

Section 3531, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2259, set forth purposes of subchapter II. See section 3551 of this title.

A prior section 3531, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, set forth purposes of subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3532, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2260, related to definitions applicable to subchapter II. See section 3552 of this title.

A prior section 3532, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, related to definitions applicable to subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3533, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2261, set forth authority and functions of the Director. See section 3553 of this title.

A prior section 3533, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, set forth authority and functions of the Director prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3534, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2262, related to Federal agency responsibilities. See section 3554 of this title.

A prior section 3534, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–268, related to Federal agency responsibilities prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3535, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2265; amended Pub. L. 108–177, title III, §377(e), Dec. 13, 2003, 117 Stat. 2631, related to annual independent evaluation. See section 3555 of this title.

A prior section 3535, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–271, related to annual independent evaluation prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3536, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2266, described responsibilities for the head of each agency operating or exercising control of a national security system. See section 3557 of this title.

A prior section 3536, added Pub. L. 106–398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–272; amended Pub. L. 107–314, div. A, title X, §1052(a), Dec. 2, 2002, 116 Stat. 2648, set forth expiration date of subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3537, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2267, authorized appropriations for fiscal years 2003 through 2007.

Section 3538, added Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2267, related to effect on existing law. See section 3558 of this title.

Sections 3541 to 3549 comprised subchapter III of this chapter “INFORMATION SECURITY”.

Section 3541, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2946, set forth purposes of subchapter III. See section 3551 of this title.

Section 3542, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947, related to definitions applicable to subchapter III. See section 3552 of this title.

Section 3543, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947, set forth authority and functions of the Director. See section 3553 of this title.

Section 3544, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2949, related to Federal agency responsibilities. See section 3554 of this title.

Section 3545, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2952; amended Pub. L. 108–177, title III, §377(e), Dec. 13, 2003, 117 Stat. 2631, related to annual independent evaluation. See section 3555 of this title.

Section 3546, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2954, related to Federal information security incident center. See section 3556 of this title.

Section 3547, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2954, described responsibilities

for the head of each agency operating or exercising control of a national security system. See section 3557 of this title.

Section 3548, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2954, authorized appropriations for fiscal years 2003 through 2007.

Section 3549, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2955, related to effect on existing law and provided that subchapter II was not to apply while subchapter III was in effect. See section 3558 of this title.

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, including through automated security tools to continuously diagnose and improve security;

(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.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3073.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3531 and 3541 of this title prior to repeal by Pub. L. 113–283.

Statutory Notes and Related Subsidiaries

CYBERSECURITY IMPROVEMENTS TO AGENCY INFORMATION SYSTEMS

Pub. L. 114–4, title V, §547, Mar. 4, 2015, 129 Stat. 69, provided that:

“(a) Of the amounts made available by this Act [Pub. L. 114–4, see Tables for classification] for ‘National Protection and Programs Directorate, Infrastructure Protection and Information Security’, \$140,525,000 for the Federal Network Security program, project, and activity shall be used to deploy on Federal systems technology to improve the information security of agency

information systems covered by [former] section 3543(a) of title 44, United States Code [see now 44 U.S.C. 3553]: *Provided*, That funds made available under this section shall be used to assist and support Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity to address escalating and rapidly evolving threats to information security, including the acquisition and operation of a continuous monitoring and diagnostics program, in collaboration with departments and agencies, that includes equipment, software, and Department of Homeland Security supplied services: *Provided further*, That continuous monitoring and diagnostics software procured by the funds made available by this section shall not transmit to the Department of Homeland Security any personally identifiable information or content of network communications of other agencies' users: *Provided further*, That such software shall be installed, maintained, and operated in accordance with all applicable privacy laws and agency-specific policies regarding network content.

“(b) Funds made available under this section may not be used to supplant funds provided for any such system within an agency budget.

“(c) Not later than July 1, 2015, the heads of all Federal agencies shall submit to the Committees on Appropriations of the Senate and the House of Representatives expenditure plans for necessary cybersecurity improvements to address known vulnerabilities to information systems described in subsection (a).

“(d) Not later than October 1, 2015, and semiannually thereafter, the head of each Federal agency shall submit to the Director of the Office of Management and Budget a report on the execution of the expenditure plan for that agency required by subsection (c): *Provided*, That the Director of the Office of Management and Budget shall summarize such execution reports and annually submit such summaries to Congress in conjunction with the annual progress report on implementation of the E-Government Act of 2002 (Public Law 107-347) [see Tables for classification], as required by section 3606 of title 44, United States Code.

“(e) This section shall not apply to the legislative and judicial branches of the Federal Government and shall apply to all Federal agencies within the executive branch except for the Department of Defense, the Central Intelligence Agency, and the Office of the Director of National Intelligence.”

