

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.

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.

§ 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.)

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, 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 existing 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; and

(7) 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);