44 USC CHAPTER 35, SUBCHAPTER II: INFORMATION SECURITY

From Title 44—PUBLIC PRINTING AND DOCUMENTS
CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

SUBCHAPTER II—INFORMATION SECURITY

§3551. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3073.)

Editorial Notes

Prior Provisions

Provisions similar to this section were contained in sections 3531 and 3541 of this title prior to repeal by Pub. L. 113–283.

Statutory Notes and Related Subsidiaries

Cybersecurity Improvements to Agency Information Systems

Pub. L. 114–4, title V, §547, Mar. 4, 2015, 129 Stat. 69, provided that:

"(a) Of the amounts made available by this Act [Pub. L. 114–4, see Tables for classification] for 'National Protection and Programs Directorate, Infrastructure Protection and Information Security', $140,525,000 for the Federal Network Security program, project, and activity shall be used to deploy on Federal systems technology to improve the information security of agency information systems covered by [former] section 3543(a) of title 44, United States Code [see now 44 U.S.C. 3553]: *Provided*, That funds made available under this section shall be used to assist and support Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity to address escalating and rapidly evolving threats to information security, including the acquisition and operation of a continuous monitoring and diagnostics program, in collaboration with departments and agencies, that includes equipment, software, and Department of Homeland Security supplied services: *Provided further*, That continuous monitoring and diagnostics software procured by the funds made available by this section shall not transmit to the Department of Homeland Security any personally identifiable information or content of network communications of other agencies' users: *Provided further*, That such software shall be installed, maintained, and operated in accordance with all applicable privacy laws and agency-specific policies regarding network content.

"(b) Funds made available under this section may not be used to supplant funds provided for any such system within an agency budget.

"(c) Not later than July 1, 2015, the heads of all Federal agencies shall submit to the Committees on Appropriations of the Senate and the House of Representatives expenditure plans for necessary

cybersecurity improvements to address known vulnerabilities to information systems described in subsection (a).

"(d) Not later than October 1, 2015, and semiannually thereafter, the head of each Federal agency shall submit to the Director of the Office of Management and Budget a report on the execution of the expenditure plan for that agency required by subsection (c): *Provided*, That the Director of the Office of Management and Budget shall summarize such execution reports and annually submit such summaries to Congress in conjunction with the annual progress report on implementation of the E-Government Act of 2002 (Public Law 107–347) [see Tables for classification], as required by section 3606 of title 44, United States Code.

"(e) This section shall not apply to the legislative and judicial branches of the Federal Government and shall apply to all Federal agencies within the executive branch except for the Department of Defense, the Central Intelligence Agency, and the Office of the Director of National Intelligence."

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 113–76, div. F, title V, §554, Jan. 17, 2014, 128 Stat. 278.

Pub. L. 113–6, div. D, title V, §558, Mar. 26, 2013, 127 Stat. 377.

§3552. Definitions

(a) In General.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) Additional Definitions.—As used in this subchapter:

(1) The term "binding operational directive" means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

(2) The term "incident" means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(3) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(4) The term "information technology" has the meaning given that term in section 11101 of title 40.

(5) The term "intelligence community" has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(7) The term "Secretary" means the Secretary of Homeland Security.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3074.)

Editorial Notes

Prior Provisions

Provisions similar to this section were contained in sections 3532 and 3542 of this title prior to repeal by Pub. L. 113–283.

§3553. Authority and functions of the Director and the Secretary

(a) Director.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) Secretary.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

(C) requirements for the mitigation of exigent risks to information systems; and

(D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

(3) monitoring agency implementation of information security policies and practices;

(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

(A) operating the Federal information security incident center established under section 3556;

(B) upon request by an agency, deploying, operating, and maintaining technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems;

(7) hunting for and identifying, with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems;

(8) upon request by an agency, and at the Secretary's discretion, with or without reimbursement—

(A) providing services, functions, and capabilities, including operation of the agency's information security program, to assist the agency with meeting the requirements set forth in section 3554(b); and

(B) deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information; and

(9) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

(c) Report.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

(d) National Security Systems.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) Department of Defense and Intelligence Community Systems.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

