(iv) a list by agency of compliance with the requirements of section 1523(b) of this title; and

(C) not later than 1 year after December 18, 2015, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 1522(a)(2) of this title; and

(ii) the improved metrics developed pursuant to section 1522(c) of this title.

(d) Form

Each report required under this section shall be submitted in unclassified form, but may include a classified annex.

(Pub. L. 114–113, div. N, title II, §226, Dec. 18, 2015, 129 Stat. 2969; Pub. L. 115–278, §2(h)(1)(F), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–263, div. G, title LXXI, §7143(d)(1)(B), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes

REFERENCES IN TEXT

Subtitle D of title II of the Homeland Security Act of 2002, referred to in subsec. (c)(1)(C)(ii), is subtitle D (§§231–237) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2159, which enacted part D (§161 et seq.) of subchapter II of chapter 1 of this title and amended sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement. Subtitle D was redesignated subtitle C of title II of the Homeland Security Act of 2002 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and is classified principally to part C (§161 et seq.) of subchapter II of chapter 1 of this title. For complete classification of subtitle C to the Code, see Tables.

AMENDMENTS

2022—Subsec. (a)(2). Pub. L. 117–263 substituted ''section 650 of this title'' for ''section 1501 of this title''.

2018—Subsec. (a)(1). Pub. L. 115–278, §2(h)(1)(F)(i)(I), substituted ''section 2213'' for ''section 230'' and struck out before period at end '', as added by section 223(a)(6) of this division''.

Subsec. (a)(4). Pub. L. 115–278, §2(h)(1)(F)(i)(II), substituted ''section 2210(b)(1)'' for ''section 228(b)(1)'' and struck out before period at end '', as added by section 223(a)(4) of this division''.

Subsec. (a)(5). Pub. L. 115–278, §2(h)(1)(F)(i)(III), substituted ''section 2213(b)'' for ''section 230(b)'' and struck out before period at end '', as added by section 223(a)(6) of this division''.

Subsec. (c)(1)(A)(vi). Pub. L. 115–278, §2(h)(1)(F)(ii), substituted ''section 2213(c)(5)'' for ''section 230(c)(5)'' and struck out '', as added by section 223(a)(6) of this division'' after ''Homeland Security Act of 2002''.

§ 1525. Termination

(a) In general

The authority provided under section 663 of this title, and the reporting requirements under section 1524(c) of this title shall terminate on March 14, 2025.

(b) Rule of construction

Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 663(d)(2)[1] of this title, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

(Pub. L. 114–113, div. N, title II, §227, Dec. 18, 2015, 129 Stat. 2971; Pub. L. 115–278, §2(h)(1)(G), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–328, div. O, title I, §101, Dec. 29, 2022, 136 Stat. 5226; Pub. L. 118–47, div. G, title I, §106, Mar. 23, 2024, 138 Stat. 857; Pub. L. 118–83, div. B, title I, §103, Sept. 26, 2024, 138 Stat. 1534; Pub. L. 118–158, div. E, §5104, Dec. 21, 2024, 138 Stat. 1771.)

[1] So in original. Probably should be ''663(c)(2)''.

Editorial Notes

AMENDMENTS

2024—Subsec. (a). Pub. L. 118–158 substituted ''March 14, 2025'' for ''December 20, 2024''.

Pub. L. 118–83 substituted ''December 20, 2024'' for ''September 30, 2024''.

Pub. L. 118–47 substituted ''September 30, 2024'' for ''September 30, 2023''.

2022—Subsec. (a). Pub. L. 117–328 substituted ''September 30, 2023'' for ''the date that is 7 years after December 18, 2015''.

2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(G)(i), substituted ''section 663 of this title'' for ''section 151 of this title, as added by section 223(a)(6) of this division,''.

Subsec. (b). Pub. L. 115–278, §2(h)(1)(G)(ii), substituted ''section 663(d)(2) of this title'' for ''section 151(d)(2) of this title, as added by section 223(a)(6) of this division,''.

§ 1526. Inventory of cryptographic systems; migration to post-quantum cryptography

(a) Inventory

(1) Establishment

Not later than 180 days after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall issue guidance on the migration of information technology to post-quantum cryptography, which shall include at a minimum—

(A) a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers, prioritized using the criteria described in subparagraph (B);

(B) criteria to allow agencies to prioritize their inventory efforts; and

(C) a description of the information required to be reported pursuant to subsection (b).

(2) Additional content in guidance

In the guidance established by paragraph (1), the Director of OMB shall include, in addition to the requirements described in that paragraph—

(A) a description of information technology to be prioritized for migration to post-quantum cryptography; and

(B) a process for evaluating progress on migrating information technology to post-quantum cryptography, which shall be automated to the greatest extent practicable.

(3) Periodic updates

The Director of OMB shall update the guidance required under paragraph (1) as the Director of OMB determines necessary, in coordination with the National Cyber Director and in consultation with the Director of CISA.

