Section by Section

AMENDMENTS TO THE FEDERAL INFORMATION SECURITY ACT OF 2002

Sec. 3 Coordination of Federal Information Security Policy.

Sec 3(a) amends Chapter 35 of title 44, U.S.C., (the Federal Information Security Management Act of 2002) striking subchapters II and III and inserting the following new subchapter:

SUBCHAPTER II—INFORMATION SECURITY

Sec. 3551. Purposes.

This subchapter provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations. The subchapter recognizes the highly networked nature of the current federal computing environment and provides effective government-wide management of policies, directives, standards and guidelines, as well as effective and nimble oversight of and response to information security risks. Additionally, the subchapter provides for the development and maintenance of controls required to protect agency information and information systems and establishes a mechanism for improving Federal agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting. This subchapter maintains many of the goals and policies established in the Federal Information Security Management Act of 2002 (FISMA) while refining provisions that proved too slow or cumbersome in implementation.

Sec. 3552. Definitions.

This section defines the following terms for the purposes of this subchapter: “agency,” “Director,” “information system,” “adequate security,” “incident,” “information security,” “information technology,” “national security system,” and “Secretary.”

Sec. 3553. Federal Information Security Authority and Coordination.

Section 3553**(**a) authorizes the Secretary of Homeland Security (Secretary), to exercise primary responsibility within the executive branch for information security. This includes implementation of information security policies and directives and compliance with the requirements of this subchapter, except as provided in subsections (d) and (e). This authority is consistent with recent FISMA practice and Office of Management and Budget (OMB) guidance.

Section 3553(b) directs the Secretary to: (1) issue compulsory and binding policies and directives governing agency information security operations and require implementation of information security policies and directives; (2) review agency information security programs

required under section 3554(b) annually; and (3) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems. Binding policies and directives shall include: (1) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems; (2) minimum operational requirements for Federal Government network operations centers and security operations centers to protect agency information systems and provide common situational awareness across all agency information systems; (3) reporting requirements regarding information security incidents; (4) requirements for agency-wide information security programs; (5) performance requirements and metrics for the security of agency information systems; (6) training and minimum security clearance requirements to ensure that agencies are able to fully and timely comply with directions issued by the Secretary under this subchapter; (7) training requirements regarding privacy, civil rights and civil liberties, and information oversight for agency information security personnel; (8) requirements for the annual reports to the Secretary under section 3554(c); and (9) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads.

Section 3553(c) directs the Secretary to consider any applicable guidelines created under the National Institute of Standards and Technology Act, 15 U.S.C.§ 278g–3 and to consult with the Director of the National Institute of Standards and Technology (NIST) when policies and directives implement standards or guidelines developed by NIST under 40 U.S.C. § 11331.

Section 3553(d) exempts national security systems from the authorities of the Secretary under this section.

Section 3553(e) exempts the Department of Defense (DoD) from the responsibilities of the Secretary under paragraphs (1) and (2) of subsection (b) and subsection (c). The DoD Secretary will carry out these authorities and responsibilities for DoD.

Section 3553(f) states that nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any Head of a federal agency over such agency.

Sec. 3554. Agency Responsibilities.

Section 3554(a) directs the head of each agency to provide information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems belonging to such agency. Each agency head will maintain the responsibility for ensuring its agency complies with the requirements of this subchapter, including: reporting and sharing appropriate incident, threat, and vulnerability information with the DHS cybersecurity center designated under 3553(b)(3) and

other appropriate entities; ensuring that senior agency officials provide security for information and information systems under their control; assessing and maintaining the resiliency of information technology systems critical to agency mission and operations; designating the Inspector General or another independent evaluator to conduct the annual independent evaluation required under section 3556; delegating to a senior agency official the authority and responsibility to implement an agency-wide information security program; delegating to appropriate agency officials who are responsible for particular agency systems or subsystems the responsibility to ensure and enforce compliance with all requirements of the agency's information security program, in coordination with the senior agency official in charge of the agency-wide program; ensuring that the agency has trained personnel who have obtained security clearances that will permit them to assist the agency in complying with the requirements of this subchapter; ensuring that the designated senior agency official, in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions; and ensuring that the designated senior agency official possesses the necessary qualifications to administer the functions described in this subchapter.