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 113-76, div. F, title V, § 554, Jan. 17, 2014, 128 Stat. 278.

Pub. L. 113-6, div. D, title V, § 558, Mar. 26, 2013, 127 Stat. 377.

Executive Documents

EX. ORD. NO. 14028. IMPROVING THE NATION'S CYBERSECURITY

Ex. Ord. No. 14028, May 12, 2021, 86 F.R. 26633, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner

with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

SEC. 2. Removing Barriers to Sharing Threat Information. (a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

(b) Within 60 days of the date of this order [May 12, 2021], the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The recommendations shall include descriptions of contractors to be covered by the proposed contract language.

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

(iii) service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and

(iv) service providers share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

(d) Within 90 days of receipt of the recommendations described in subsection (b) of this section, the FAR Council shall review the proposed contract language and conditions and, as appropriate, shall publish for public comment proposed updates to the FAR.

(e) Within 120 days of the date of this order, the Secretary of Homeland Security and the Director of OMB shall take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks.

(f) It is the policy of the Federal Government that:

(i) information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies;

(ii) ICT service providers must also directly report to CISA whenever they report under subsection (f)(i) of this section to Federal Civilian Executive Branch (FCEB) Agencies, and CISA must centrally collect and manage such information; and

(iii) reports pertaining to National Security Systems, as defined in section 10(h) of this order, must be received and managed by the appropriate agency as to be determined under subsection (g)(i)(E) of this section.

(g) To implement the policy set forth in subsection (f) of this section:

(i) Within 45 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB, shall recommend to the FAR Council contract language that identifies:

(A) the nature of cyber incidents that require reporting;

(B) the types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation;

(C) appropriate and effective protections for privacy and civil liberties;

(D) the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection;

(E) National Security Systems reporting requirements; and

(F) the type of contractors and associated service providers to be covered by the proposed contract language.

(ii) Within 90 days of receipt of the recommendations described in subsection (g)(i) of this section, the FAR Council shall review the recommendations and publish for public comment proposed updates to the FAR.

(iii) Within 90 days of the date of this order, the Secretary of Defense acting through the Director of the NSA, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies.

(h) Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements

across agencies will streamline and improve compliance for vendors and the Federal Government.

(i) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA, the Director of OMB, and the Administrator of General Services, shall review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language.

(j) Within 60 days of receiving the recommended contract language developed pursuant to subsection (i) of this section, the FAR Council shall review the recommended contract language and publish for public comment proposed updates to the FAR.

(k) Following any updates to the FAR made by the FAR Council after the public comment period described in subsection (j) of this section, agencies shall update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of such FAR updates.

(l) The Director of OMB shall incorporate into the annual budget process a cost analysis of all recommendations developed under this section.

SEC. 3. *Modernizing Federal Government Cybersecurity.*
 (a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to subsection (b)(i) and (ii) of this section.

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

(i) Within 90 days of the date of this order, the Director of OMB, in consultation with the Secretary of Homeland Security acting through the Director of CISA, and the Administrator of General Services acting through FedRAMP, shall develop a Federal cloud-security strategy and provide guidance to agencies accordingly. Such guidance shall seek to ensure that risks to the FCEB from using cloud-based services are broadly understood and effectively addressed, and that FCEB Agencies move closer to Zero Trust Architecture.

(ii) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the FCEB, cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

(iii) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall develop and issue, for FCEB Agencies, a cloud-service governance framework. That framework shall identify a range of services and protections available to agencies based on incident severity. That framework shall also identify data and processing activities associated with those services and protections.

(iv) Within 90 days of the date of this order, the heads of FCEB Agencies, in consultation with the Secretary of Homeland Security acting through the Director of CISA, shall evaluate the types and sensitivity of their respective agency's unclassified data, and shall provide to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB a report based on such evaluation. The evaluation shall prioritize identification of the unclassified data considered by the agency to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

(d) Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. To that end:

(i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multi-factor authentication and encryption of data at rest and in transit. Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption.

(ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit.

(iii) Heads of FCEB Agencies that are unable to fully adopt multi-factor authentication and data encryption within 180 days of the date of this order shall, at the end of the 180-day period, provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

(e) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Attorney General, the Director of the FBI, and the Administrator of General Services acting through the Director of FedRAMP, shall establish a framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology, in order to ensure effective information sharing among agencies and between agencies and CSPs.

