

submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) Contents

The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) Form of report

The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) Intelligence community defined

In this section, the term “intelligence community” has the meaning given that term in section 3003 of title 50.

(Pub. L. 114–113, div. N, title I, § 109, Dec. 18, 2015, 129 Stat. 2955.)

§ 1509. Exception to limitation on authority of Secretary of Defense to disseminate certain information

Notwithstanding subsection (c)(3) of section 393 of title 10, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this subchapter.

(Pub. L. 114–113, div. N, title I, § 110, Dec. 18, 2015, 129 Stat. 2956.)

§ 1510. Effective period

(a) In general

Except as provided in subsection (b), this subchapter and the amendments made by this subchapter shall be effective during the period beginning on December 18, 2015 and ending on September 30, 2025.

(b) Exception

With respect to any action authorized by this subchapter or information obtained pursuant to an action authorized by this subchapter, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this subchapter shall continue in effect.

(Pub. L. 114–113, div. N, title I, § 111, Dec. 18, 2015, 129 Stat. 2956.)

Editorial Notes

REFERENCES IN TEXT

The amendments made by this subchapter, referred to in subsec. (a), was in the original “the amendments made by this title”, meaning title I of div. N of Pub. L. 114–113, which is classified generally to this subchapter.

**SUBCHAPTER II—FEDERAL
CYBERSECURITY ENHANCEMENT**

§ 1521. Definitions

In this subchapter:

(1) Agency

The term “agency” has the meaning given the term in section 3502 of title 44.

(2) Agency information system

The term “agency information system” has the meaning given the term in section 660 of this title.

(3) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the Committee on Homeland Security and Governmental Affairs of the Senate; and
- (B) the Committee on Homeland Security of the House of Representatives.

(4) Cybersecurity risk; information system

The terms “cybersecurity risk” and “information system” have the meanings given those terms in section 650 of this title.

(5) Director

The term “Director” means the Director of the Office of Management and Budget.

(6) Intelligence community

The term “intelligence community” has the meaning given the term in section 3003(4) of title 50.

(7) National security system

The term “national security system” has the meaning given the term in section 11103 of title 40.

(8) Secretary

The term “Secretary” means the Secretary of Homeland Security.

(Pub. L. 114–113, div. N, title II, §222, Dec. 18, 2015, 129 Stat. 2963; Pub. L. 115–278, §2(h)(1)(D), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–263, div. G, title LXXI, §7143(d)(1)(A), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, which is classified principally to this subchapter. For complete classification of subtitle B to the Code, see Tables.

AMENDMENTS

2022—Par. (4). Pub. L. 117–263 substituted “section 650 of this title” for “section 659 of this title”.

2018—Par. (2). Pub. L. 115–278, §2(h)(1)(D)(i), substituted “section 660 of this title” for “section 149 of this title, as added by section 223(a)(4) of this division”.

Par. (4). Pub. L. 115–278, §2(h)(1)(D)(ii), substituted “section 659 of this title” for “section 148 of this title, as so redesignated by section 223(a)(3) of this division”.

§ 1522. Advanced internal defenses

(a) Advanced network security tools

(1) In general

The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

(2) Development of plan

The Director shall develop and the Secretary shall implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) Prioritizing advanced security tools

The Director and the Secretary, in consultation with appropriate agencies, shall—

- (1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and
- (2) brief appropriate congressional committees on such prioritization and use.

(c) Improved metrics

The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44 to include measures of intrusion and incident detection and response times.

(d) Transparency and accountability

The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro-agencies.

(e) Omitted

(f) Exception

The requirements under this section shall not apply to the Department of Defense, a national

security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, §224, Dec. 18, 2015, 129 Stat. 2967.)

Editorial Notes

CODIFICATION

Section is comprised of section 224 of title II of div. N of Pub. L. 114–113. Subsec. (e) of section 224 of title II of div. N of Pub. L. 114–113 amended section 3553 of Title 44, Public Printing and Documents.

§ 1523. Federal cybersecurity requirements

(a) Implementation of Federal cybersecurity standards

Consistent with section 3553 of title 44, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40¹ for securing agency information systems.

(b) Cybersecurity requirements at agencies

(1) In general

Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section 11331 of title 40 and except as provided in paragraph (2), not later than 1 year after December 18, 2015, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals’ need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 7464 of title 15, including multi-factor authentication, for—

- (i) remote access to an agency information system; and
- (ii) each user account with elevated privileges on an agency information system.

(2) Exception

The requirements under paragraph (1) shall not apply to an agency information system for which—

¹ See References in Text note below.

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) Construction

Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114-113, div. N, title II, §225, Dec. 18, 2015, 129 Stat. 2967.)

Editorial Notes

REFERENCES IN TEXT

The text of section 11331 of title 40, referred to in subsec. (a), was generally amended by Pub. L. 117-167, div. B, title II, §10246(f), Aug. 9, 2022, 136 Stat. 1492, so as to provide for the prescription by the Secretary of Commerce of standards and guidelines pertaining to Federal information systems.

§ 1524. Assessment; reports

(a) Definitions

In this section:

(1) Agency information

The term “agency information” has the meaning given the term in section 2213 of the Homeland Security Act of 2002 [6 U.S.C. 663].

(2) Cyber threat indicator; defensive measure

The terms “cyber threat indicator” and “defensive measure” have the meanings given those terms in section 650 of this title.

(3) Intrusion assessments

The term “intrusion assessments” means actions taken under the intrusion assessment

plan to identify and remove intruders in agency information systems.

(4) Intrusion assessment plan

The term “intrusion assessment plan” means the plan required under section 2210(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 660(b)(1)].

(5) Intrusion detection and prevention capabilities

The term “intrusion detection and prevention capabilities” means the capabilities required under section 2213(b) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)].

(b) Third-party assessment

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) Reports to Congress

(1) Intrusion detection and prevention capabilities

(A) Secretary of Homeland Security report

Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 2213(c)(5) of the Homeland

Security Act of 2002 [6 U.S.C. 663(c)(5)], including the number of new technologies tested and the number of participating agencies.

(B) OMB report

Not later than 18 months after December 18, 2015, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(C) Chief information officer

Not earlier than 18 months after December 18, 2015, and not later than 2 years after December 18, 2015, the Federal Chief Information Officer shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities, including—

(i) the effectiveness of the system in detecting, disrupting, and preventing cyber-threat actors, including advanced persistent threats, from accessing agency information and agency information systems;

(ii) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed under subtitle D¹ of title II of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) are effective in securing Federal information systems;

(iii) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools and including the value of classified cyber threat indicators; and

(iv) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

¹ See References in Text note below.

(2) OMB report on development and implementation of intrusion assessment plan, advanced internal defenses, and Federal cybersecurity requirements

The Director shall—

(A) not later than 6 months after December 18, 2015, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after December 18, 2015, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) a description of the advanced network security tools included in the efforts to continuously diagnose and mitigate cybersecurity risks pursuant to section 1522(a)(1) of this title; and

(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 September 30, 2023.

(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.)

Editorial Notes

AMENDMENTS

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 Tech-

¹ So in original. Probably should be “663(c)(2)”.

nology, 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

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