I

111TH CONGRESS
2D SESSION

H. R. 4900

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 22, 2010

Ms. WATSON introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

A BILL

To amend chapter 35 of title 44, United States Code, to create the National Office for Cyberspace, 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.

(a) SHORT TITLE.—This Act may be cited as the ''Federal Information Security Amendments Act of 2010''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

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;

''(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.

''§ 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 promulgated under section 3554 and the standards promulgated under section 3558.

''(2) 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.

''(3) The term 'information infrastructure' means the underlying framework that information systems and assets rely on in processing, storing, or transmitting information electronically.

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

''(6)(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).

''§ 3553. National Office for Cyberspace

''(a) ESTABLISHMENT.—There is established within the Executive Office of the President an office to be known as the National Office for Cyberspace.

''(b) DIRECTOR.—There shall be at the head of the Office a Director, who shall be appointed by the President by and with the advice and consent of the Senate. The Director of the National Office for Cyberspace shall administer all functions under this subchapter and collaborate to the extent practicable with the heads of appropriate agencies, the private sector, and international partners. The Office shall serve as the principal office for coordinating issues relating to achieving an assured, reliable,

secure, and survivable information infrastructure and related capabilities for the Federal Government.

"§ 3554. Federal Cybersecurity Practice Board

''(a) ESTABLISHMENT.—Within the National Office for Cyberspace, there shall be established a board to be known as the 'Federal Cybersecurity Practice Board' (in this section referred to as the 'Board').

''(b) MEMBERS.—The Board shall be chaired by the Director of the National Office for Cyberspace and consist of at least one representative from—

''(1) the Office of Management and Budget;

''(2) civilian agencies;

''(3) the Department of Defense;

''(4) the law enforcement community; and

''(5) such additional military and civilian agencies as the Director considers appropriate.

''(c) RESPONSIBILITIES.—

''(1) DEVELOPMENT OF POLICIES AND PROCEDURES.—Subject to the authority, direction, and control of the Director of the National Office for Cyberspace, the Board shall be responsible for developing and periodically updating information security policies and procedures relating to the matters described in paragraph (2). In developing such policies and procedures, the Board shall require that all

matters addressed in the policies and procedures are consistent, to the maximum extent practicable and in accordance with applicable law, among the civilian, military, intelligence, and law enforcement communities.

''(2) SPECIFIC MATTERS COVERED IN POLICIES AND PROCEDURES.—

''(A) MINIMUM SECURITY CONTROLS.—The Board shall be responsible for developing and periodically updating information security policies and procedures relating to minimum security controls for information technology, in order to—

''(i) provide Governmentwide protection of Government-networked computers against common attacks; and

''(ii) provide agencywide protection against threats, vulnerabilities, and other risks to the information infrastructure within individual agencies.

''(B) MEASURES OF EFFECTIVENESS.—The Board shall be responsible for developing and periodically updating information security policies and procedures relating to measurements needed to assess the effectiveness of the

minimum security controls referred to in subparagraph (A). Such measurements shall include a risk scoring system to evaluate risk to information security both Governmentwide and within contractors of the Federal Government.

"(C) PRODUCTS AND SERVICES.—The Board shall be responsible for developing and periodically updating information security policies and procedures relating to criteria for products and services to be used in agency information systems and agency information infrastructure that will meet the minimum security controls referred to in subparagraph (A). In carrying out this subparagraph, the Board shall, in consultation with the Office of Management and Budget and the General Services Administration—

"(i) develop a list, set forth in order of priority, of technologies that agencies can use to automate security functions; and

"(ii) define minimum standards for secure development of software products and services.

''(D) REMEDIES.—The Board shall be responsible for developing and periodically updating information security policies and procedures relating to methods for providing remedies for security deficiencies identified in agency information systems.

''(3) RELATIONSHIP TO OTHER STANDARDS.—The policies and procedures developed under paragraph (1) are supplemental to the standards promulgated by the Director of the National Office for Cyberspace under section 3558.