(f) Within 60 days of the date of this order, the Administrator of General Services, in consultation with the Director of OMB and the heads of other agencies as the Administrator of General Services deems appropriate, shall begin modernizing FedRAMP by:

(i) establishing a training program to ensure agencies are effectively trained and equipped to manage

FedRAMP requests, and providing access to training materials, including videos-on-demand;

(ii) improving communication with CSPs through automation and standardization of messages at each stage of authorization. These communications may include status updates, requirements to complete a vendor's current stage, next steps, and points of contact for questions;

(iii) incorporating automation throughout the lifecycle of FedRAMP, including assessment, authorization, continuous monitoring, and compliance;

(iv) digitizing and streamlining documentation that vendors are required to complete, including through online accessibility and pre-populated forms; and

(v) identifying relevant compliance frameworks, mapping those frameworks onto requirements in the FedRAMP authorization process, and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate.

SEC. 4. *Enhancing Software Supply Chain Security.* (a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software"—software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)—is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(1) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

(E) employing encryption for data; and
 (F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

(g) Within 45 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, the Secretary of Homeland Security acting through the Director of CISA, the Director of OMB, and the Director of National Intelligence, shall publish a definition of the term “critical software” for inclusion in the guidance issued pursuant to subsection (e) of this section. That definition shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

(h) Within 30 days of the publication of the definition required by subsection (g) of this section, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to subsection (g) of this section.

(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.

(k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.

(l) Agencies may request an extension for complying with any requirements issued pursuant to subsection (k) of this section. Any such request shall be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB shall on a quarterly basis provide a report to the APNSA identifying and explaining all extensions granted.

(m) Agencies may request a waiver as to any requirements issued pursuant to subsection (k) of this section. Waivers shall be considered by the Director of OMB, in consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks.

(n) Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.

(o) After receiving the recommendations described in subsection (n) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, amend the FAR.

(p) Following the issuance of any final rule amending the FAR as described in subsection (o) of this section, agencies shall, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.

(q) The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, shall require agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to subsection (k) of this section or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to subsection (k) of this section, unless an extension or waiver is granted in accordance with subsection (l) or (m) of this section.

(r) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines recommending minimum standards for vendors’ testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

(s) The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal

Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

(u) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, shall identify secure software development practices or criteria for a consumer software labeling program, and shall consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director of NIST shall examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.

(v) These pilot programs shall be conducted in a manner consistent with OMB Circular A-119 and NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).

(w) Within 1 year of the date of this order, the Director of NIST shall conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.

(x) Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the APNSA, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.

SEC. 5. *Establishing a Cyber Safety Review Board.* (a) The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board (Board), pursuant to section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451).

(b) The Board shall review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination) (PPD-41)) affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

(c) The Secretary of Homeland Security shall convene the Board following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group (UCG) as provided by section V(B)(2) of PPD-41; at any time as directed by the President acting through the APNSA; or at any time the Secretary of Homeland Security deems necessary.

(d) The Board's initial review shall relate to the cyber activities that prompted the establishment of a UCG in December 2020, and the Board shall, within 90 days of the Board's establishment, provide recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices, as outlined in subsection (i) of this section.

(e) The Board's membership shall include Federal officials and representatives from private-sector entities. The Board shall comprise representatives of the Department of Defense, the Department of Justice, CISA, the NSA, and the FBI, as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security. A representative from OMB shall participate in Board activities when an incident under review involves FCEB Information Systems, as determined by the Secretary of Homeland Security. The Secretary of Homeland Security may invite the participation of others on a case-by-case basis depending on the nature of the incident under review.

(f) The Secretary of Homeland Security shall biennially designate a Chair and Deputy Chair of the Board from among the members of the Board, to include one Federal and one private-sector member.

(g) The Board shall protect sensitive law enforcement, operational, business, and other confidential information that has been shared with it, consistent with applicable law.

(h) The Secretary of Homeland Security shall provide to the President through the APNSA any advice, information, or recommendations of the Board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident.

(i) Within 30 days of completion of the initial review described in subsection (d) of this section, the Secretary of Homeland Security shall provide to the President through the APNSA the recommendations of the Board based on the initial review. These recommendations shall describe:

(i) identified gaps in, and options for, the Board's composition or authorities;

(ii) the Board's proposed mission, scope, and responsibilities;

(iii) membership eligibility criteria for private-sector representatives;

(iv) Board governance structure including interaction with the executive branch and the Executive Office of the President;

(v) thresholds and criteria for the types of cyber incidents to be evaluated;

(vi) sources of information that should be made available to the Board, consistent with applicable law and policy;

(vii) an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents; and

(viii) administrative and budgetary considerations required for operation of the Board.

(j) The Secretary of Homeland Security, in consultation with the Attorney General and the APNSA, shall review the recommendations provided to the President through the APNSA pursuant to subsection (i) of this section and take steps to implement them as appropriate.

