

FEDERAL INFORMATION SECURITY AMENDMENTS ACT OF 2012

APRIL 26, 2012.—Committed to the Committee of the Whole House on the State of
the Union and ordered to be printed

Mr. ISSA, from the Committee on Oversight and Government
Reform, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 4257]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Government Reform, to whom
was referred the bill (H.R. 4257) to amend chapter 35 of title 44,
United States Code, to revise requirements relating to Federal in-
formation security, and for other purposes, having considered the
same, report favorably thereon with an amendment and rec-
ommend that the bill as amended do pass.

CONTENTS

	Page
Committee Statement and Views	8
Section-by-Section	12
Explanation of Amendments	15
Committee Consideration	15
Correspondence	16
Application of Law to the Legislative Branch	19
Statement of Oversight Findings and Recommendations of the Committee	19
Statement of General Performance Goals and Objectives	19
Federal Advisory Committee Act	19
Unfunded Mandate Statement	19
Committee Estimate	19
Budget Authority and Congressional Budget Office Cost Estimate	20
Changes in Existing Law Made by the Bill as Reported	21
Additional Views	51

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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

“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. 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.

COMMITTEE STATEMENT AND VIEWS

PURPOSE AND SUMMARY

The Federal Information Security Amendments Act of 2012 (H.R. 4257) enhances the Federal Information Security Management Act (FISMA) of 2002 by improving the framework for securing federal information technology systems. It also establishes a mechanism for stronger oversight of information technology systems by focusing on “automated and continuous monitoring” of cybersecurity threats and regular “threat assessments.” The severity and nature of the threat necessitates these changes, to enhance “real-time” cyber-security. Although these changes are now being implemented in some form by agencies, it is important that Congress codify a requirement that agencies Government-wide continue progressing toward the achievement of real time or near-real time continuous monitoring of federal information technology systems.

BACKGROUND AND NEED FOR LEGISLATION

The nature of cybersecurity threats

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges confronting our nation. These threats range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced Nation states. These types of threats appear likely to remain prevalent for years. The Federal Government must respond, then, by rapidly increasing its ability to defend against them. The President himself has acknowledged the existing deficit, stating recently that, “Cybersecurity . . . [is] a challenge that we as a government or as a country are not adequately prepared to counter.”¹

¹ The Comprehensive National Cybersecurity Initiative, President Obama, Mar. 2, 2010.

During the past few years, cybersecurity risks have continued to rapidly evolve and increase in both frequency and sophistication. On January 31, 2012, Robert S. Mueller, III, Director of the Federal Bureau of Investigations (FBI), testified before the Senate Select Committee on Intelligence that “stopping terrorists is the number one priority [for the United States], but down the road, the cyber threat will be the number one threat to the country.”² On July 28, 2010, Mueller testified before the Senate Judiciary Committee that the FBI found a 22 percent increase in cybersecurity breaches, with “more than 330,000 complaints involving more than \$550 million in losses.”³ Just as troubling, in October 2011, the Government Accountability Office found that security incidents among 24 key agencies had increased more than 650% during the last five years.⁴

Today, cybersecurity threats pose serious risks not only to the government, but also to private companies. Cyber criminals now target private firms in the finance, energy, and telecommunications industries, among others, seeking economic benefits and sometimes military advantages. For example, cyber criminals recently hacked Global Payments, a credit card, debit and gift card-processing firm for Visa and MasterCard, obtaining 1.5 million card numbers.⁵ Online retailer Zappos.com experienced a cybersecurity breach, ultimately endangering personally identifiable information from more than 24 million customers.⁶

The Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 (FISMA) was introduced by Rep. Tom Davis (R-VA) on March 5, 2002, in order to create a framework to protect federal information systems. FISMA became Title III of the E-Government Act of 2002, P.L. 107-347, addressing electronic government services, and was signed into law by President George W. Bush on December 17, 2002. The primary purpose of FISMA was to “provide for [the] development and maintenance of minimum controls required to protect federal information and information systems.”⁷ In doing so, FISMA established that each federal agency would develop and implement an agency-wide program to provide information security for the information systems that support that agency.⁸

Additionally, FISMA authorized the Director of the Office of Management and Budget to oversee federal agency information security policies and practices. This oversight included requiring each federal agency to “identify and provide information security protec-

²Testimony, Robert S. Mueller, III, Director, Federal Bureau of Investigations, Senate Select Intelligence Committee hearing, “Worldwide Threat Assessment of the US Intelligence Community,” Jan. 31, 2012.