(f) Consideration.—

(1) In general.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.[1]

(2) Directives.—The Secretary shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.[1]

(3) Rule of construction.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.[1]

(g) Exercise of Authority.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

(h) Direction to Agencies.—

(1) AUTHORITY.—
(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.
(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—
(A) in coordination with the Director, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—
(i) thresholds and other criteria;
(ii) privacy and civil liberties protections; and
(iii) providing notice to potentially affected third parties;

(B) specify the reasons for the required action and the duration of the directive;
(C) minimize the impact of a directive under this subsection by—
(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and
(ii) limiting directives to the shortest period practicable;

(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;
(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;
(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;
(G) consider any applicable standards or guidelines developed by the National Institute of Standards and Technology issued by the Secretary of Commerce under section 11331 of title 40; and
(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

(3) IMMINENT THREATS.—
(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use under this subsection of the intrusion detection and prevention capabilities established under section 230(b)(1) [1] of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—
(i) the Secretary determines there is an imminent threat to agency information systems;
(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;
(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of the intrusion detection and prevention capabilities under the control of the Secretary;
(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—
(I) any action taken under this paragraph; and
(II) the reasons for and duration and nature of the action;

(v) the action of the Secretary is consistent with applicable law; and
(vi) the Secretary authorizes the use of the intrusion detection and prevention capabilities in accordance with the advance procedures established under subparagraph (C).

(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated by the Secretary.
(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of the intrusion detection and prevention capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

(4) Limitation.—The Secretary may direct or authorize lawful action or the use of the intrusion detection and prevention capabilities under this subsection only to—

(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

(B) require the remediation of or protect against identified information security risks with respect to—

(i) information collected or maintained by or on behalf of an agency; or

(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

(i) Annual Report to Congress.—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

(j) Rule of Construction.—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).

(k) Appropriate Congressional Committees Defined.—In this section, the term "appropriate congressional committees" means—

(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

(l) Information Sharing.—

(1) In general.—Notwithstanding any other provision of law, including any provision of law that would otherwise restrict or prevent the head of an agency from disclosing information to the Secretary, the Secretary in carrying out this section and title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) may access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks.

(2) Exception.—Paragraph (1) shall not apply to national security systems or to information systems described in paragraph (2) or (3) of subsection (e).

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3075; amended Pub. L. 114–113, div. N, title II, §§224(e), 229(a), Dec. 18, 2015, 129 Stat. 2967, 2972; Pub. L. 115–390, title II, §204(a)(1), Dec. 21, 2018, 132 Stat. 5192; Pub. L. 116–92, div. E, title LXIV, §6432, Dec. 20, 2019, 133 Stat. 2200; Pub. L. 116–283, div. A, title XVII, §1705, Jan. 1, 2021, 134 Stat. 4082.)

Editorial Notes

References in Text

Section 11331 of title 40, referred to in subsec. (f), was generally amended by both Pub. L. 107–347 and Pub. L. 107–296. As amended by Pub. L. 107–347, effective Dec. 17, 2002, section 11331 of title 40 provided for the prescription by the Secretary of Commerce of standards and guidelines pertaining to Federal information systems. See 2002 Amendment note under that section. As amended by Pub. L. 107–296, effective 60 days after Nov. 25, 2002, section 11331 of title 40 provided for the promulgation by the Director of the Office of Management and Budget of information security standards pertaining to Federal information systems.

Section 230(b)(1) of the Homeland Security Act of 2002, referred to in subsec. (h)(3)(A), is section 230(b)(1) of title II of Pub. L. 107–296, as added by Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which was redesignated section 2213(b)(1) of Pub. L. 107–296 by section 2(g)(2)(I) of Pub. L. 115–278, Nov. 16, 2018, 132 Stat. 4178, and is classified to section 663(b)(1) of Title 6, Domestic Security.

The Homeland Security Act of 2002, referred to in subsec. (l)(1), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135. Title XXII of the Act is classified generally to subchapter XVIII (§651 et seq.) of chapter 1 of Title 6, Domestic Security. For complete classification of this Act to the Code, see Short Title note set out under section 101 of Title 6 and Tables.