(k) Unless otherwise directed by the President, the Secretary of Homeland Security shall extend the life of the Board every 2 years as the Secretary of Homeland Security deems appropriate, pursuant to section 871 of the Homeland Security Act of 2002.

SEC. 6. *Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.* (a) The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies.

Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses.

(b) Within 120 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB,

the Federal Chief Information Officers Council, and the Federal Chief Information Security Council, and in coordination with the Secretary of Defense acting through the Director of the NSA, the Attorney General, and the Director of National Intelligence, shall develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting FCEB Information Systems. The playbook shall:

(i) incorporate all appropriate NIST standards;
 (ii) be used by FCEB Agencies; and
 (iii) articulate progress and completion through all phases of an incident response, while allowing flexibility so it may be used in support of various response activities.

(c) The Director of OMB shall issue guidance on agency use of the playbook.

(d) Agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook may use such procedures only after consulting with the Director of OMB and the APNSA and demonstrating that these procedures meet or exceed the standards proposed in the playbook.

(e) The Director of CISA, in consultation with the Director of the NSA, shall review and update the playbook annually, and provide information to the Director of OMB for incorporation in guidance updates.

(f) To ensure comprehensiveness of incident response activities and build confidence that unauthorized cyber actors no longer have access to FCEB Information Systems, the playbook shall establish, consistent with applicable law, a requirement that the Director of CISA review and validate FCEB Agencies' incident response and remediation results upon an agency's completion of its incident response. The Director of CISA may recommend use of another agency or a third-party incident response team as appropriate.

(g) To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms and use such terms consistently with any statutory definitions of those terms, to the extent practicable, thereby providing a shared lexicon among agencies using the playbook.

SEC. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks. (a) The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government's cybersecurity efforts.

(b) FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

(c) Within 30 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall provide to the Director of OMB recommendations on options for implementing an EDR initiative, centrally located to support host-level visibility, attribution, and response regarding FCEB Information Systems.

(d) Within 90 days of receiving the recommendations described in subsection (c) of this section, the Director of OMB, in consultation with Secretary of Homeland Security, shall issue requirements for FCEB Agencies to adopt Federal Government-wide EDR approaches. Those requirements shall support a capability of the Secretary of Homeland Secretary, acting through the Director of CISA, to engage in cyber hunt, detection, and response activities.

(e) The Director of OMB shall work with the Secretary of Homeland Security and agency heads to ensure that agencies have adequate resources to comply with the requirements issued pursuant to subsection (d) of this section.

(f) Defending FCEB Information Systems requires that the Secretary of Homeland Security acting through the Director of CISA have access to agency data that are relevant to a threat and vulnerability analysis, as well as for assessment and threat-hunting purposes. Within 75 days of the date of this order, agencies shall establish or update Memoranda of Agreement (MOA) with CISA for the Continuous Diagnostics and Mitigation Program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law.

(g) Within 45 days of the date of this order, the Director of the NSA as the National Manager for National Security Systems (National Manager) shall recommend to the Secretary of Defense, the Director of National Intelligence, and the Committee on National Security Systems (CNSS) appropriate actions for improving detection of cyber incidents affecting National Security Systems, to the extent permitted by applicable law, including recommendations concerning EDR approaches and whether such measures should be operated by agencies or through a centralized service of common concern provided by the National Manager.

(h) Within 90 days of the date of this order, the Secretary of Defense, the Director of National Intelligence, and the CNSS shall review the recommendations submitted under subsection (g) of this section and, as appropriate, establish policies that effectuate those recommendations, consistent with applicable law.

(i) Within 90 days of the date of this order, the Director of CISA shall provide to the Director of OMB and the APNSA a report describing how authorities granted under section 1705 of Public Law 116-283 [amending 44 U.S.C. 3553], to conduct threat-hunting activities on FCEB networks without prior authorization from agencies, are being implemented. This report shall also recommend procedures to ensure that mission-critical systems are not disrupted, procedures for notifying system owners of vulnerable government systems, and the range of techniques that can be used during testing of FCEB Information Systems. The Director of CISA shall provide quarterly reports to the APNSA and the Director of OMB regarding actions taken under section 1705 of Public Law 116-283.

