challenge that we as a government or as a country are not adequately prepared to counter.''

Madam Speaker, it is essential that we, in fact, change that here today.

Current 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 security threats, and yet the Government Accountability Office recently found that security incidents among 24 key agencies increased more than 650 percent during the last 5 years.

To address the rising challenge posed by cyberthreats, Ranking Member CUMMINGS and I introduced H.R. 4257, the Federal Information Security Amendments Act of 2012. The bill aims to harness the last decade of technological innovation in securing the Federal information systems. It amends FISMA to move beyond the check-the-box compliance mentality. It enhances the current framework for securing Federal information technology systems.

Our bill calls for automated and continuous monitoring of government information systems. And it ensures that control monitoring finally incorporates regular threat assessment and—Madam Speaker, this is the most important part of what we do—continuous monitoring and constant threat assessments so that never again will we find that the incidents are going up double digits every month in some cases.

The bill also reaffirms the role of the Office of Management and Budget, or OMB, 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 of its IT systems.

While our bill does not include new requirements, restrictions, or mandates on private or non-Federal computer systems, H.R. 4257 does highlight the need for stronger public-private partnerships. Through our Web site, keepthewebopen.com, our bill has been vetted by the American people. It has also received strong support from cybersecurity experts and industry, including the Information Technology Industry Council and the Business Software Alliance.

I'd like to thank my ranking member, Mr. CUMMINGS, for a one-on-one equal partnership with me in the efforts to address the growing threat for cybersecurity. He has led the way on his side of the aisle, and I have been honored to serve on my side. We have encouraged all Members to support this timely legislation. We recognize that some things are too important to be partisan. This certainly is one of them.

I reserve the balance of my time.

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

Madam Speaker, first of all, I'd like to express my appreciation to the chairman of our committee for his kind words and for his cooperation. I start by thanking him for working with me and my staff to make this a bipartisan effort, and it is truly a bipartisan effort. From the beginning, we agreed that we did not want to make securing our Federal information systems a partisan issue and that securing our Nation against a cyberattack is an issue that transcends any party lines. This bill is evidence of the good work that we can do when we work together to address an important issue like cybersecurity.

Not only does this bill enjoy bipartisan support, but it is noncontroversial. Last week, the bill was marked up in committee and passed on a voice vote. The only amendments considered made constructive changes to the bill that were recommended by the National Institute of Standards and Technology and the Government Accountability Office. These changes enjoyed universal support in committee.

This legislation will ensure that Federal agencies use a risk-based approach to defend against cyberattacks and protect government information from being compromised by our adversaries. The bill would make key changes to help protect our Federal information systems from cyberattacks. It would shift the Federal Government to a system of continuous monitoring of information systems, streamline reporting requirements, and ensure that agencies take a smart, risk-based approach to securing networks.

This bill will 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 agencies accountable for developing appropriate standards and living up to them. However, nothing in this bill would prevent the Department of Homeland Security from continuing the great work it is doing to protect our Nation against potential cyberattacks.

The Department has dramatically expanded its cybersecurity workforce, and it has built the National Cybersecurity and Communications Integration Center to serve as Federal Government's cybersecurity command center. This command center is a vital part of our efforts to protect Federal information systems.

Earlier this month, the head of U.S. Cyber Command, General Keith Alexander, testified that securing our Nation against cyberthreats is one of our biggest national security challenges. Securing our Federal information systems is a critical component of addressing this challenge, and I urge my colleagues to join me and our chairman in supporting this legislation.

With that, Madam Speaker, I reserve the balance of my time.

Mr. ISSA. Madam Speaker, we have a speaker on the other side for a colloquy, so I'd reserve at this time to allow him to go next.

Mr. CUMMINGS. I want to thank the gentleman.

Madam Speaker, I yield 3 minutes to the gentleman from Virginia (Mr. CONNOLLY).

Mr. CONNOLLY of Virginia. I thank my friend from Maryland, the distinguished ranking member.

I want to thank Chairman ISSA and appreciate the work of him and the ranking member, Mr. CUMMINGS, and their staff on this legislation, which I think is a thoughtful, bipartisan update to an information security bill actually written by my predecessor and the chairman's, Tom Davis of Virginia.

The FISMA Amendments Act transitions from compliance to performance metrics to address major shortcomings in Federal agency cybersecurity implementation. Of course, when considering the performance of Federal agencies, it's a natural extension to question the relationship between the executive branch and those agencies and the relationship among technology and cybersecurity-related positions within the executive branch.

I appreciate President Obama's focus on technology, particularly the chief information officer's 25-point plan, but I'm concerned that the current ad hoc nature of the CIO, CTO, and Cybersecurity coordinator could create certain risk and continuity of operations challenges when we look out to further administrations. I would ask Chairman ISSA if he shares those concerns.

