AMENDMENTS

2003—Subsec. (b)(1). Pub. L. 108–177 inserted ''or any other law'' after ''1978''.

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

§ 3536. 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. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2266.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

PRIOR PROVISIONS

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 this subchapter prior to the general amendment of this subchapter by Pub. L. 107–296.

EFFECTIVE DATE

Section effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as a note under section 101 of Title 6, Domestic Security.

§ 3537. Authorization of appropriations

There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

(Added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2267.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

§ 3538. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards[1] 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 chapters 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 Congress or the Comptroller General of the United States.

(Added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2267.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

SUBCHAPTER III—INFORMATION SECURITY

§ 3541. 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;

(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. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2946.)

EFFECTIVE DATE

Pub. L. 107–347, title IV, § 402(b), Dec. 17, 2002, 116 Stat. 2962, provided that: ''Title III [see Short Title of 2002

[1] So in original. Probably should be ''National Institute of Standards''.

Amendments note set out under section 101 of this title] and this title [enacting provisions set out as a note under section 3601 of this title] shall take effect on the date of enactment of this Act [Dec. 17, 2002].''

CYBERSECURITY IMPROVEMENTS TO AGENCY INFORMATION SYSTEMS

Pub. L. 113–6, div. D, title V, § 558, Mar. 26, 2013, 127 Stat. 377, provided that:

''(a) Of the amounts made available by this Act [div. D of Pub. L. 113—6, see Tables for classification] for National Protection and Programs Directorate, 'Infrastructure Protection and Information Security', $202,000,000 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 section 3543(a) of title 44, United States Code: *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 not later than April 1, 2013, and quarterly thereafter, the Under Secretary of Homeland Security of the National Protection and Programs Directorate shall submit to the Committees on Appropriations of the Senate and House of Representatives a report on the obligation and expenditure of funds made available under this section: *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, 2013, the heads of all Federal agencies shall submit to the Committees on Appropriations of the Senate and 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, 2013, and quarterly 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), 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.''

§ 3542. 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 ''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.

(2)(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).

(3) The term ''information technology'' has the meaning given that term in section 11101 of title 40.

(Added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

§ 3543. Authority and functions of the Director

(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

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