''(4) RECOMMENDATIONS FOR REGULATIONS.—The Board shall be responsible for making recommendations to the Director of the National Office for Cyberspace on regulations to carry out the policies and procedures developed by the Board under paragraph (1).

''(d) REGULATIONS.—The Director of the National Office for Cyberspace, in consultation with the Director of the Office of Management and the Administrator of General Services, shall promulgate and periodically update regulations to carry out the policies and procedures developed by the Board under subsection (c).

''(e) ANNUAL REPORT.—The Director of the National Office for Cyberspace shall provide to Congress a

report containing a summary of agency progress in implementing the regulations promulgated under this section as part of the annual report to Congress required under section 3555(a)(8).

''(f) EXEMPTION FROM DISCLOSURE.—Information regarding threats, vulnerabilities, and risks submitted by agencies to the Board shall be exempt from disclosure under section 552 of title 5.

''§ 3555. Authority and functions of the Director of the National Office for Cyberspace

''(a) IN GENERAL.—The Director of the National Office for Cyberspace 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 3558;

''(2) requiring agencies, consistent with the standards promulgated under section 3558 and other 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 3556(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 3559; 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 audits required by section 3557;

''(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 3558;

''(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 of the National Office for Cyberspace 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 of the National Office for Cyberspace 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 of the National Office for Cyberspace 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.

"§ 3556. 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) the regulations promulgated under section 3554 and the information security standards promulgated under section 3558;

"(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 under the agency head are complementary and uniform, to the extent practicable; 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

regulations promulgated under section 3554 and standards promulgated under section 3558, for information security classifications and related requirements;

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

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

''(3) delegate to an agency official designated to oversee agency information security the authority 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 on an automated and continuous basis that can—

''(i) assess the state of compliance of all networks and systems with prescribed controls issued pursuant to section 3558 and report immediately any variance therefrom and, where appropriate, shut down

systems that are found to be non-compliant;

''(ii) detect, report, respond to, contain, and mitigate incidents that impair adequate security of the information and information infrastructure, in accordance with policy provided by the Director of the National Office for Cyberspace, in consultation with the Chief Information Officers Council, and guidance from the National Institute of Standards and Technology;

''(iii) collaborate with the National Office for Cyberspace and appropriate public and private sector security operations centers to address incidents that impact the security of information and information infrastructure that extend beyond the control of the agency; and

''(iv) not later than 24 hours after discovery of any incident described under subparagraph (A (ii)), unless otherwise directed by policy of the National Office for Cyberspace, provide notice to the appropriate security operations center, the Na-

tional Cyber Investigative Joint Task Force, and inspector general;

''(B) developing, maintaining, and overseeing an agency wide 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 sections 3555 and 3558;

''(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 and cleared personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

''(5) ensure that the agency official designated to oversee agency information security, in coordination with other senior agency officials, reports bian-

nually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions; and

''(6) ensure that the agency official designated to oversee agency information security possesses 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.

''(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director of the National Office for Cyberspace under section 3555(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) continuous automated monitoring of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency to assure conformance with regulations promulgated under section 3554 and standards promulgated under section 3558;

''(2) penetration tests commensurate with risk (as defined by the National Institute of Standards and Technology and the National Office for Cyberspace) for agency information systems;

''(3) information security vulnerabilities are mitigated based on the risk posed to the agency;

''(4) policies and procedures that—

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

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

''(C) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director of the National Office for Cyberspace, and information security standards promulgated under section 3558;

''(iii) minimally acceptable system configuration requirements, as determined by the Director of the National Office for Cyberspace; 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; of how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

''(I) the policy of the Director of the National Office for Cyberspace;

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

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

''(D) developing, maintaining, and overseeing an agency wide information security program as required by subsection (b);

''(E) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under sections 3555 and 3558;

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

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

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

''(6) ensure that the agency official designated to oversee agency information security, in coordination with other senior agency officials, reports biannually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions; and

''(7) ensure that the agency official designated to oversee agency information security possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and has informa-

tion security duties as the primary duty of that official.

