

44 USCS § 3555

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)**

§ 3555. Annual independent evaluation

(a) In general.

- (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 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 of the effectiveness of the information security policies, procedures, and practices of the agency; and
 - (C)** separate presentations, as appropriate, regarding information security relating to national security systems.

(b) Independent auditor. Subject to subsection (c)—

- (1)** for each agency with an Inspector General appointed under chapter 4 of title 5 [5 USCS §§ 401 et seq.], 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) National security systems. 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) Existing evaluations. The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) Agency reporting.

- (1) 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.
- (2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) Protection of information. 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) OMB reports to Congress.

- (1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c) [44 USCS § 3553(c)].
- (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 National 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) Comptroller General. 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 [44 USCS §§ 3551 et seq.].

(i) Assessment technical assistance. The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

(j) Guidance. The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603 [44 USCS § 3603], the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

History

HISTORY:

§ 3555. Annual independent evaluation

Added Dec. 18, 2014, P. L. 113-283, § 2(a), 128 Stat. 3082; Dec. 27, 2022, P.L. 117-286, § 4(b)(89), 136 Stat. 4352.

United States Code Service

Copyright © 2024 All rights reserved.

End of Document