I

117TH CONGRESS
2D SESSION

H. R. 7535

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

IN THE HOUSE OF REPRESENTATIVES

APRIL 18, 2022

Mr. KHANNA (for himself, Ms. MACE, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Oversight and Reform

---

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.—The Congress finds the following:

(1) Cryptography is essential for our national security and the functioning of our economy.

(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 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 (IP), and software that can be easily updated to support developing cryptographic agility.

SEC. 3. MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.

(a) 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, in consultation with the Chief Information Officers Council, shall begin to prioritize the migration to post-quantum cryptography and assessment of information technology systems of executive agencies that does not use post-quantum cryptography, including digital signatures.

(2) DESIGNATION OF SYSTEMS FOR MIGRATION.—Not later than 1 year after the date on which post-quantum cryptography standards have been set by NIST and on an ongoing basis thereafter, the Director of OMB, in consultation with the Chief Information Officers Council, shall designate and prioritize for migration to post-quantum cryptography information technology systems of executive agencies based on the risk of systems that do not use post-quantum cryptography.

(b) REPORT ON POST-QUANTUM CRYPTOGRAPHY.—Not later than 1 year after the date of the enactment of this section, 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 such encryption.

(2) The funding necessary to secure such information technology systems from the threat posed by adversarial access to quantum computers.

(3) A description and analysis of ongoing coordination efforts, including any framework and timeline, with international standards development organizations and consortia (such as the International Organization for Standardization) to develop standards for post-quantum cryptography, including any Federal Information Processing Standards developed under chapter 35 of title 44, United States Code.

(c) REPORT ON MIGRATION TO POST-QUANTUM CRYPTOGRAPHY IN INFORMATION TECHNOLOGY SYSTEMS.—Not later than 1 year after the date on which the Director of NIST has issued post-quantum cryptography standards, and annually thereafter until the date that is 9 years after the date on which such standards are issued, the Director of OMB shall submit to Congress a report

on the progress of the Federal Government in transitioning to post-quantum cryptography standards.

(d) DEFINITIONS.—In this section:

(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 NIST.—The term ''Director of NIST'' means the Director of the National Institute for Standards and Technology.

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

(4) EXECUTIVE AGENCY.—The term ''executive agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United States Code.

(5) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given that term in section 11101 of title 40, United States Code.

(6) 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.

(7) QUANTUM COMPUTER.—The term ''quantum computer'' means a device for computation that uses quantum mechanics like superposition and entanglement to perform computational operations on data.

(8) SUPERPOSITION.—The term ''superposition'' refers to the ability of quantum systems to exist in two or more states simultaneously.

(9) ENTANGLEMENT.—The term ''entanglement'' is a property where two or more quantum objects in a system can be intrinsically linked such that the measurement of one dictates the possible measurement outcomes for another, regardless of how far apart the objects are.

○