[DISCUSSION DRAFT]

MARCH 22, 2012

112TH CONGRESS
2D SESSION

H. R. _____

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. ISSA introduced the following bill; which was referred to the Committee on _____

A BILL

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Federal Information Security Amendments Act of 2012''.

SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

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

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are to—

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

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

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

''(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 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.

''§ 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) The term 'adequate security' means security that complies with the regulations and standards promulgated under section 11331 of title 40.

''(2) 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) The term 'incident' means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, information infrastructure, 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) The term 'information infrastructure' means the underlying framework that information systems and assets rely on in processing, storing, or transmitting information electronically.

''(5) The term 'information security' means protecting information and information infrastructure 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 using digital credentials to assure the identity of users and validate access of such users.

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

''(7)(A) The term 'national security system' means any information infrastructure (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).

''(8) The term 'information system' means any equipment or interconnected system or subsystem 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.

''(9) The term 'threat assessment' means the real time or near real time process of formally evaluating the degree of threat to an information system or information technology enterprise and describing the nature of the threat.

"§ 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 11331and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm result-

ing 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 infor-

mation 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 infrastructure 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 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);

"(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 infrastructure 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 infrastructure;

''(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) periodically, and to the extent practicable, continuously testing and evaluating information security controls and techniques to ensure that such controls and techniques are effectively implemented and operated; and

''(E) periodically, and to the extent practicable, continuously conducting threat assessments by monitoring information infrastructure, 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 can—

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

''(ii) monitor and, on a risk-based basis, mitigate the vulnerabilities of every information system within the agency information infrastructure;

''(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 the risk-based security of such information and information systems;

''(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 appropriate security operations center and 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 and threat assessments; and

''(C) the progress of remedial actions;

''(6) ensure that the Chief Information Security Officer possesses the necessary qualifications, including education, professional certifications, 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;

''(7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Of-

ficer 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; and

''(8) delegate to agency officials who are responsible for particular agency systems or subsystems the responsibility to ensure and enforce compliance with all requirements of the agency's information security program in consultation with the Chief Information Security Officer designated under paragraph (3).

''(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 infrastructure 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—

''(A) 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 informa-

tion systems that support the operations and assets of the agency; and

''(B) that assesses whether information or information systems should be removed or migrated to more secure networks or standards and make recommendations to the head of the agency and the Director based on that assessment;

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

''(3) policies and procedures that—

''(A) mitigate and, to the extent practicable, remediate information security vulnerabilities based on the risk posed to the agency;

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

''(C) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director, and infor-

mation 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;

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

"(III) the Chief Information Officers Council recommended approaches;

"(D) 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

"(E) ensure the oversight and training of personnel with significant responsibilities for in-

formation security with respect to such responsibilities;

''(4) on the basis of risk, automated and continuous monitoring for testing, and evaluation of the effectiveness and compliance of information security policies, procedures, and practices, including—

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

''(B) management, operational, and technical 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) to the extent practicable, automated and continuous monitoring for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued by the Director, including—

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

''(B) notifying and consulting with the appropriate security operations response center; 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 infrastructure 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 and information infrastructure 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 and information infrastructure 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 and information infrastructure 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)(6) 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.