³Testimony, Robert S. Mueller, III, Director, Federal Bureau of Investigations, Senate Committee on the Judiciary hearing, “Oversight of the Federal Bureau of Investigation,” Jul. 28, 2010.

⁴See, “Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements,” GAO-12-137, U.S. Government Accountability Office, Oct. 2011.

⁵“Global Payments Breach Details Fuzzy: 2 Weeks Later, Questions About Timing, Vulnerabilities Remain,” Tracy Kitten, GovInfoSecurity, April 13, 2012; See also, <http://www.govinfosecurity.com/global-payments-breach-details-fuzzy-a-4678> (last visited April 18, 2012).

⁶“Zappos Cyber Attack: ID Info Hacked,” David Li, NYPOST, Jan. 17, 2012; See also, http://www.nypost.com/p/news/national/zappos_cyber_attack_pWsrU60crm8SGHJWYGup7K (last visited April 18, 2012).

⁷The Federal Information Security Management Act of 2002 (FISMA).

⁸Id.

tions commensurate with the risk and magnitude of harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of information or information systems.”⁹ In addition to delegating responsibility to OMB, FISMA directed the National Institute of Standards and Technology (NIST) to set security compliance standards for federal information systems.¹⁰

Since its enactment, however, FISMA has become a compliance activity, where all too often ‘check-the-box’ compliance has taken precedence over security enhancement. To ensure that FISMA focuses on “real-time” threats and incorporates technological developments occurring in the decade since its enactment, H.R. 4257 was introduced. To address the increasing security breaches highlighted by the aforementioned GAO study, H.R. 4257 requires automated and continuous monitoring, when possible, and regular threat assessments.

The Office of Management and Budget Circular M-10-28

On July 6, 2010, OMB issued Memorandum, M-10-28, transferring many of its federal information security roles and responsibilities to the Department of Homeland Security. Individual agencies, however, are historically hesitant, often unwilling, to respond to the demands of another agency. Agencies tend to view themselves as being on equal footing within the broad government bureaucracy. Therefore, to maintain the budgetary leverage of the Executive Office of the President in ensuring FISMA compliance, H.R. 4257 reaffirms the current role of OMB in overseeing effective security over information technology systems. This will help ensure that all agencies attain high standards of FISMA compliance.

The legislation, however, continues to allow DHS—under the direction of OMB—to exercise responsibility within the executive branch for many of the operational aspects of FISMA. OMB will continue to be held firmly accountable for ensuring that individual agencies meet the new standards.

The Federal Information Security Amendments Act of 2012

To address the shortcomings of FISMA, H.R. 4257 updates and amends the activities required to secure federal information systems. It establishes 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, when possible, and through conducting regular threat assessments.

This bill gives responsibility to individual agencies required to adhere to FISMA standards. Each agency is made responsible for providing information security protections from a “risk based model” providing security from harms resulting from “unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by an agency.”¹¹ The head of each agency is also charged with designating a Chief Information Security Officer with the authority and primary responsibility to develop, implement and oversee an agency-wide information security program, to ensure and enforce compliance with the require-

⁹See, FISMA.

¹⁰Id.

¹¹Id.

ments imposed on the agency. Each agency head must ensure that the agency has a sufficient number of trained and cleared personnel to assist in complying with the statute. In ensuring an adequately trained workforce, agencies may utilize existing government cyberspace technical centers of excellence for purposes of training and certification attainment.

Under H.R. 4257, each agency is directed to develop, document, and implement an agency-wide information security program that includes a system that involves automated and continuous monitoring. Each agency is also directed to conduct vulnerability assessments and penetration tests commensurate with the risk posed to agency information systems.

Moreover, the legislation highlights the need for a stronger public/private relationship, by emphasizing the importance of commercially developed information security products to national security. The bill has received strong support from cybersecurity experts and industry.

Oversight hearings on cybersecurity

During this Congress, the House Oversight and Government Reform Committee has thoroughly examined a broad range of cybersecurity-related matters. On May 25, 2011, the Subcommittee on National Security, Homeland Defense, and Foreign Operations held a hearing entitled, “Cybersecurity: Assessing the Immediate Threat to the United States,” at which cyber-related intrusions and threats were broadly examined, and discussed as being among the greatest threats to our national security.

The full committee held a hearing on July 7, 2011, entitled, “Cybersecurity: Assessing the Nation’s Ability to Address the Growing Cyber Threat,” which examined cyberthreats and the importance of a well-coordinated strategic cybersecurity partnership with the private sector.