The responsibilities of the senior agency official designated to implement the agency-wide information security program shall include: overseeing the establishment and maintenance of an enterprise security operations and continuous monitoring capability; developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under sections 3552 and 3553 and section 11331 of title 40; training and overseeing agency personnel with significant responsibilities for information security; and assisting senior agency officials concerning their respective information security responsibilities.

Section 3554 (b) states that the agency-wide information security programs described in subsection (a) shall include: (1) the development and maintenance of a risk management strategy for information security; (2) security testing commensurate with risk and impact; (3) mitigation of information security vulnerabilities commensurate with risk and impact; (4) risk-based, cost-effective policies and procedures that ensure adequate security throughout the lifecycle of each agency information system and are compliant with the requirements of this subchapter; (5) information security, privacy, civil rights, civil liberties, and information oversight training to inform information security personnel with access to agency information systems; (6) continuous monitoring of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices; (7) a process for ensuring that remedial actions have been taken to address any deficiencies in the information security policies, procedures, and practices of the agency; (8) operation of appropriate technical capabilities to detect, mitigate, report, and respond to information security incidents, consistent with policies and directives issued under section

3553(b); and (9) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Section 3554(c) requires each agency to submit an annual report on their information security program and information systems to the Secretary.

Sec. 3555. Periodic assessments

Section 3555(a) directs the Secretary to prepare periodic summaries of agency security programs and practices. Such summaries shall assess the effectiveness of agency information security policies, procedures, and practices; provide an overall assessment of Federal Government-wide agency information system security posture; and include recommendations for improving agency specific and Federal Government-wide agency information system security.

Section 3555(b) directs that periodic summaries relating to national security systems will be prepared as specified by the President and periodic summaries related to agency information systems under the control of the DoD shall be prepared by the Secretary of Defense.

Section 3555(c) directs assessors to take appropriate actions to ensure the protection of information that, if disclosed, may adversely affect information security.

Section 3555(d) directs the Secretary, in coordination with the Secretary of Defense, to evaluate and report to Congress annually on the adequacy and effectiveness of the information security summaries established under this section.

Sec. 3556. Independent Evaluations.

Section 3556 directs the Council of Inspectors General on Integrity and Efficiency, in consultation with the Director of OMB and Secretary, to issue and maintain criteria for cost-effective, risk-based, and independent evaluations for agency information security programs and practices in order to determine the effectiveness of such programs and practices. It directs that reports prepared under this section be provided to the Secretary upon delivery of the report to the agency head. It also directs that evaluations involving national security systems be conducted as directed by President.

Sec. 3557. Savings Provisions and Technical and Conforming Amendments.

Section 3557(a) contains savings provisions to maintain the effect of various OMB and Department of Commerce policies, standards, and compliance guidance.

Section 3557 (b) makes technical and conforming amendments to chapter 35 of title 44.

Sec. 4. Management of Information Technology.

Section 4(a) amends section 11331 of title 40, U.S.C., by revising the entire section as follows:

Sec. 11331. Responsibilities for Federal Information Systems Standards.

Section 11331(a) authorizes the Secretary of Commerce, in consultation with the Secretary of Homeland Security, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to federal information systems. However, standards and guidelines for national security systems will be developed, prescribed, enforced, and overseen in a manner directed by the President.

Section 11331(b) directs the Secretary of Commerce to make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of federal information systems. Standards prescribed under subsection (a)(1) shall include standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

Section 11331(c) authorizes the President to disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may be delegated to the Director of Office of Management and Budget. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President or the Director of Office of Management and Budget.

Section 11331(d) directs the Secretary of Commerce to exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget to ensure fiscal and policy consistency.

Section 11331(e) authorizes the head of any executive agency to employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary of Commerce prescribes under this section.

Section 11331(f) directs the Secretary of Commerce to make any decision regarding the promulgation of any standard under this section not later than 6 months after the submission of the proposed standard to the Secretary of Commerce by NIST.

Section 11331(g) defines the following terms for the purpose of this section: “federal information system,” “information security,” and “national security system.”

Section 4(b) makes technical and conforming amendments to section 21 of the National Institute of Standards and Technology Act (15 U.S.C. § 278g–4).