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.

(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.

(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.

(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—

[1] See References in Text note below.

(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 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. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

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.''

NO TIKTOK ON GOVERNMENT DEVICES

Pub. L. 117–328, div. R, Dec. 29, 2022, 136 Stat. 5258, provided that:

''SEC. 101. SHORT TITLE.

''This division may be cited as the 'No TikTok on Government Devices Act'.

''SEC. 102. PROHIBITION ON THE USE OF TIKTOK.

''(a) DEFINITIONS.—In this section—

''(1) the term 'covered application' means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited;

''(2) the term 'executive agency' has the meaning given that term in section 133 of title 41, United States Code; and

''(3) the term 'information technology' has the meaning given that term in section 11101 of title 40, United States Code.

''(b) PROHIBITION ON THE USE OF TIKTOK.—

''(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act [Dec. 29, 2022], the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the Secretary of Defense, and consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code, shall develop standards and guidelines for executive agencies requiring the removal of any covered application from information technology.

''(2) NATIONAL SECURITY AND RESEARCH EXCEPTIONS.—The standards and guidelines developed under paragraph (1) shall include—

''(A) exceptions for law enforcement activities, national security interests and activities, and security researchers; and

''(B) for any authorized use of a covered application under an exception, requirements for executive agencies to develop and document risk mitigation actions for such use.''

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.

§ 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;