During its review of cybersecurity policies, the Committee placed great emphasis on obtaining input from non-government entities, which also confront significant cyber threats. According to experts, eighty-five to ninety percent of U.S. Government cyber traffic travels over non-government networks. Consequently, any policy initiatives must recognize the operating role of the private sector. Due to the potential impact of cyber attacks against government and non-government systems, private and public sectors must work together closely in addressing such threats.

Legislative history

On March 26, 2012, Chairman Issa introduced the “Federal Information Security Amendments Act of 2012” (H.R. 4257), with Ranking Member Cummings as original cosponsor. On April 18, 2012, the Committee marked up the bill, and it was ordered to be reported favorably to the House (as amended), by voice vote. Legislation that attempted to amend FISMA preceded H.R. 4257 during the 111th Congress. On March 22, 2010, Rep. Watson introduced the “Federal Information Security Amendments Act of 2010,” (H.R. 4900) which also intended to update FISMA. On May 5, 2010, Rep. Watson’s bill was ordered to be reported (as amended) by voice Vote by the House Oversight and Government Reform Committee. On May 6, 2012, Rep. Langevin (D-RI) introduced the “Executive

Cyberspace Authorities Act of 2010,” (H.R. 5247) which included amendments to FISMA and was referred to the House Oversight and Government Reform Committee. On May 28, 2010, the House passed the National Defense Authorization Act, which included an amendment, offered by Rep. Watson and Rep. Langevin, to update FISMA. The amendment in the NDAA, however, did not survive conference.

SECTION-BY-SECTION

Sec. 1. Short title

Sec. 1 states that the Act may be cited as the “Federal Information Security Amendments Act of 2012.”

Sec. 2. Coordination of Federal information policy

Sec. 2 amends chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, striking subchapters II and III and inserting the following new subchapter:

SUBCHAPTER II—INFORMATION SECURITY

Sec. 3551. Purposes

The purpose of this subchapter is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The subchapter recognizes the highly networked nature of the current Federal computing environment and provides effective government-wide 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. Additionally, the subchapter provides for the development and maintenance of minimum controls required to protect Federal information and information systems and establishes 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. The subchapter also recognizes the importance of commercially developed information security products to national security.

Sec. 3552. Definitions

This section defines the following terms for the purposes of this subchapter: adequate security, automated and continuous monitoring, incident, information systems, information security, information technology, national security system, information system, and threat assessment.

Sec. 3553. Authority and functions of the Director

Subsection 3553(a) authorizes the Director of the Office of Management and Budget to: (1) oversee the development and implementation of policies, principles, standards, and guidelines on information security; (2) require agencies 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 information collected or information systems; (3) coordinate 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; (4) oversee 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) review and approve or disapprove, agency information security programs required under section 3554(b); (6) coordinate information security policies and procedures with related information resources management policies and procedures; (7) oversee the operation of the Federal information security incident center required under section 3555; and (8) report to Congress on agency compliance with the requirements of this subchapter.

Subsection 3553(b) stipulates that, 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.

Subsection 3553(c) clarifies that: (1) certain authorities of the Director shall be delegated to the Secretary of Defense in the case of 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; and (2) certain authorities of the Director shall be delegated to the Director of Central Intelligence in the case of 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.

Sec. 3554. Agency responsibilities

Subsection 3554(a) directs the head of each agency to: (1) provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; (3) designate a Chief Information Security Officer with the authority and primary responsibility to develop, implement and oversee an agency-wide information security program to ensure and enforce compliance with the requirements imposed on the agency under this subchapter; (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 reports periodically, but not less than annually, to the agency head on the effectiveness of the agency information security program, along with information derived from automated and continuous monitoring, when possible, and threat assessments, including progress of remedial actions; (6) ensure that the Chief Information Security Officer possesses the necessary qualifications and the security clearance required to administer the functions described under this subchapter; and (7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Officer to implement, monitor, and hold senior agency officers accountable for the

implementation of appropriate security policies, procedures, and controls of agency components.

Subsection 3554(b) directs each agency to develop, document, and implement an agency-wide information security program that includes: (1) automated and continuous monitoring, when possible; (2) vulnerability assessments and penetration tests commensurate with the risk posed to agency information systems; (3) policies and procedures that cost effectively reduce information security risks and ensure compliance with the requirements of this subchapter and any other applicable policies, procedures and requirements; (4) automated and continuous monitoring, when possible for testing, and evaluation of the effectiveness and compliance of information security policies, procedures, and practices; (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) 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, to include notifying and, as appropriate, consulting with law enforcement agencies, relevant Offices of Inspectors General, and any other agency, office or entity; in accordance with the 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.

