# 44 USCS § 3554

Current through Public Law 118-62, approved May 13, 2024.

*United States Code Service > TITLE 44. PUBLIC PRINTING AND DOCUMENTS (§§ 101 — 4104) > CHAPTER 35. Coordination of Federal Information Policy (Subchs. I — III) > Subchapter II. Information Security (§§ 3551 — 3559)*

## § 3554. 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 [44 USCS §§ 3551 et seq.], subchapter III of chapter 13 of title 41 [41 USCS §§ 1321 et seq.], and related policies, procedures, standards, and guidelines, including—

**(i)** information security standards promulgated under section 11331 of title 40 [40 USCS § 11331];

**(ii)** operational directives developed by the Secretary under section 3553(b) [44 USCS § 3553(b)];

**(iii)** policies and procedures issued by the Director;

**(iv)** information security standards and guidelines for national security systems issued in accordance with law and as directed by the President;

**(v)** emergency directives issued by the Secretary under section 3553(h) [44 USCS § 3553(h)]; and

**(vi)** responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41 [41 USCS § 1326], and complying with exclusion and removal orders issued under section 1323 of such title [41 USCS § 1323]; and

**(C)** ensuring that information security management processes are integrated with agency strategic, operational, and budgetary 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 [40 USCS § 11331], 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 [44 USCS § 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 [44 USCS §§ 3551 et seq.], 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 3553 of this title [44 USCS § 3553] and section 11331 of title 40 [40 USCS § 11331];

**(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 [44 USCS §§ 3551 et seq.] and related policies, procedures, standards, and guidelines;

**(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;

**(6)** ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter [44 USCS §§ 3551 et seq.] as directed by the official delegated authority under paragraph (3); and

**(7)** ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

**(b) Agency program.** Each agency shall develop, document, and implement an agency-wide information security program 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, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40 [40 USCS § 11331];

**(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 [44 USCS §§ 3551 et seq.];

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

**(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) [44 USCS § 3505(c)];

**(B)** may include testing relied on in an evaluation under section 3555 [44 USCS § 3555]; and

**(C)** shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40 [40 USCS § 11331];

**(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, which—

**(A)** shall be consistent with the standards and guidelines described in section 3556(b) [44 USCS § 3556(b)];

**(B)** may include using automated tools; and

**(C)** shall include—

**(i)** mitigating risks associated with such incidents before substantial damage is done;

**(ii)** notifying and consulting with the Federal information security incident center established in section 3556 [44 USCS § 3556]; and

**(iii)** notifying and consulting with, as appropriate—

**(I)** law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

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

**(III)** for a major incident, the committees of Congress described in subsection (c)(1)—

**(aa)** not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

**(bb)** after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

**(IV)** 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.**

**(1)** Annual report.

**(A)** In general. Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on

Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

**(i)** a description of each major information security incident or related sets of incidents, including summaries of—

**(I)** the threats and threat actors, vulnerabilities, and impacts relating to the incident;

**(II)** the risk assessments conducted under section 3554(a)(2)(A) [44 USCS § 3554(a)(2)(A)] of the affected information systems before the date on which the incident occurred;

**(III)** the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

**(IV)** the detection, response, and remediation actions;

**(ii)** the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

**(iii)** a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

**(I)** the number of individuals whose information was affected by the major information security incident; and

**(II)** a description of the information that was breached or exposed; and

**(iv)** any other information as the Director or the Secretary, in consultation with the Director, may require.

**(B)** Unclassified report.

**(i)** In general. Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

**(ii)** Access to information. The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

**(2)** Other plans and reports. Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

**(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 [31 USCS § 1115] 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)(1).

**(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.

## History

**HISTORY:**

Added Dec. 18, 2014, P. L. 113-283, § 2(a), 128 Stat. 3078; Dec. 18, 2015, P. L. 114-113, Div N, Title II, Subtitle B, § 229(b), 129 Stat. 2974; Dec. 21, 2018, P.L. 115-390, Title II, § 204(a)(2), 132 Stat. 5193.