AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 4257 OFFERED BY MR. CHAFFETZ OF UTAH

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 sys-

tems, 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)(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.

☒