I yield to the gentleman from California.

Mr. ISSA. I thank the gentleman. I do share those concerns and appreciate the gentleman's work on this.

Proper organization of the executive branch is essential to the successful long-term management of technology, and particularly cybersecurity.

This policy is going to require additional work. FISMA is not the end but, in fact, a starting point; and I look forward to working with the gentleman to make sure that as we work with the executive branch, including OMB, that we get it right and we keep the focus where it needs to be on all the agencies and bringing them together.

Mr. CONNOLLY of Virginia. Madam Speaker, I thank the chairman and look forward to working with him and the ranking member, as well as Mr. LANGEVIN of Rhode Island, who has been a leader on this subject, to advance legislation that will address executive branch organization in the context of cybersecurity. With the right framework, I believe the current and future administrations will be able to more efficiently implement these FISMA reforms and other related legislation. Given its jurisdiction, the Oversight and Government Reform Committee is the appropriate venue to develop such legislation, and I look forward to working with the committee chair and ranking member to advance it.

□ 1850

Mr. CUMMINGS. Madam Speaker, I yield 3 minutes to the gentleman from Rhode Island (Mr. LANGEVIN).

Mr. LANGEVIN. I thank the gentleman for yielding.

Madam Speaker, I rise to engage in a colloquy with my colleague and friend, the chairman of the Committee on

Oversight and Government Reform, Mr. ISSA.

I'd first like to thank the chairman for his hard work. His efforts to update the Federal Information Security Management Act have been commendably inclusive and bipartisan, and I want to thank him and his staff, as well as Mr. CUMMINGS and Mr. CONNOLLY and their staff, for all the outreach and good faith negotiation that's occurred during the crafting of this legislation.

There can be no question that the FISMA reform language before the House today is both sorely needed and long overdue. To this end, together with my good friend and our former colleague, Ms. Watson, I introduced an amendment that passed the House overwhelmingly last Congress during consideration of the FY 2011 National Defense Authorization Act.

That amendment, which was, unfortunately, stripped out during conference with the Senate, would have made important updates to FISMA, in addition to establishing a National Office for Cyberspace in the Executive Office of the President.

Such an office has been recommended by the Obama administration's 60–Day Cyberspace Policy Review, public-private sector working groups such as the CSIS Commission on Cybersecurity for the 44th Presidency, which I cochaired with my good friend, Mr. MCCAUL, and the GAO, as a response to security deficiencies throughout the Federal Government.

While I applaud my friend for delivering on the need for FISMA reform, I'd like to ask the chairman if he gave thought to such organizational changes within the executive branch and, in particular, an organization like a National Office for Cyberspace during the drafting of this legislation.

I yield to my friend.

Mr. ISSA. I thank the gentleman. And yes, we did. Your leadership on cybersecurity matters, including FISMA reform, have been essential.

When you and I served on the Select Intelligence Committee, I recognized that you put more time and effort into the behind-the-door work than any of us. And, in fact, you and I share some of the challenges that we faced with the DNI and other earlier organizations.

But I share with you that your suggestions on how we can, in fact, find single-point accountability in future legislation, in concert with this administration, is essential. I look forward to working with you on exactly that. I know of no other partner I could have on the other side of the aisle that is more prepared to do it, and I thank the gentleman.

Mr. LANGEVIN. I thank the gentleman for that. In that spirit, I'd like to encourage the gentleman to continue in this open and bipartisan fashion. I'd like to ask if you would be interested in working together on such subsequent legislation, along with Mr. CUMMINGS and Mr. CONNOLLY, who have been so involved and thoughtful on this issue.

I believe that such legislation should include strong, centralized oversight to protect our Nation's critical infrastructure, including budgetary oversight powers, while remaining accountable to Congress.

Mr. ISSA. I couldn't agree with the gentleman more. Your work with our staff has been essential. I look forward to doing exactly that, and I think we have to have that ongoing effort to get to there.

I saw the ranking member's head also shaking. I know that we will both look forward to working with you on a bipartisan basis.

Mr. LANGEVIN. I thank the gentleman for that, and I look forward to working with my good friend to ensure that our Federal Government is properly addressing this critically important issue.

Mr. ISSA. Madam Speaker, I yield 3 minutes to my colleague and the gentleman from Utah (Mr. CHAFFETZ), the chairman of the subcommittee that has done so much on, in fact, cybersecurity.

Mr. CHAFFETZ. Madam Speaker, I appreciate Chairman ISSA and his foresight and leadership on this issue in driving this forward. This is so, so important to our country and our nation, and for the Federal Government to operate properly.