(j) To ensure alignment between Department of Defense Information Network (DODIN) directives and FCEB Information Systems directives, the Secretary of Defense and the Secretary of Homeland Security, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, establish procedures for the Department of Defense and the Department of Homeland Security to immediately share with each other Department of Defense Incident Response Orders or Department of Homeland Security Emergency Directives and Binding Operational Directives applying to their respective information networks;

(ii) evaluate whether to adopt any guidance contained in an Order or Directive issued by the other Department, consistent with regulations concerning sharing of classified information; and

(iii) within 7 days of receiving notice of an Order or Directive issued pursuant to the procedures established under subsection (j)(i) of this section, notify the APNSA and Administrator of the Office of Electronic Government within OMB of the evaluation described in subsection (j)(ii) of this section, including a determination whether to adopt guidance issued by the other Department, the rationale for that determination, and a timeline for application of the directive, if applicable.

SEC. 8. Improving the Federal Government's Investigative and Remediation Capabilities. (a) Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide

them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

(b) Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency's systems and networks. Such recommendations shall include the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations. Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order.

(c) Within 90 days of receiving the recommendations described in subsection (b) of this section, the Director of OMB, in consultation with the Secretary of Commerce and the Secretary of Homeland Security, shall formulate policies for agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

(d) The Director of OMB shall work with agency heads to ensure that agencies have adequate resources to comply with the requirements identified in subsection (c) of this section.

(e) To address cyber risks or incidents, including potential cyber risks or incidents, the proposed recommendations issued pursuant to subsection (b) of this section shall include requirements to ensure that, upon request, agencies provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law. These requirements should be designed to permit agencies to share log information, as needed and appropriate, with other Federal agencies for cyber risks or incidents.

SEC. 9. National Security Systems. (a) Within 60 days of the date of this order, the Secretary of Defense acting through the National Manager, in coordination with the Director of National Intelligence and the CNSS, and in consultation with the APNSA, shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order that are otherwise not applicable to National Security Systems. Such requirements may provide for exceptions in circumstances necessitated by unique mission needs. Such requirements shall be codified in a National Security Memorandum (NSM). Until such time as that NSM is issued, programs, standards, or requirements established pursuant to this order shall not apply with respect to National Security Systems.

(b) Nothing in this order shall alter the authority of the National Manager with respect to National Security Systems as defined in National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD-42). The FCEB network shall continue to be within the authority of the Secretary of Homeland Security acting through the Director of CISA.

SEC. 10. Definitions. For purposes of this order:

(a) the term "agency" has the meaning ascribed to it under 44 U.S.C. 3502.

(b) the term "auditing trust relationship" means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

(c) the term "cyber incident" has the meaning ascribed to an "incident" under 44 U.S.C. 3552(b)(2).

(d) the term "Federal Civilian Executive Branch Agencies" or "FCEB Agencies" includes all agencies except for the Department of Defense and agencies in the Intelligence Community.

(e) the term "Federal Civilian Executive Branch Information Systems" or "FCEB Information Systems" means those information systems operated by Federal Civilian Executive Branch Agencies, but excludes National Security Systems.

(f) the term "Federal Information Systems" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency, including FCEB Information Systems and National Security Systems.

(g) the term "Intelligence Community" or "IC" has the meaning ascribed to it under 50 U.S.C. 3003(4).

(h) the term "National Security Systems" means information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3).

(i) the term "logs" means records of the events occurring within an organization's systems and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.

(j) the term "Software Bill of Materials" or "SBOM" means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

(k) the term "Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

SEC. 11. *General Provisions.* (a) Upon the appointment of the National Cyber Director (NCD) and the establishment of the related Office within the Executive Office of the President, pursuant to section 1752 of Public Law 116-283 [enacting 6 U.S.C. 1500], portions of this order may be modified to enable the NCD to fully execute its duties and responsibilities.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) This order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) Nothing in this order confers authority to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a criminal or national security investigation.

J.R. BIDEN, JR.

§ 3552. Definitions

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

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

(1) The term “binding operational directive” means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

(2) The term “incident” means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(3) 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.

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

(5) The term “intelligence community” has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(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).

(7) The term “Secretary” means the Secretary of Homeland Security.

(Added Pub. L. 113-283, §2(a), Dec. 18, 2014, 128 Stat. 3074.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3532 and 3542 of this title prior to repeal by Pub. L. 113-283.

§ 3553. Authority and functions of the Director and the Secretary

(a) DIRECTOR.—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) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

(C) requirements for the mitigation of exigent risks to information systems; and

(D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

(3) monitoring agency implementation of information security policies and practices;

(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

(5) coordinating Government-wide efforts on information security policies and practices,

including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

(A) operating the Federal information security incident center established under section 3556;

(B) upon request by an agency, deploying, operating, and maintaining technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems;

(7) hunting for and identifying, with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems;

(8) upon request by an agency, and at the Secretary's discretion, with or without reimbursement—

(A) providing services, functions, and capabilities, including operation of the agency's information security program, to assist the agency with meeting the requirements set forth in section 3554(b); and

