

subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

- (A) computers and computer networks;
- (B) ancillary equipment;
- (C) software, firmware, and related procedures;
- (D) services, including support services; and
- (E) related resources.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2260.)

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 3532, added Pub. L. 106-398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A-266, related to definitions applicable to this subchapter prior to the general amendment of this subchapter by Pub. L. 107-296.

§ 3533. Authority and functions of the Director

(a) The Director shall oversee agency information security policies and practices, by—

- (1) promulgating information security standards under section 11331 of title 40;
- (2) overseeing the implementation of policies, principles, standards, and guidelines on information security;
- (3) 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;
- (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(b)(5) of title 40, to enforce accountability for compliance with such requirements;
- (6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);
- (7) coordinating information security policies and procedures with related information resources management policies and procedures; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

- (A) a summary of the findings of evaluations required by section 3535;
- (B) significant deficiencies in agency information security practices;
- (C) planned remedial action to address such deficiencies; and
- (D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(9) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2261.)

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 3533, added Pub. L. 106-398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A-266, set forth authority and functions of the Director prior to the general amendment of this subchapter by Pub. L. 107-296.

§ 3534. Federal agency responsibilities

(a) The head of each agency shall—

- (1) be responsible for—
 - (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
 - (i) information collected or maintained by or on behalf of the agency; and
 - (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
 - (B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—
 - (i) information security standards promulgated by the Director under section 11331 of title 40; and
 - (ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and
 - (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;
- (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—
 - (A) assessing the risk and magnitude of the harm that could result from the unau-

thorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40 for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agency-wide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another

agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

(B) may include testing relied on in a¹ evaluation under section 3535;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, including—

(A) mitigating risks associated with such incidents before substantial damage is done; and

(B) notifying and consulting with, as appropriate—

(i) law enforcement agencies and relevant Offices of Inspector General;

¹ So in original. Probably should be "an".

(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.