Subsection 3554(c) requires each agency to 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).

Sec. 3555. Federal information security incident center

Subsection 3555(a) directs the Director to ensure that the operation of a central Federal information security incident center: (1) provides timely technical assistance to operators of agency information systems regarding security incidents; (2) compiles and analyzes information about incidents that threaten information security; (3) informs operators of agency information systems about current and potential information security threats, and vulnerabilities; and (4) consults with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems regarding information security incidents and related matters.

Subsection 3555(b) directs agencies operating or exercising control of a national security system to 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.

Subsection 3555(c), directs the Director to review and approve the policies, procedures, and guidance established in this subchapter to ensure that the Federal information security incident center has the capability to detect, correlate, respond to, contain, mitigate, and remediate incidents that impair the adequate security of the information systems of more than one agency.

Sec. 3556. National security systems

Section 3556 makes responsible the head of each agency operating or exercising control of a national security system to ensure 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; and (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.

Sec. 3. Technical and conforming amendments

Section 3 amends the table of sections for chapter 35 of title 44, United States Code and amends other references.

Sec. 4. Effective date

Section 4 directs that this Act (including the amendments made by this Act) shall take effect 30 days after the date of the enactment of this Act.

EXPLANATION OF AMENDMENTS

The provisions of the Amendment in the Nature of a Substitute, offered by Rep. Jason Chaffetz, are explained in the Section-by-Section portion of this report.

COMMITTEE CONSIDERATION

On April 18, 2012, the Committee met in open session and ordered reported favorably the bill, H.R. 4257, as amended, by voice vote, a quorum being present.

CORRESPONDENCE

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (201) 225-5874
 FREEDOM (201) 225-2974
 MINORITY (202) 225-9051
<http://oversight.house.gov>

April 25, 2012

DARRELL E. ISSA, CALIFORNIA
 CHAIRMAN

DAN DURTON, INDIANA
 JOHN L. MICA, FLORIDA
 TODD RUSSELL PLATTIS, PENNSYLVANIA
 MICHAEL R. TURNER, OHIO
 PATRICK MCHENRY, NORTH CAROLINA
 JIM JORDAN, OHIO
 JASON CHAFFETZ, UTAH
 CONNIE MACK, FLORIDA
 TIM WALBERG, MICHIGAN
 JAMES LANKFORD, OKLAHOMA
 JUSTIN AMASH, MICHIGAN
 ANN MARIE BUEKLE, NEW YORK
 PAUL A. GOSAR, D.D.S., ARIZONA
 RAUL R. LABRADOR, IDAHO
 PATRICK MEEHAN, PENNSYLVANIA
 SCOTT DEJARLAIS, M.D., TENNESSEE
 JOE WALSH, ILLINOIS
 TREY GOWDY, SOUTH CAROLINA
 DENNIS A. ROSS, FLORIDA
 FRANK C. QUINTA, NEW HAMPSHIRE
 BLAKE FARENTHOLD, TEXAS
 MIKE KELLY, PENNSYLVANIA

LAWRENCE J. BRADY
 STAFF DIRECTOR

ELIJAH E. CUMMINGS, MARYLAND
 RANKING MINORITY MEMBER

BOBPHUS TOWNS, NEW YORK
 CAROLYN B. MALONEY, NEW YORK
 ELEANOR HOLMES NORTON,
 DISTRICT OF COLUMBIA
 DENNIS J. KUCINICH, OHIO
 JOHN F. TIERNEY, MASSACHUSETTS
 WM. LACY CLAY, MISSOURI
 STEPHEN F. LYNCH, MASSACHUSETTS
 JIM COOPER, TENNESSEE
 GERALD E. CONNOLLY, VIRGINIA
 MIKE GUGLEY, ILLINOIS
 DANNY K. DAVIS, ILLINOIS
 BRUCE L. BRALEY, IOWA
 PETER WELCH, VERMONT
 JOHN A. YARMUTH, KENTUCKY
 CHRISTOPHER S. MURPHY, CONNECTICUT
 JACKIE SPIER, CALIFORNIA

The Honorable Ralph M. Hall
 Chairman
 Committee on Science, Space, and Technology
 U.S. House of Representatives
 Washington, D.C. 20515

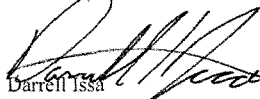
Dear Mr. Chairman:

Thank you for your letter regarding the Committee on Science, Space, and Technology's jurisdictional interest in H.R. 4257, the Federal Information Security Amendments Act of 2012, and your willingness to forego consideration of H.R. 4257 by your committee.