(B) deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information; and

(9) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in sub-

section (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY 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 National 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 an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

(f) CONSIDERATION.—

(1) IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.¹

(2) DIRECTIVES.—The Secretary shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.¹

(3) RULE OF CONSTRUCTION.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.¹

(g) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

(h) DIRECTION TO AGENCIES.—

(1) AUTHORITY.—

(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a sub-

stantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

(A) in coordination with the Director, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

(i) thresholds and other criteria;

(ii) privacy and civil liberties protections; and

(iii) providing notice to potentially affected third parties;

(B) specify the reasons for the required action and the duration of the directive;

(C) minimize the impact of a directive under this subsection by—

(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

(ii) limiting directives to the shortest period practicable;

(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

(G) consider any applicable standards or guidelines developed by the National Institute of Standards and Technology issued by the Secretary of Commerce under section 11331 of title 40; and

(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

(3) IMMINENT THREATS.—

(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use under this subsection of the intrusion detection and prevention capabilities established under section 230(b)(1)¹ of the Homeland Security Act of 2002 for the purpose of ensuring

¹ See References in Text note below.

the security of agency information systems, if—

(i) the Secretary determines there is an imminent threat to agency information systems;

(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of the intrusion detection and prevention capabilities under the control of the Secretary;

(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—

(I) any action taken under this paragraph; and

(II) the reasons for and duration and nature of the action;

(v) the action of the Secretary is consistent with applicable law; and

(vi) the Secretary authorizes the use of the intrusion detection and prevention capabilities in accordance with the advance procedures established under subparagraph (C).

(B) **LIMITATION ON DELEGATION.**—The authority under this paragraph may not be delegated by the Secretary.

(C) **ADVANCE PROCEDURES.**—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of the intrusion detection and prevention capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

(4) **LIMITATION.**—The Secretary may direct or authorize lawful action or the use of the intrusion detection and prevention capabilities under this subsection only to—

(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

(B) require the remediation of or protect against identified information security risks with respect to—

(i) information collected or maintained by or on behalf of an agency; or

(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

(i) **ANNUAL REPORT TO CONGRESS.**—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), includ-

ing any actions taken pursuant to section 11303(b)(5) of title 40.

(j) **RULE OF CONSTRUCTION.**—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).

(k) **APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.**—In this section, the term “appropriate congressional committees” means—

(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

(l) **INFORMATION SHARING.**—

(1) **IN GENERAL.**—Notwithstanding any other provision of law, including any provision of law that would otherwise restrict or prevent the head of an agency from disclosing information to the Secretary, the Secretary in carrying out this section and title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) may access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks.

(2) **EXCEPTION.**—Paragraph (1) shall not apply to national security systems or to information systems described in paragraph (2) or (3) of subsection (e).

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3075; amended Pub. L. 114–113, div. N, title II, §§224(e), 229(a), Dec. 18, 2015, 129 Stat. 2967, 2972; Pub. L. 115–390, title II, §204(a)(1), Dec. 21, 2018, 132 Stat. 5192; Pub. L. 116–92, div. E, title LXIV, §6432, Dec. 20, 2019, 133 Stat. 2200; Pub. L. 116–283, div. A, title XVII, §1705, Jan. 1, 2021, 134 Stat. 4082.)

Editorial Notes

REFERENCES IN TEXT

Section 11331 of title 40, referred to in subsec. (f), was generally amended by both Pub. L. 107–347 and Pub. L. 107–296. As amended by Pub. L. 107–347, effective Dec. 17, 2002, section 11331 of title 40 provided for the prescription by the Secretary of Commerce of standards and guidelines pertaining to Federal information systems. See 2002 Amendment note under that section. As amended by Pub. L. 107–296, effective 60 days after Nov. 25, 2002, section 11331 of title 40 provided for the promulgation by the Director of the Office of Management and Budget of information security standards pertaining to Federal information systems.

Section 230(b)(1) of the Homeland Security Act of 2002, referred to in subsec. (h)(3)(A), is section 230(b)(1) of title II of Pub. L. 107–296, as added by Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which was redesignated section 2213(b)(1) of Pub. L. 107–296 by section 2(g)(2)(I) of Pub. L. 115–278, Nov. 16, 2018, 132 Stat. 4178, and is classified to section 663(b)(1) of Title 6, Domestic Security.

The Homeland Security Act of 2002, referred to in subsec. (l)(1), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135. Title XXII of the Act is classified generally to subchapter XVIII (§651 et seq.) of chapter 1 of Title 6, Domestic Security. For complete classification of this Act to the Code, see Short Title note set out under section 101 of Title 6 and Tables.