Madam Speaker, I also want to thank and recognize the ranking member, Mr. CUMMINGS, his unparalleled support and need and just patriotism for what's good for this Nation, working together in a bipartisan way. This is what I think the American people want, and this is what they get in this bill.

I also want to share the fact that cybersecurity is a real threat. It's a threat to the mom who's got the computer sitting in there in the kitchen, and the kids are going in every direction, to the most secure infrastructure we have in our Federal Government. It is imperative that we get this right, because everything from a guy in a van down by the river to nation-states, our country is under a constant bombardment and attack, for our intellectual property, to trade secrets, to what's going on in this government.

And while this is focused on what our government is doing and how it's organized, it updates the law so that we have the right provisions at the right place, and we're doing the right things. We have to be vigilant as a people. So this is focused, not—it doesn't give a new mandate. There's no new mandate upon the American people. There's no mandate upon businesses.

What this does is get the structure for what should happen in the Federal Government right, and updating and doing things like continuous monitoring, vulnerability assessments and penetration tests that are done within the Federal Government. It requires a chief information security officer within these different agencies, and it focuses these efforts upon the Director of OMB.

By really putting the focal point on the executive branch within the White House, you will get a much better response, because everything, from the Bureau of Indian Affairs to the Department of Defense and everywhere in between, we have to make sure that our systems are updated because the threat is constant, it is real, it is 24/7. And without these updates, without the constant monitoring, without these types of things, we will be doing a disservice to the American people, and we will not be living up to the commitment that we have to make sure that these networks are as secure as they possibly can be.

This is something that will be with us, not just for the next 6 months, not just for the next year, but for the foreseeable future. And Madam Speaker, that's why I'm so enthusiastic about this bill. I appreciate the bipartisan nature in which it was done. And I certainly appreciate Chairman ISSA and his leadership on this. I'm glad to be part of it.

I would encourage my colleagues to vote in favor of this bill.

Mr. CUMMINGS. We don't have any additional speakers. I reserve the balance of my time.

Mr. ISSA. Madam Speaker, I yield 2 minutes to the gentleman from Texas (Mr. THORNBERRY) who coordinated so much of the work that we're doing today from multiple committees.

Mr. THORNBERRY. I thank Chairman ISSA for yielding. Madam Speaker, I want to commend the chairman and the ranking member for working together and bringing this important bill to the floor.

I also want to commend the gentleman from Utah (Mr. CHAFFETZ), who was a member of our task force and, as the chairman noted, has done so much work on this.

Madam Speaker, this is an important bill on cybersecurity. The FISMA law passed in 2002 needs to be updated. The growth in the number and sophistication of the threats has not been matched by our response, and so laws and policies are increasingly outdated and not able to keep up with the threats faced by Federal networks as well as private sector networks.

And this bill requires continuous monitoring, as you have heard. The threat is dynamic. It changes. It doesn't work anymore to just check a box and say, I've done this. You have to have that continuous monitoring of what's happening within your networks. That's important for defense of the Federal Government, but it's also important to be an example for the rest of the country. And in cybersecurity, it seems to me, it's particularly important for the Federal Government to lead by example.

I also want to just say that this is an example of an issue, a part of cybersecurity, on which everybody agrees needs to happen, and this committee

has brought a bipartisan answer. We cannot allow differences that may exist between this body and the other body on other cybersecurity issues prevent us from taking action, getting something accomplished on something that everybody agrees on.

This is one of the things everybody agrees needs to happen. Information-sharing, everybody agrees on. Research and development that we'll have tomorrow on the floor, everybody agrees needs to happen.

I appreciate the work of this committee. It's an important bill. It will help make the Nation more secure, as well as this government, and I hope all Members will support it.

Mr. ISSA. Madam Speaker, at this time I have no other speakers, and I'm prepared to close.

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

Madam Speaker, I want to associate myself with all the words that have been said by both sides this evening, because we understand that cybersecurity is so very, very important to our Nation. We often look back to 9/11 and we think about what happened in that very short time, and how it disrupted our entire Nation, taking planes out of the air, causing our world to at least pause.

□ 1900

We saw the damage that was done in a matter of a few minutes.

Cybersecurity and the cyberthreat is just as great, if not far greater, and can happen very, very quickly. A cyberattack can take place very, very quickly, and it is something that we must do everything in our power to protect ourselves against. This bill does not solve all the problems, but it certainly leads us in the right direction.

Again, I want to thank the chairman. I want to thank everybody involved for the bipartisan effort and for making the security of our Nation our number one priority.

With that, I urge all of the Members to vote for this bill, and I yield back the balance of my time.

