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


Section 3550, added Pub. L. 107–347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2955, relating 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.


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:

§ 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 1101 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 on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency; or

(C) information systems operated or maintained by or on behalf of an agency; or

(D) 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;

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


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 11331 of title 40, to enforce accountability for compliance with such requirements; and