''(8) to the extent practicable, automated and continuous technical 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(b); and

''(B) management, operational, and technical controls relied on for an evaluation under section 3556;

''(9) 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;

''(10) to the extent practicable, continuous technical monitoring for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued by the Director of the National Office for Cyberspace, 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;

''(ii) the National Office for Cyberspace; and

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

''(11) 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 National Office for Cyberspace;

''(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) (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; 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 National Office for Cyberspace, 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) and operational evaluations required under section 3553(d).

''(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.

''§ 3557. Annual independent audit

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

''(2) Each audit under this section shall include—

''(A) testing of the effectiveness of the information systems of the agency for automated, continuous monitoring of the state of compliance of its information systems with regulations promulgated under section 3554 and standards promulgated under section 3558 in a representative subset of—

''(i) the information systems used or operated by the agency; and

''(ii) the information systems used, operated, or supported on behalf of the agency by a contractor of the agency, a subcontractor (at

any tier) of such contractor, or any other entity;

''(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;

''(C) separate presentations, as appropriate, regarding information security relating to national security systems; and

''(D) a conclusion regarding whether the information security controls of the agency are effective, including an identification of any significant deficiencies in such controls.

''(3) Each audit under this section shall be performed in accordance with applicable generally accepted Government auditing standards.

''(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 audit 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 audit.

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

''(1) only by an entity designated 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 AUDITS.—The audit required by this section may be based in whole or in part on another audit relating to programs or practices of the applicable agency.

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

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

''(f) PROTECTION OF INFORMATION.—Agencies and auditors 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 of the National Office for Cyberspace shall summarize the results of the audits conducted under this section in the annual report to Congress required under section 3555(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) Audits 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.

''(i) CONTRACTOR AUDITS.—Each year each contractor that operates, uses, or supports an information system by or on behalf of an agency and each subcontractor of such contractor—

''(1) shall conduct an audit using an independent external auditor, as determined by the Comptroller General, in accordance with subsection (a), including an assessment of compliance with the applicable requirements of this subchapter; and

''(2) shall submit the results of such audit to such agency not later than such date established by the Agency.

''§ 3558. Responsibilities for Federal information systems standards

''(a) REQUIREMENT TO PRESCRIBE STANDARDS.—

''(1) IN GENERAL.—

''(A) REQUIREMENT.—Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

''(B) REQUIRED STANDARDS.—Standards promulgated under subparagraph (A) shall include—

''(i) standards that provide minimum information security requirements as determined under section 20(b) of the National

Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

''(C) REQUIRED STANDARDS BINDING.—Information security standards described under subparagraph (B) shall be compulsory and binding.

''(2) STANDARDS AND GUIDELINES FOR NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems, as defined under section 3552(b), shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director of the Office of Management and Budget under this section, if such standards—

''(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

''(2) are otherwise consistent with policies and guidelines issued under section 3555.

''(c) REQUIREMENTS REGARDING DECISIONS BY DIRECTOR.—

''(1) DEADLINE.—The decision regarding the promulgation of any standard by the Director of the Office of Management and Budget under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(2) NOTICE AND COMMENT.—A decision by the Director of the Office of Management and Budget to significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), shall be made after the public is given an oppor-

tunity to comment on the Director's proposed decision.

"§ 3559. Federal information security incident center

''(a) IN GENERAL.—The Director of the National Office for Cyberspace 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 in-

cidents, 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.—In coordination with the Administrator for Electronic Government and Information Technology, the Director of the National Office for Cyberspace 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, and mitigate 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.

''§ 3560. 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. INFORMATION SECURITY ACQUISITION REQUIREMENTS.

(a) IN GENERAL.—Chapter 113 of title 40, United States Code, is amended by adding at the end of subchapter II the following new section:

''§ 11319. Information security acquisition requirements.

''(a) PROHIBITION.—Notwithstanding any other provision of law, beginning one year after the date of the enactment of the Federal Information Security Amendments Act of 2010, no agency may enter into a contract, an order under a contract, or an interagency agreement for—

''(1) the collection, use, management, storage, or dissemination of information on behalf of the agency;

''(2) the use or operation of an information system on behalf of the agency; or

''(3) information technology;

unless such contract, order, or agreement includes requirements to provide effective information security that supports the operations and assets under the control of the agency, in compliance with the policies, standards, and guidance developed under subsection (b), and otherwise ensures compliance with this section.