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3533 and 3543 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2021—Subsec. (b)(7) to (9). Pub. L. 116–283, §1705(1), added pars. (7) and (8) and redesignated former par. (7) as (9).

Subsec. (l). Pub. L. 116–283, §1705(2), added subsec. (l).
2019—Subsecs. (j), (k). Pub. L. 116–92 added subsec. (j) and redesignated former subsec. (j) as (k).

2018—Subsec. (a)(5). Pub. L. 115–390 inserted “and section 1326 of title 41” after “compliance with the requirements of this subchapter”.

2015—Subsec. (b)(6)(B). Pub. L. 114–113, §224(e), inserted “, operating, and maintaining” after “deploying”.

Subsecs. (h) to (j). Pub. L. 114–113, §229(a), added subsecs. (h) to (j).

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019.

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of this title.

CONSTRUCTION

Pub. L. 115–390, title II, §204(b), Dec. 21, 2018, 132 Stat. 5193, provided that: “Nothing in this title [see section 201 of Pub. L. 115–390, set out as a Short Title of 2018 note under section 101 of Title 41, Public Contracts] shall be construed to alter or impede any authority or responsibility under section 3553 of title 44, United States Code.”

BREACHES

Pub. L. 113–283, §2(d), Dec. 18, 2014, 128 Stat. 3085, provided that:

“(1) REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

“(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall—

“(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

“(ii) include—

“(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

“(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

“(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

“(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

“(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

“(2) NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

“(3) REPORTS.—

“(A) DIRECTOR OF OMB.—During the first 2 years beginning after the date of enactment of this Act [Dec. 18, 2014], the Director of the Office of Management and Budget shall, on an annual basis—

“(i) assess agency implementation of data breach notification policies and guidelines in aggregate; and

“(ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code.

“(B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.

“(4) EXCEPTION.—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

“(5) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to alter any authority of a Federal agency or department.”

Similar provisions were contained in Pub. L. 113–282, §7(b), Dec. 18, 2014, 128 Stat. 3071.

§ 3554. Federal agency responsibilities

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter, subchapter III of chapter 13 of title 41, and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40;

(ii) operational directives developed by the Secretary under section 3553(b);

(iii) policies and procedures issued by the Director;

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

(v) emergency directives issued by the Secretary under section 3553(h); and

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; and

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

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

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

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

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

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

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

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

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

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

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

(B) developing and maintaining an agency-wide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

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

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

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

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

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

(2) policies and procedures that—

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

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

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

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

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

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

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

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

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

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

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

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);¹

(B) may include testing relied on in an evaluation under section 3555; and

(C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

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

(A) shall be consistent with the standards and guidelines described in section 3556(b);

(B) may include using automated tools; and

(C) shall include—

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

(ii) notifying and consulting with the Federal information security incident center established in section 3556; and

(iii) notifying and consulting with, as appropriate—

(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

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

(III) for a major incident, the committees of Congress described in subsection (c)(1)—

(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

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

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

(c) AGENCY REPORTING.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Com-

mittee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

(i) a description of each major information security incident or related sets of incidents, including summaries of—

(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred;

(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

(IV) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

(I) the number of individuals whose information was affected by the major information security incident; and

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) UNCLASSIFIED REPORT.—

(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

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

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

¹ So in original. Section 3505 contains two subsecs. (c).

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)(1).

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

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3078; amended Pub. L. 114–113, div. N, title II, § 229(b), Dec. 18, 2015, 129 Stat. 2974; Pub. L. 115–390, title II, § 204(a)(2), Dec. 21, 2018, 132 Stat. 5193.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3534 and 3544 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2018—Subsec. (a)(1)(B). Pub. L. 115–390, § 204(a)(2)(A), inserted “, subchapter III of chapter 13 of title 41,” after “complying with the requirements of this subchapter” in introductory provisions.

Subsec. (a)(1)(B)(vi). Pub. L. 115–390, § 204(a)(2)(B), (C), added cl. (vi).

2015—Subsec. (a)(1)(B)(v). Pub. L. 114–113 added cl. (v).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of Title 41, Public Contracts.

MAJOR INCIDENT

Pub. L. 113–283, §2(b), Dec. 18, 2014, 128 Stat. 3085, provided that: “The Director of the Office of Management and Budget shall—

“(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

“(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.”

§ 3555. Annual independent evaluation

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

(2) Each evaluation under this section shall include—

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

(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

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

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

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

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

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

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

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

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

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

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

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

(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

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

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of National 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) **ASSESSMENT TECHNICAL ASSISTANCE.**—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

(j) **GUIDANCE.**—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3082.)