I agree that the Committee on Science, Space, and Technology has a valid jurisdictional interest in certain provisions of H.R. 4257 and that the Committee's jurisdiction will not be adversely affected by your decision not to request a sequential referral of H.R. 4257. 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

cc: The Honorable John A. Boehner, Speaker

The Honorable Eddie Bernice Johnson, Ranking Minority Member
 Committee on Science, Space, and Technology

The Honorable Elijah E. Cummings, Ranking Minority Member
 Committee on Oversight and Government Reform

Mr. Tom Wickham, Parliamentarian

RALPH M. HALL, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

April 26, 2012

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Issa:

I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 4257, the Federal Information Security Amendments Act of 2012.

As you know the staffs on our Committees have worked together to execute improvements to the legislation and I ask your assurances that the jurisdictional interests of the Committee on Science, Space, and Technology be protected and kept in mind as the bill proceeds. I would ask for your continuing cooperation in addressing remaining issues to our mutual satisfaction.

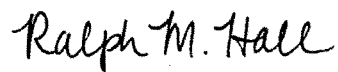
I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, 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. 4257, as well as any similar or related legislation.

I ask that a copy of this letter be placed 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 H.R. 4257's enactment.

Sincerely,

A handwritten signature in black ink that reads "Ralph M. Hall". The signature is written in a cursive, slightly slanted style.

Ralph M. Hall
Chairman
Committee on Science, Space, and Technology

cc: The Hon. John Boehner, Speaker,
The Hon. Eric Cantor, Majority Leader
The Hon. Eddie Bernice Johnson, Ranking Member, Committee on Science,
Space, and Technology
The Hon. Elijah Cummings, Ranking Member, Committee on Oversight and
Government Reform
Mr. Thomas J. Wickham, Jr., Parliamentarian

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Section 102(b)(3) of Public Law 104–1 requires a description of the application of this bill to the legislative branch where the bill relates to the terms and conditions of employment or access to public services and accommodations. This bill enhances the Federal Information Security Management Act (FISMA) of 2002 by improving the framework for securing federal information technology systems. As such this bill does not relate to employment or access to public services and accommodations.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goals and objectives are reflected in the descriptive portions of this report.

FEDERAL ADVISORY COMMITTEE ACT

The Committee finds that the legislation does not establish or authorize the establishment of an advisory committee within the definition of 5 U.S.C. App., Section 5(b).

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandate Reform Act, P.L. 104–4) requires a statement as to whether the provisions of the reported include unfunded mandates. In compliance with this requirement the Committee has received a letter from the Congressional Budget Office included herein.

EARMARK IDENTIFICATION

H.R. 4257 does not include any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.

COMMITTEE ESTIMATE

Clause 3(d)(2) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison by the Committee of the costs that would be incurred in carrying out H.R. 4257. However, clause 3(d)(3)(B) of that rule provides that this requirement does not apply when the Committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST
ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 4257 from the Director of Congressional Budget Office:

APRIL 20, 2012.

Hon. DARRELL ISSA,
*Chairman, Committee on Oversight and Government Reform,
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4257, the Federal Information Security Amendments Act of 2012.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 4257—Federal Information Security Amendments Act of 2012

Summary: H.R. 4257 would amend the Federal Information Security Management Act of 2002 (FISMA) to improve the security of federal information technology systems. The legislation would require continuous monitoring of computer systems and provide the Office of Management and Budget (OMB) and federal agencies with specific new responsibilities to secure federal information systems.

Based on information from the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and other major agencies working to ensure the security of federal information systems, CBO estimates that implementing H.R. 4257 would cost \$710 million over the 2013–2017 period, assuming appropriation of the necessary amounts. Most of those funds would be spent on salaries, expenses, and computer hardware and software. Enacting the bill would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

H.R. 4257 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4257 is shown in the following table. The costs of this legislation fall within budget functions 800 (general government) and all other budget functions that include spending for computer information systems.

	By fiscal year, in millions of dollars—					
	2013	2014	2015	2016	2017	2013– 2017
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	70	120	150	200	220	760
Estimated Outlays	50	110	145	190	215	710

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted in fiscal year 2012, that the necessary amounts will be appropriated each year, and that spending will follow historical patterns for salaries and expenses related to securing federal information systems.