(b) Agency reports

Not later than 1 year after December 21, 2022, and on an ongoing basis thereafter, the head of

each agency shall provide to the Director of OMB, the Director of CISA, and the National Cyber Director—

(1) the inventory described in subsection (a)(1); and

(2) any other information required to be reported under subsection (a)(1)(C).

(c) Migration and assessment

Not later than 1 year after the date on which the Director of NIST has issued post-quantum cryptography standards, the Director of OMB shall issue guidance requiring each agency to—

(1) prioritize information technology described under subsection (a)(2)(A) for migration to post-quantum cryptography; and

(2) develop a plan to migrate information technology of the agency to post-quantum cryptography consistent with the prioritization under paragraph (1).

(d) Interoperability

The Director of OMB shall ensure that the prioritizations made under subsection (c)(1) are assessed and coordinated to ensure interoperability.

(e) Office of Management and Budget reports

(1) Report on post-quantum cryptography

Not later than 15 months after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report on the following:

(A) A strategy to address the risk posed by the vulnerabilities of information technology of agencies to weakened encryption due to the potential and possible capability of a quantum computer to breach that encryption.

(B) An estimate of the amount of funding needed by agencies to secure the information technology described in subsection (a)(1)(A) from the risk posed by an adversary of the United States using a quantum computer to breach the encryption of the information technology.

(C) A description of Federal civilian executive branch coordination efforts led by the National Institute of Standards and Technology, including timelines, to develop standards for post-quantum cryptography, including any Federal Information Processing Standards developed under chapter 35 of title 44, as well as standards developed through voluntary, consensus standards bodies such as the International Organization for Standardization.

(2) Report on migration to post-quantum cryptography in information technology

Not later than 1 year after the date on which the Director of OMB issues guidance under subsection (c)(2), and thereafter until the date that is 5 years after the date on which post-quantum cryptographic standards are issued, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, with the report submitted pursuant to section 3553(c) of title 44, a report on the progress of agencies in adopting post-quantum cryptography standards.

(Pub. L. 117–260, § 4, Dec. 21, 2022, 136 Stat. 2390.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Quantum Computing Cybersecurity Preparedness Act, and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

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.

FINDINGS; SENSE OF CONGRESS

Pub. L. 117–260, § 2, Dec. 21, 2022, 136 Stat. 2389, provided that:

''(a) FINDINGS.—Congress finds the following:

''(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

''(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

''(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

''(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

''(b) SENSE OF CONGRESS.—It is the sense of Congress that—

''(1) a strategy for the migration of information technology of the Federal Government to post-quantum cryptography is needed; and

''(2) the governmentwide and industrywide approach to post-quantum cryptography should prioritize developing applications, hardware intellectual property, and software that can be easily updated to support cryptographic agility.''

EXEMPTION OF NATIONAL SECURITY SYSTEMS

Pub. L. 117–260, § 5, Dec. 21, 2022, 136 Stat. 2392, provided that: ''This Act [see Short Title of 2022 Amendment note set out under section 1500 of this title] shall not apply to any national security system.''

DEFINITIONS

Pub. L. 117–260, § 3, Dec. 21, 2022, 136 Stat. 2389, provided that: ''In this Act [see Short Title of 2022 Amendment note set out under section 1500 of this title]:

''(1) AGENCY .—The term 'agency'—

''(A) means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

''(B) does not include—

''(i) the Government Accountability Office; or

''(ii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions.

''(2) CLASSICAL COMPUTER.—The term 'classical computer' means a device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed and encodes information in binary bits that can either be 0s or 1s.

''(3) DIRECTOR OF CISA.—The term 'Director of CISA' means the Director of the Cybersecurity and Infrastructure Security Agency.

''(4) DIRECTOR OF NIST.—The term 'Director of NIST' means the Director of the National Institute of Standards and Technology.

''(5) DIRECTOR OF OMB.—The term 'Director of OMB' means the Director of the Office of Management and Budget.

''(6) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 3502 of title 44, United States Code.

''(7) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44, United States Code.

''(8) POST-QUANTUM CRYPTOGRAPHY.—The term 'post-quantum cryptography' means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a quantum computer or classical computer.

''(9) QUANTUM COMPUTER.—The term 'quantum computer' means a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations.''

SUBCHAPTER III—OTHER CYBER MATTERS

§ 1531. Apprehension and prosecution of international cyber criminals

(a) International cyber criminal defined

In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) Consultations for noncooperation

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) Annual report

(1) In general

The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) Form

The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) Appropriate congressional committees

For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(Pub. L. 114–113, div. N, title IV, § 403, Dec. 18, 2015, 129 Stat. 2979.)

§ 1532. Enhancement of emergency services

(a) Collection of data

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, acting through the center established under section 659 of this title, in coordination with appropriate Federal entities and the Assistant Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 101 of this title) within the State.

(b) Analysis of data

Not later than 1 year after December 18, 2015, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration