II

Calendar No. 635

117TH CONGRESS
2D SESSION

S. 4592

[Report No. 117–251]

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

IN THE SENATE OF THE UNITED STATES

JULY 21, 2022

Ms. HASSAN (for herself, Mr. PORTMAN, Ms. ROSEN, Mr. TILLIS, Mr. YOUNG, and Mr. HEINRICH) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 13, 2022

Reported by Mr. PETERS, with an amendment

[Insert the part printed in italic]

A BILL

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. SHORT TITLE.

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

SEC. 2. 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 systems 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.

SEC. 3. DEFINITIONS.

In this Act:

(1) 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.

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

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

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

(5) EXECUTIVE AGENCY.—The term ''executive agency'' has the meaning given the term ''Executive

agency'' in section 105 of title 5, United States Code.

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

(7) POST-QUANTUM CRYPTOGRAPHY.—The term ''post-quantum cryptography'' means a cryptographic system that—

(A) is secure against decryption attempts using a quantum computer or classical computer; and

(B) can interoperate with existing communications protocols and networks.

(8) QUANTUM COMPUTER.—The term ''quantum computer'' means a computer that uses the collective properties of quantum states to perform calculations.

SEC. 4. 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 shall establish, by rule or binding guidance, a requirement for each executive agency to establish

and maintain an inventory of each cryptographic system in use by the agency.

(2) ADDITIONAL CONTENT IN RULE OR BINDING GUIDANCE.—In the rule or binding guidance established by paragraph (1), the Director of OMB shall include, in addition to the requirement described under that paragraph—

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

(B) a description of the information required to be reported pursuant to subsection (b); and

(C) 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 rule or binding guidance established by paragraph (1) as the Director determines necessary.

(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 executive agency shall provide to the Director of OMB, the Director of CISA, and the

National Cyber Director an inventory of all information technology in use by the executive agency that is vulnerable to decryption by quantum computers, prioritized pursuant to the guidance issued under subsection (a)(2).

(c) MIGRATION AND ASSESSMENT.—

(1) MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.—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 executive agency to develop a plan to migrate information technology of the agency to post-quantum cryptography.

(2) DESIGNATION OF SYSTEMS FOR MIGRATION.—Not later than 90 days after the date on which the guidance required by paragraph (1) has been issued, the Director of OMB shall issue guidance for *executive* agencies to—

(A) designate information technology to be migrated to post-quantum cryptography; and

(B) prioritize information technology designated under subparagraph (A), on the basis of the amount of risk posed by decryption by quantum computers to that technology, for migration to post-quantum cryptography.

(d) INTEROPERABILITY.—The Director of OMB shall ensure that the designations and prioritizations made under subsection (c)(2) are assessed and coordinated to ensure interoperability.

(e) REPORT ON POST-QUANTUM CRYPTOGRAPHY.—Not later than 15 months after the date of enactment of this Act, the Director of OMB shall submit to Congress a report on the following:

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

(2) The amount of funding needed by executive agencies to secure the information technology systems described in paragraph (1) from the risk posed by an adversary of the United States using a quantum computer to breach the encryption of information technology systems.

(3) 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.

(f) REPORT ON MIGRATION TO POST-QUANTUM CRYPTOGRAPHY IN INFORMATION TECHNOLOGY SYSTEMS.—Not later than 1 year after the date on which the Director of OMB issues guidance under subsection (c)(2), and annually thereafter until the date that is 5 years after the date on which post-quantum cryptographic standards are issued, the Director of OMB shall submit to Congress, with the report submitted pursuant to section 3553(c) of title 44, United States Code, a report on the progress of executive agencies in adopting post-quantum cryptography standards.

SEC. 5. 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.

Calendar No. 635

117TH CONGRESS
2D SESSION

S. 4592

[Report No. 117–251]

A BILL

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

DECEMBER 13, 2022

Reported with an amendment