FISMA sets forth a comprehensive framework for ensuring that security controls for information resources that support federal operations and assets are effective. Specifically, FISMA requires the head of each federal agency to provide protections commensurate with the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information and systems used or operated by that agency. OMB reports that in 2011, 24 federal agencies (all agencies that have appointed Chief Financial Officers), spent more than \$13 billion on security for information technology. That security spending accounts for about 18 percent of all federal spending on information technology and includes spending for testing, training, equipment, and personnel costs. Inspector General reviews of federal agencies report that less than half of the agencies have implemented adequate continuous monitoring operations of their computer systems and about half have unresolved security problems involving alternative computer processing sites, contingency planning for emergencies, and adequate backup of computer information.

H.R. 4257 would expand the requirements in FISMA to strengthen and coordinate security controls for computer systems across federal agencies. Some of those new requirements include establishing uniform standards across agencies' information systems, implementing automated and continuous monitoring of systems to secure information, conducting threat assessments, and maintaining secure facilities. Based on information from OMB, the Department of Homeland Security and other agencies, CBO estimates that when fully implemented, the new activities specified in H.R. 4257 would add about 2 percent—roughly \$200 million a year—to the annual cost of implementing FISMA. CBO expects that it would take about four years to reach that level of effort for the thousands of federal computer systems currently operating. Over the 2013–2017 period, we estimate that implementing those additional requirements and authorities would cost about \$710 million, assuming appropriation of the necessary amounts.

Pay-As-You-Go Considerations: None.

Intergovernmental and private-sector impact: H.R. 4257 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Estimate prepared by: Federal Costs: Matthew Pickford; Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omit-

ted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

* * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * *

[SUBCHAPTER II—INFORMATION SECURITY

[Sec.
3531. Purposes
3532. Definitions.
3533. Authority and functions of the Director.
3534. Federal agency responsibilities.
3535. Annual independent evaluation.
3536. National security systems.
3537. Authorization of appropriations.
3538. Effect on existing law.

[SUBCHAPTER III—INFORMATION SECURITY

[Sec.
3541. Purposes.
3542. Definitions.
3542. Authority and functions of the Director.
3544. Federal agency responsibilities.
3545. Annual independent evaluation.
3546. Federal information security incident center.
3547. National security systems.
3548. Authorization of appropriations.
3549. Effect on existing law.]

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.

* * * * *

[SUBCHAPTER II—INFORMATION SECURITY

[§ 3531. 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;

[(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;

[(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 infrastructures 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.

[§ 3532. Definitions

[(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

[(b) ADDITIONAL DEFINITIONS.—As used in this subchapter—

[(1) 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;

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

[(D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access;

[(2) 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, the function, operation, or use of which—

[(A) involves intelligence activities;

[(B) involves cryptologic activities related to national security;

[(C) involves command and control of military forces;

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

[(E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

[(3) the term “information technology” has the meaning given that term in section 11101 of title 40; and

[(4) the term “information system” means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange,

transmission, or reception of data or 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.

[(§ 3533. Authority and functions of the Director

[(a) The Director shall oversee agency information security policies and practices, by—

[(1) promulgating information security standards under section 11331 of title 40;

[(2) overseeing the implementation of policies, principles, standards, and guidelines on information security;

[(3) 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;

[(4) 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;

[(5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303(b)(5) of title 40, to enforce accountability for compliance with such requirements;

[(6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);

[(7) coordinating information security policies and procedures with related information resources management policies and procedures; and

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

[(A) a summary of the findings of evaluations required by section 3535;

[(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)(9) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

[(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

[§ 3534. Federal agency responsibilities

[(a) 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 promulgated by the Director under section 11331 of title 40; and

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

[(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

[(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 systems;

[(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40 for information security classifications and related requirements;

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

[(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

[(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

[(A) designating a senior agency information security officer who shall—

[(i) carry out the Chief Information Officer's responsibilities under this section;

[(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

[(iii) have information security duties as that official's primary duty; and

[(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

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

[(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and 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 trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

[(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

[(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(a)(5), 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) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

[(2) policies and procedures that—

[(A) are based on the risk assessments required by paragraph (1);

[(B) cost-effectively reduce information security risks to an acceptable level;

[(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

[(D) 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 under section 11331 of title 40;

[(iii) minimally acceptable system configuration requirements, as determined by the agency; and