Editorial Notes

REFERENCES IN TEXT

The Inspector General Act of 1978, referred to in subsec. (b)(1), is Pub. L. 95–452, Oct. 12, 1978, 92 Stat. 1101, which is set out in the Appendix to Title 5, Government Organization and Employees.

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3535 and 3545 of this title prior to repeal by Pub. L. 113–283.

§ 3556. Federal information security incident center

(a) **IN GENERAL.**—The Secretary 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;

(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

(5) 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.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in section 3546 of this title prior to repeal by Pub. L. 113–283.

§ 3557. 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.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3536 and 3547 of this title prior to repeal by Pub. L. 113–283.

§ 3558. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards¹ and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters² 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3538 and 3549 of this title prior to repeal by Pub. L. 113–283.

¹So in original. Probably should be “National Institute of Standards”.

²So in original. Probably should be “chapter”.

§ 3559. Federal websites required to be mobile friendly

(a) IN GENERAL.—If, on or after the date that is 180 days after the date of the enactment of this section, an agency creates a website that is intended for use by the public or conducts a redesign of an existing legacy website that is intended for use by the public, the agency shall ensure to the greatest extent practicable that the website is mobile friendly.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term “agency” has the meaning given that term in section 551 of title 5.

(2) MOBILE FRIENDLY.—The term “mobile friendly” means, with respect to a website, that the website is configured in such a way that the website may be navigated, viewed, and accessed on a smartphone, tablet computer, or similar mobile device.

(Added Pub. L. 115–114, §2(a), Jan. 10, 2018, 131 Stat. 2278.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of this section, referred to in subsec. (a), is the date of enactment of Pub. L. 115–114, which was approved Jan. 10, 2018.

SUBCHAPTER III—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

Editorial Notes

PRIOR PROVISIONS

Provisions similar to those in parts A to C of this subchapter were contained in Pub. L. 107–347, title V, Dec. 17, 2002, 116 Stat. 2962, which was set out as a note under section 3501 of this title, prior to repeal by Pub. L. 115–435, title III, §302(c)(1), title IV, §403, Jan. 14, 2019, 132 Stat. 5552, 5557, effective 180 days after Jan. 14, 2019.

PART A—GENERAL

§ 3561. Definitions

In this subchapter:

(1) AGENCY.—The term “agency” means any entity that falls within the definition of the term “executive agency”, as defined in section 102 of title 31, or “agency”, as defined in section 3502.

(2) AGENT.—The term “agent” means an individual—

(A)(i) who is an employee of a private organization or a researcher affiliated with an institution of higher learning (including a person granted special sworn status by the Bureau of the Census under section 23(c) of title 13), and with whom a contract or other agreement is executed, on a temporary basis, by an executive agency to perform exclusively statistical activities under the control and supervision of an officer or employee of that agency;

(ii) who is working under the authority of a government entity with which a contract or other agreement is executed by an executive agency to perform exclusively statis-

tical activities under the control of an officer or employee of that agency;

(iii) who is a self-employed researcher, a consultant, a contractor, or an employee of a contractor, and with whom a contract or other agreement is executed by an executive agency to perform a statistical activity under the control of an officer or employee of that agency; or

(iv) who is a contractor or an employee of a contractor, and who is engaged by the agency to design or maintain the systems for handling or storage of data received under this subchapter; and

(B) who agrees in writing to comply with all provisions of law that affect information acquired by that agency.

(3) BUSINESS DATA.—The term “business data” means operating and financial data and information about businesses, tax-exempt organizations, and government entities.

(4) DATA ASSET.—The term “data asset” has the meaning given that term in section 3502.

(5) DIRECTOR.—The term “Director” means the Director of the Office of Management and Budget.

(6) EVIDENCE.—The term “evidence” means information produced as a result of statistical activities conducted for a statistical purpose.

(7) IDENTIFIABLE FORM.—The term “identifiable form” means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means.

(8) NONSTATISTICAL PURPOSE.—The term “nonstatistical purpose”—

(A) means the use of data in identifiable form for any purpose that is not a statistical purpose, including any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent; and

(B) includes the disclosure under section 552 of title 5 of data that are acquired for exclusively statistical purposes under a pledge of confidentiality.

(9) RESPONDENT.—The term “respondent” means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

(10) STATISTICAL ACTIVITIES.—The term “statistical activities”—

(A) means the collection, compilation, processing, or analysis of data for the purpose of describing or making estimates concerning the whole, or relevant groups or components within, the economy, society, or the natural environment; and

(B) includes the development of methods or resources that support those activities, such as measurement methods, models, statistical classifications, or sampling frames.

(11) STATISTICAL AGENCY OR UNIT.—The term “statistical agency or unit” means an agency or organizational unit of the executive branch whose activities are predominantly the collec-