

means the Federal Financial Management Improvement Act of 1996, Pub. L. 104-208, div. A, title I, §101(f) [title VIII], Sept. 30, 1996, 110 Stat. 3009-314, 3009-389, which is set out as a note under section 3512 of Title 31, Money and Finance. For complete classification of this Act to the Code, see Tables.

PRIOR PROVISIONS

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 this subchapter by Pub. L. 107-296.

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives and Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Science and Technology of House of Representatives changed to Committee on Science, Space, and Technology of House of Representatives by House Resolution No. 5, One Hundred Twelfth Congress, Jan. 5, 2011.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§ 3535. Annual independent evaluation

(a)(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 by an agency 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 (made on the basis of the results of the testing) of compliance with—

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

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

(b) Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, 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) 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) The evaluation required by this section—

(1) shall be performed in accordance with generally accepted government auditing standards; and

(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) 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.

(f) 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)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(a)(8).

(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 Central 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) 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.

(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.)

APPLICABILITY OF SECTION

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

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, as amended, which is set out in the Appendix to Title 5, Government Organization and Employees.

PRIOR PROVISIONS

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 this subchapter by Pub. L. 107-296.

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 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 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

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