[(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

[(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

[(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

[(A) information security risks associated with their activities; and

[(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

[(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

[(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

[(B) may include testing relied on in a evaluation under section 3535;

[(6) 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;

[(7) procedures for detecting, reporting, and responding to security incidents, including—

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

[(B) notifying and consulting with, as appropriate—

[(i) law enforcement agencies and relevant Offices of Inspector General;

[(ii) an office designated by the President for any incident involving a national security system; and

[(iii) any other agency or office, in accordance with law or as directed by the President; and

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

[(c) Each agency shall—

[(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General 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);

[(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 under subchapter 1 of this chapter;

[(C) information technology management under subtitle III of title 40;

[(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) (and the amendments made by that Act);

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

[(G) internal accounting and administrative controls under section 3512 of title 31, United States Code, (known as the “Federal Managers Financial Integrity Act”); 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 (31 U.S.C. 3512 note).

[(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

[(A) the time periods; and

[(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

[(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

[(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

§ 3535. Annual independent evaluation

[(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

[(2) Each evaluation by an agency under this section shall include—

[(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;

[(B) an assessment (made on the basis of the results of the testing) of compliance with—

[(i) the requirements of this subchapter; and

[(ii) related information security policies, procedures, standards, and guidelines; and

[(C) separate presentations, as appropriate, regarding information security relating to national security systems.

[(b) Subject to subsection (c)—

[(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

[(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

[(c) For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

[(1) only by an entity designated by the agency head; and

[(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(d) The evaluation required by this section—

[(1) shall be performed in accordance with generally accepted government auditing standards; and

[(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

[(e) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

[(f) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

[(g)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(a)(8).

[(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

[(h) The Comptroller General shall periodically evaluate and report to Congress on—

[(1) the adequacy and effectiveness of agency information security policies and practices; and

[(2) implementation of the requirements of this subchapter.

[§ 3536. Expiration

[This subchapter shall not be in effect after May 31, 2003.]

[§ 3537. Authorization of appropriations

[There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.]

[§ 3538. Effect on existing law

[Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to Congress or the Comptroller General of the United States.]

[SUBCHAPTER III—INFORMATION SECURITY**[§ 3541. 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;

[(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;

[(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 infrastructures 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.]

§ 3542. Definitions

[(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

[(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

[(1) 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.

[(2)(A) 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) 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).

[(3) The term “information technology” has the meaning given that term in section 11101 of title 40.

§ 3542. 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 3544(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 3546; and

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

[(A) a summary of the findings of evaluations required by section 3545;

[(B) 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;

[(C) significant deficiencies in agency information security practices;

[(D) planned remedial action to address such deficiencies; and

[(E) 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.

§ 3544. Federal 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 promulgated under section 11331 of title 40; and

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

[(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

[(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 systems;

[(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

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

[(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

[(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

[(A) designating a senior agency information security officer who shall—

[(i) carry out the Chief Information Officer's responsibilities under this section;

[(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

[(iii) have information security duties as that official's primary duty; and

[(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

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

[(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3542 of this title, and 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 trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

[(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

[(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3542(a)(5), 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) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

[(2) policies and procedures that—

[(A) are based on the risk assessments required by paragraph (1);

- [(B) cost-effectively reduce information security risks to an acceptable level;
- [(C) ensure that information security is addressed throughout the life cycle of each agency information system; and
- [(D) 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 under section 11331 of title 40;
 - [(iii) minimally acceptable system configuration requirements, as determined by the agency; and
 - [(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;
- [(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- [(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
 - [(A) information security risks associated with their activities; and
 - [(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- [(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
 - [(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and
 - [(B) may include testing relied on in a evaluation under section 3545;
- [(6) 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;
- [(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—
 - [(A) mitigating risks associated with such incidents before substantial damage is done;
 - [(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and
 - [(C) notifying and consulting with, as appropriate—
 - [(i) law enforcement agencies and relevant Offices of Inspector General;
 - [(ii) an office designated by the President for any incident involving a national security system; and
 - [(iii) any other agency or office, in accordance with law or as directed by the President; and

[(8) 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) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General 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);

[(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 under subchapter 1 of this chapter;

[(C) information technology management under subtitle III of title 40;

[(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) (and the amendments made by that Act);

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

[(G) internal accounting and administrative controls under section 3512 of title 31, (known as the “Federal Managers Financial Integrity Act”); 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 (31 U.S.C. 3512 note).

[(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

[(A) the time periods, and

[(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

[(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

[(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent

that such policies and procedures affect communication with the public.

