

(ii) an office designated by the President for any incident involving a national security system; and

(iii) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) Each agency shall—

(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

(A) annual agency budgets;

(B) information resources management under subchapter 1² of this chapter;

(C) information technology management under subtitle III of title 40;

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

(G) internal accounting and administrative controls under section 3512 of title 31, United States Code,³ (known as the “Federal Managers Financial Integrity Act”); and

(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

(A) as a material weakness in reporting under section 3512 of title 31; and

(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2262.)

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 Chief Financial Officers Act of 1990, referred to in subsec. (c)(2)(E), is Pub. L. 101-576, Nov. 15, 1990, 104 Stat. 2838. For complete classification of this Act to the Code, see Short Title of 1990 Amendment note set out under section 501 of Title 31, Money and Finance, and Tables.

The Federal Financial Management Improvement Act, referred to in subsec. (c)(2)(F), (3)(B), probably 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 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.

² So in original. Probably should be “I”.

³ So in original. The comma probably should not appear.

(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 401 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.