(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; amended Pub. L. 117–286, § 4(b)(89), Dec. 27, 2022, 136 Stat. 4352.)

Editorial Notes

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.

AMENDMENTS

2022—Subsec. (b)(1). Pub. L. 117–286 substituted ''chapter 4 of title 5,'' for ''the Inspector General Act of 1978,''.

§ 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.)

Editorial Notes

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.)

Editorial Notes

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.

Statutory Notes and Related Subsidiaries

ENFORCEMENT OF CYBERSECURITY REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS

Pub. L. 117–263, div. F, title LXIII, § 6309, Dec. 23, 2022, 136 Stat. 3506, as amended by Pub. L. 118–31, div. G, title III, § 7352, Dec. 22, 2023, 137 Stat. 1065, provided that:

''(a) DEFINITIONS.—In this section:

''(1) CYBERSECURITY REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS.—The term 'cybersecurity requirements for national security systems' means the minimum cybersecurity requirements established by the National Manager, consistent with the direction of the President and in consultation with the Director of National Intelligence, that applies to all national security systems operated by, on the behalf of, or administered by the head of an element of the intelligence community.

''(2) NATIONAL MANAGER.—The term 'National Manager' means the National Manager for National Security Systems designated by the President.

''(3) NATIONAL SECURITY SYSTEMS.—The term 'national security systems' includes—

''(A) national security systems (as defined in section 3552(b) of title 44, United States Code); and

''(B) information systems described in paragraph (2) or (3) of section 3553(e) of such title.

''(b) IMPLEMENTATION DEADLINE.—The cybersecurity requirements for national security systems shall include appropriate deadlines by which all elements of the intelligence community shall have fully implemented the requirements.

''(c) REEVALUATION AND UPDATES.—Not less frequently than once every 2 years, the National Manager shall reevaluate and update the cybersecurity requirements for national security systems.

''(d) RESOURCES.—Each head of an element of the intelligence community that owns or operates a national

security system shall update plans of the element to prioritize resources in such a manner as to fully implement the cybersecurity requirements for national security systems by the deadline established pursuant to subsection (b) for the next 10 fiscal years.

''(e) IMPLEMENTATION REPORT.—Each head of an element of the intelligence community that owns or operates a national security system shall submit to the congressional intelligence committees not later than 90 days after the date of the enactment of this subsection [Dec. 22, 2023] a plan detailing the cost and schedule requirements necessary to meet all of the cybersecurity requirements for national security systems by the end of fiscal year 2026.

''(f) EXEMPTIONS.—

''(1) IN GENERAL.—The head of an element of the intelligence community may exempt a national security system owned or operated by the element from the cybersecurity requirements for national security systems if done so in accordance with the procedures established under paragraph (2).

''(2) EXEMPTION PROCEDURES.—The National Manager shall, consistent with the direction of the President, establish procedures that govern—

''(A) the circumstances under which the head of an element of the intelligence community may exempt a national security system under paragraph (1); and

''(B) the process for implementing the exemption.

''(3) ANNUAL REPORTS ON EXEMPTIONS.—

''(A) IN GENERAL.—Each year, the National Manager and the Director of National Intelligence shall—

''(i) submit to the congressional intelligence committees an annual report documenting all exemptions made under paragraph (1) during the period covered by the report, along with the justifications for the exemptions; and

''(ii) in the case of an exemption made by the Assistant Secretary of State for Intelligence and Research under such paragraph, submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a separate report describing the exemption and the justification for it.

''(B) MANNER.—Each report submitted under subparagraph (A) shall be submitted with such classification as the Director considers appropriate and with due regard for the protection of sensitive intelligence sources and methods.''

[For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in section 6309 of Pub. L. 117–263, set out above, see section 3003 of Title 50, War and National Defense, as made applicable by section 6002 of Pub. L. 117–263, which is set out as a note under section 3003 of Title 50.]

§ 3558. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards[1] 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 under section 552 of title 5, the management and disposition of records under chapters[2] 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.

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

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3538 and 3549 of this title prior to repeal by Pub. L. 113–283.

§ 3559. Federal websites required to be mobile friendly

(a) IN GENERAL.—If, on or after the date that is 180 days after the date of the enactment of this section, an agency creates a website that is intended for use by the public or conducts a redesign of an existing legacy website that is intended for use by the public, the agency shall ensure to the greatest extent practicable that the website is mobile friendly.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5.

(2) MOBILE FRIENDLY.—The term ''mobile friendly'' means, with respect to a website, that the website is configured in such a way that the website may be navigated, viewed, and accessed on a smartphone, tablet computer, or similar mobile device.

(Added Pub. L. 115–114, §2(a), Jan. 10, 2018, 131 Stat. 2278.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of this section, referred to in subsec. (a), is the date of enactment of Pub. L. 115–114, which was approved Jan. 10, 2018.

SUBCHAPTER III—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

Editorial Notes

PRIOR PROVISIONS

Provisions similar to those in parts A to C of this subchapter were contained in Pub. L. 107–347, title V, Dec. 17, 2002, 116 Stat. 2962, which was set out as a note under section 3501 of this title, prior to repeal by Pub. L. 115–435, title III, §302(c)(1), title IV, §403, Jan. 14, 2019, 132 Stat. 5552, 5557, effective 180 days after Jan. 14, 2019.

PART A—GENERAL

§ 3561. Definitions

In this subchapter:

(1) AGENCY.—The term ''agency'' means any entity that falls within the definition of the term ''executive agency'', as defined in section 102 of title 31, or ''agency'', as defined in section 3502.

(2) AGENT.—The term ''agent'' means an individual—

(A)(i) who is an employee of a private organization or a researcher affiliated with an

[1] So in original. Probably should be ''National Institute of Standards''.

[2] So in original. Probably should be ''chapter''.