§ 3545. Annual independent evaluation

[(a) IN GENERAL.—(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

[(2) Each evaluation under this section shall include—

[(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

[(B) an assessment (made on the basis of the results of the testing) of compliance with—

[(i) the requirements of this subchapter; and

[(ii) related information security policies, procedures, standards, and guidelines; and

[(C) separate presentations, as appropriate, regarding information security relating to national security systems.

[(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

[(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

[(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

[(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

[(1) only by an entity designated by the agency head; and

[(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

[(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

[(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

[(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

[(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3542(a)(8).

[(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

[(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

[(1) the adequacy and effectiveness of agency information security policies and practices; and

[(2) implementation of the requirements of this subchapter.

[(§ 3546. 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.

[(§ 3547. 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.

[§ 3548. Authorization of appropriations

[There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

[§ 3549. Effect on existing law

[Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.]

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 Government-wide 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 in-

dividual 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 con-

tractor 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 sub-

chapter 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.

* * * * *

HOMELAND SECURITY ACT OF 2002

* * * * *

TITLE X—INFORMATION SECURITY

SEC. 1001. INFORMATION SECURITY.

(a) * * *

* * * * *

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by [section 3532(3)] *section 3552(b)* of title 44, United States Code.

* * * * *

TITLE 10, UNITED STATES CODE

SUBTITLE A—GENERAL MILITARY LAW

* * * * *

PART IV—SERVICE, SUPPLY, AND PROCUREMENT

* * * * *

CHAPTER 131—PLANNING AND COORDINATION

* * * * *

§ 2222. Defense business systems: architecture, accountability, and modernization

(a) * * *

* * * * *

(j) DEFINITIONS.—In this section:

(1) * * *

* * * * *

(5) The term “national security system” has the meaning given that term in [section 3542(b)(2)] *section 3552(b)* of title 44.

§ 2223. Information technology: additional responsibilities of Chief Information Officers

(a) * * *

* * * * *

(c) DEFINITIONS.—In this section:

(1) * * *

* * * * *

(3) The term “national security system” has the meaning given that term by [section 3542(b)(2)] *section 3552(b)* of title 44.

* * * * *

CHAPTER 137—PROCUREMENT GENERALLY

* * * * *

§ 2315. Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes

For purposes of subtitle III of title 40, the term “national security system”, with respect to a telecommunications and information system operated by the Department of Defense, has the meaning given that term by [section 3542(b)(2)] *section 3552(b)* of title 44.

* * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * *

SEC. 20. (a) The Institute shall—

(1) * * *

(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in [section 3532(b)(2)] *section 3552(b)* of title 44, United States Code);

* * * * *

(e) As used in this section—

(1) * * *

(2) the term “information security” has the same meaning as provided in [section 3532(1)] *section 3552(b)* of such title;

* * * * *

(5) the term “national security system” has the same meaning as provided in [section 3532(b)(2)] *section 3552(b)* of such title.

* * * * *

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

* * * * *

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) * * *

* * * * *

(d) FEDERAL AGENCY INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—In developing the agencywide information security program required by [section 3534(b)] *section 3554(b)* of title 44, United States Code, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) * * *

* * * * *

ADDITIONAL VIEWS

During the last Congress the Oversight Committee held several hearings on the Federal Information Security Management Act (FISMA) which showed agencies have focused more on compliance than on cybersecurity. H.R. 4257 responds to that problem by emphasizing continuous monitoring of cyber threats rather than compliance measures such as mere attendance at an employee training. In that sense H.R. 4257 is similar to legislation which passed the House in 2010, but H.R. 4257 has a narrower scope. It does not address the Executive Branch organization of positions related to technology and cybersecurity: the Chief Technology Officer (CTO), Chief Information Officer (CIO), and Cybersecurity Coordinator. While this Administration has provided a laudable focus on technology policy and made strategic appointments for these positions, Congress needs to provide a statutory framework to ensure that these positions function efficiently and harmoniously in future administrations. To that end, the Watson-Langevin FISMA Amendments Act of 2010 included language addressing the relationship of the CTO and other positions. H.R. 4257 does not yet address Executive Branch organization, and while I support H.R. 4257's language to improve cybersecurity I also believe that implementation of new cybersecurity performance standards will be far more effective if it includes language on technology positions within the Executive Branch. To that end, Chairman Issa and I agreed in a colloquy during the markup to address Executive Branch organization through additional legislation in coordination with Mr. Langevin.

GERALD E. CONNOLLY.

○