Mr. ISSA. Madam Speaker, in closing, I urge all Members to support the passage of this bill, H.R. 4257, as amended. I want to make one closing statement.

Often we talk about cybersecurity, and people think just about the Internet. We sit here in a room that is essentially windowless. I've been in this room when the lights are out. It is very, very dark. We would have a hard time finding our way out. Yet the very essence of keeping the grid up requires computers to talk to each other. Our phone systems, our lights, our power, our sewage, our water all depend today on interoperable computer systems that span the entire country and, in many cases, the entire world.

So, as people realize the government-to-government relationship and, particularly, the public-private partnerships that this bill encourages and asks the Office of Management and Budget to assure occur, we are doing so, of course, in order to maintain a reliable Internet; but much more importantly, the fundamentals of the very electricity that powers the Internet must be maintained and protected. I believe we've gone a long way today in the passage of this bill. I urge its passage.

I thank the gentleman from Maryland for his leadership on this important matter.

I yield back the balance of my time.

Mr. HALL. Madam Speaker, I would like to thank Chairman ISSA for the hard work that he and the Committee on Oversight and Government Reform has undertaken in the development of H.R. 4257, the Federal Information Security Amendments Act of 2012.

This bill updates and improves the decade old Federal Information Security and Management Act (FISMA). FISMA currently requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for their systems.

The Science, Space, and Technology Committee receives annual FISMA reports from each Federal agency. These reports detail the management and security of each agency's information technology resources, and the actions necessary to ensure the effectiveness of the government's information security policies.

The Science, Space, and Technology Committee monitors these reports to review the cybersecurity standards and guidelines that the National Institute of Standards and Technology sets for Federal information systems. These standards and guidelines are particularly important because along with agency use, the same standards and guidelines are frequently adopted on a voluntary basis by many organizations in the private sector. The Committee will continue to receive and review these annual FISMA reports from Federal agencies, and will provide continued oversight of NIST's role in FISMA process.

H.R. 4257 takes an important step forward in the protection of the government's information technology resources by establishing a mechanism for stronger oversight. The bill ensures implementation of new developments in technological innovation, including automated and continuous monitoring of cybersecurity threats as well as regular threat assessments.

Our Federal agencies depend on FISMA to guide them to protect federal networks. Officials are already working to integrate some of the concepts proposed by H.R. 4257, such as continuous monitoring, into the management of information systems. I am encouraged that this bill will help agencies more easily comply with the latest cybersecurity standards and guidelines set forth by NIST.

H.R. 4257 is a good bill that represents another critical piece in Congress's overall efforts to address the Nation's cybersecurity needs. There are additional tweaks that could make the bill even better, and I look forward to working with Mr. ISSA as the bill moves through the process to address remaining issues to our mutual satisfaction.

I support the passage of H.R. 4257 and encourage my colleagues to do the same.

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. 4257, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

HATERS OF RELIGION

(Mr. POE of Texas asked and was given permission to address the House for 1 minute.)

Mr. POE of Texas. Madam Speaker, in the quiet town of Woonsocket, Rhode Island, a 91-year-old memorial honoring hometown soldiers stands tall outside a local fire station. A stone bottom statue with a cross on top immortalizes the fallen heroes who sacrificed so much for our country. For decades, the memorial has stood in the shadows of the fire station with no complaints from local residents.

But a group of out-of-towners, not from Woonsocket, not even from Rhode Island, but from 1,000 miles away in Wisconsin, have self-righteously objected to the cross on top of the 91-year-old memorial. The antireligious hate group demands that the cross be removed. They also demand that the firefighters' prayer and angel from the Woonsocket Fire Department Web site be removed.

Madam Speaker, the firefighter prayer asks God to give them ''strength to save lives'' and to protect the families of the firefighters.

County officials will not succumb to the intimidation tactics of the bigoted group. The mayor has said he will not remove the cross under any circumstances because the Constitution protects the free exercise of religion whether this hate group likes it or not.

And that's just the way it is.

PAYCHECK FAIRNESS

(Ms. BERKLEY asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. BERKLEY. Madam Speaker, it's hard to believe that in the 21st century women in Nevada are still making only 83 cents for every dollar that a man makes.

What does that mean in real terms? It means a difference of $7,326 a year. It is not fair. In most cases, working women in Nevada are either the primary or the sole breadwinners of their families.

That's why I'm calling on the Speaker to follow the Senate's lead and to schedule a vote on the Paycheck Fairness Act, which is legislation that will help close the unacceptable wage gap between men and women in this country. Unfortunately, far too many in the House and the Senate are still living in the Dark Ages when it comes to basic fairness for women.

Women in Nevada are still shaking their heads in disbelief that in the year