''(b) COORDINATION OF SECURE ACQUISITION POLICIES.—

''(1) IN GENERAL.—The Director, in consultation with the Director of the National Institute of Standards and Technology, the Director of the National Office for Cyberspace, and the Administrator of General Services, shall oversee the development and implementation of policies, standards, and guidance, including through revisions to the Federal Acquisition Regulation and the Department of Defense supplement to the Federal Acquisition Regulation, to cost effectively enhance agency information security, including—

''(A) minimum information security requirements for agency procurement of commercial off-the-shelf information technology and other products and services; and

''(B) approaches for evaluating and mitigating significant supply chain security risks

associated with products or services to be acquired by agencies.

''(2) REPORT.—Not later than two years after the date of the enactment of the Federal Information Security Amendments Act of 2010, the Director shall submit to Congress a report describing—

''(A) actions taken to improve the information security associated with the procurement of products and services by the Federal Government; and

''(B) plans for overseeing and coordinating efforts of agencies to use best practice approaches for cost-effectively purchasing more secure products and services.

''(c) VULNERABILITY ASSESSMENTS OF MAJOR SYSTEMS.—

''(1) REQUIREMENT FOR INITIAL VULNERABILITY ASSESSMENTS.—The Director shall require each agency to conduct an initial vulnerability assessment for any major system and its significant items of supply prior to its development. The initial vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach to—

''(A) identify vulnerabilities;

''(B) define exploitation potential;

''(C) examine the system's potential effectiveness;

''(D) determine overall vulnerability; and

''(E) make recommendations for risk reduction.

''(2) SUBSEQUENT VULNERABILITY ASSESSMENTS.—

''(A) The Director shall require, if the Director determines that a change in circumstances warrants the issuance of a subsequent vulnerability assessment, a subsequent vulnerability assessment of each major system and its significant items of supply within the program.

''(B) Upon the request of a congressional committee, the Director may require a subsequent vulnerability assessment of a particular major system and its significant items of supply within the program.

''(C) Any subsequent vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach and, if applicable, a testing-based approach, to monitor the exploitation po-

tential of such system and reexamine the factors described in subparagraphs (A) through (E) of paragraph (1).

''(3) CONGRESSIONAL OVERSIGHT.—The Director shall provide to the appropriate congressional committees a copy of each vulnerability assessment conducted under paragraph (1) or (2) not later than 10 days after the date of the completion of such assessment.

''(d) DEFINITIONS.—In this section:

''(1) ITEM OF SUPPLY.—The term 'item of supply'—

''(A) means any individual part, component, subassembly, assembly, or subsystem integral to a major system, and other property which may be replaced during the service life of the major system, including a spare part or replenishment part; and

''(B) does not include packaging or labeling associated with shipment or identification of an item.

''(2) VULNERABILITY ASSESSMENT.—The term 'vulnerability assessment' means the process of identifying and quantifying vulnerabilities in a major system and its significant items of supply.

''(3) MAJOR SYSTEM.—The term 'major system' has the meaning given that term in section 4 of the Office of Federal Procurement Policy Act (41 U.S.C. 403).''.

SEC. 4. 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

(b) TABLE OF SECTIONS IN TITLE 40.—The table of sections for chapter 113 of title 40, United States Code, is amended by inserting after the item relating to section 11318 the following new item:

(c) 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)'';

(B) in subsection (e)(2), by striking ''section 3532(1)'' and inserting ''section 3552(b)''; and

(C) in subsections (c)(3) and (d)(1), by striking ''section 11331 of title 40'' and inserting ''section 3558 of title 44''.

(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 3556(b)''.

(d) REPEAL.—

(1) Subchapter III of chapter 113 of title 40, United States Code, is repealed.

(2) The table of sections for chapter 113 of such title is amended by striking the matter relating to subchapter III.

SEC. 5. EFFECTIVE DATE.

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

○