

tions conducted under this section in the report to Congress required under section 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.

(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, 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.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3082.)

#### 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, which is set out in the Appendix to Title 5, Government Organization and Employees.

#### PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3535 and 3545 of this title prior to repeal by Pub. L. 113–283.

### § 3556. Federal information security incident center

(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to—

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;

(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

(5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

#### PRIOR PROVISIONS

Provisions similar to this section were contained in section 3546 of this title prior to repeal by Pub. L. 113–283.

### § 3557. 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. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

#### PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3536 and 3547 of this title prior to repeal by Pub. L. 113–283.

### § 3558. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards<sup>1</sup> and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information

<sup>1</sup>So in original. Probably should be “National Institute of Standards”.