Quantum Computing Cybersecurity Preparedness Act

[Public Law 117–260]

[This law has not been amended]

[Currency: This publication is a compilation of the text of Public Law 117-260. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at https://www.govinfo.gov/app/collection/comps/]

[Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).]

AN ACT To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. [6 U.S.C. 1500 note] SHORT TITLE.

This Act may be cited as the "Quantum Computing Cybersecurity Preparedness Act".

SEC. 2. [6 U.S.C. 1526 note] FINDINGS; SENSE OF CONGRESS.

(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 appli-

cations, hardware intellectual property, and software that can be easily updated to support cryptographic agility.

SEC. 3. [6 U.S.C. 1526 note] DEFINITIONS.

In this Act:

(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.

SEC. 4. [6 U.S.C. 1526] INVENTORY OF CRYPTOGRAPHIC SYSTEMS; MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.

(a) INVENTORY.—

(1) ESTABLISHMENT. Not later than 180 days after the date of enactment of this Act, 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 the date of enactment of this Act, 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 the date of enactment of this Act, 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, United States Code, 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, United States Code, a report on the progress of agencies in adopting post-quantum cryptography standards.

SEC. 5. [6 U.S.C. 1526 note] EXEMPTION OF NATIONAL SECURITY SYSTEMS.

This Act shall not apply to any national security system.

SEC. 6. DETERMINATION OF BUDGETARY EFFECTS.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the House Budget Committee, provided that such statement has been submitted prior to the vote on passage.