

**TITLE 44 - PUBLIC PRINTING AND DOCUMENTS**  
**CHAPTER 35 - COORDINATION OF FEDERAL INFORMATION POLICY**  
**SUBCHAPTER III - INFORMATION SECURITY**

**§ 3544. Federal agency responsibilities**

- (a) **In General.**— 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 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 unauthorized 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 agencywide 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 3543 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) Agency Program.**— Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543 (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 a<sup>1</sup> evaluation under section 3545;
  - (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, consistent with standards and guidelines issued pursuant to section 3546 (b), including—
    - (A) mitigating risks associated with such incidents before substantial damage is done;

- (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and
  - (C) notifying and consulting with, as appropriate—
    - (i) law enforcement agencies and relevant Offices of Inspector General;
    - (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) **Agency Reporting.**— 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 1<sup>2</sup> 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,<sup>3</sup> (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) **Performance Plan.**—
- (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).

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscpri.html>).*

**(e) Public Notice and Comment.**— 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.

### **Footnotes**

<sup>1</sup> So in original. Probably should be “an”.

<sup>2</sup> So in original. Probably should be “I”.

<sup>3</sup> So in original. The comma probably should not appear.

(Added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2949.)

### **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.

### **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.