Prior Provisions

Provisions similar to this section were contained in sections 3533 and 3543 of this title prior to repeal by Pub. L. 113–283.

Amendments

2021—Subsec. (b)(7) to (9). Pub. L. 116–283, §1705(1), added pars. (7) and (8) and redesignated former par. (7) as (9).

Subsec. (l). Pub. L. 116–283, §1705(2), added subsec. (l).

2019—Subsecs. (j), (k). Pub. L. 116–92 added subsec. (j) and redesignated former subsec. (j) as (k).

2018—Subsec. (a)(5). Pub. L. 115–390 inserted "and section 1326 of title 41" after "compliance with the requirements of this subchapter".

2015—Subsec. (b)(6)(B). Pub. L. 114–113, §224(e), inserted ", operating, and maintaining" after "deploying".

Subsecs. (h) to (j). Pub. L. 114–113, §229(a), added subsecs. (h) to (j).

Statutory Notes and Related Subsidiaries

Change of Name

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019.

Effective Date of 2018 Amendment

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of this title.

Construction

Pub. L. 115–390, title II, §204(b), Dec. 21, 2018, 132 Stat. 5193, provided that: "Nothing in this title [see section 201 of Pub. L. 115–390, set out as a Short Title of 2018 note under section 101 of Title 41, Public Contracts] shall be construed to alter or impede any authority or responsibility under section 3553 of title 44, United States Code."

Breaches

Pub. L. 113–283, §2(d), Dec. 18, 2014, 128 Stat. 3085, provided that:

"(1) Requirements.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

"(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall—

"(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

"(ii) include—

"(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

"(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

"(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

"(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

"(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

"(2) National security; law enforcement; remediation.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

"(3) Reports.—

"(A) Director of omb.—During the first 2 years beginning after the date of enactment of this Act [Dec. 18, 2014], the Director of the Office of Management and Budget shall, on an annual basis—

"(i) assess agency implementation of data breach notification policies and guidelines in aggregate; and

"(ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code.

"(B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.

"(4) EXCEPTION.—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

"(5) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to alter any authority of a Federal agency or department."

Similar provisions were contained in Pub. L. 113–282, §7(b), Dec. 18, 2014, 128 Stat. 3071.

[1] *See References in Text note below.*

§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, subchapter III of chapter 13 of title 41, and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40;

(ii) operational directives developed by the Secretary under section 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); and

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; 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, 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 3553 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;

(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 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;

(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); [1]

(B) may include testing relied on in an evaluation under section 3555; and

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

(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);

(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; 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) 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 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.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3078; amended Pub. L. 114–113, div. N, title II, §229(b), Dec. 18, 2015, 129 Stat. 2974; Pub. L. 115–390, title II, §204(a)(2), Dec. 21, 2018, 132 Stat. 5193.)

EDITORIAL NOTES

Prior Provisions

Provisions similar to this section were contained in sections 3534 and 3544 of this title prior to repeal by Pub. L. 113–283.

Amendments

2018—Subsec. (a)(1)(B). Pub. L. 115–390, §204(a)(2)(A), inserted ", subchapter III of chapter 13 of title 41," after "complying with the requirements of this subchapter" in introductory provisions.

Subsec. (a)(1)(B)(vi). Pub. L. 115–390, §204(a)(2)(B), (C), added cl. (vi).

2015—Subsec. (a)(1)(B)(v). Pub. L. 114–113 added cl. (v).

Statutory Notes and Related Subsidiaries

Effective Date of 2018 Amendment

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of Title 41, Public Contracts.

Major Incident

Pub. L. 113–283, §2(b), Dec. 18, 2014, 128 Stat. 3085, provided that: "The Director of the Office of Management and Budget shall—

"(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

"(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued."

[1] *So in original. Section 3505 contains two subsecs. (c).*

§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 the Inspector General Act of 1978, 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).

(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.)

Editorial Notes

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.)

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.

§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.

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

[2] *So in original. Probably should be "chapter".*

§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.