119TH CONGRESS
1ST SESSION

S. 2558

To require the Subcommittee on the Economic and Security Implications of Quantum Information Science to assess possible migration by Federal agencies to post-quantum cryptography, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 30, 2025

Mr. PETERS (for himself and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To require the Subcommittee on the Economic and Security Implications of Quantum Information Science to assess possible migration by Federal agencies to post-quantum 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 ''The National Quantum Cybersecurity Migration Strategy Act of 2025.''.

SEC. 2. DEFINITIONS.

In this Act:

(1) CRYPTOGRAPHY.—The term ''cryptography'' has the meaning given such term in the National Institute of Standards and Technology Special Publication 1800–21B (relating to mobile device security) and the National Institute of Standards and Technology Special Publication 800–59 (relating to guidelines for identifying an information system as a national security system).

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

(3) 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.

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

(5) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(6) HIGH-IMPACT SYSTEM.—The term ''high-impact system'' means a Federal information system that holds sensitive information, the loss of which would be categorized as high impact under Federal Information Processing Standards Publication 199 (relating to standards for security categorization of Federal information and information systems), as in effect on the day before the date of the enactment of this Act.

(7) SECTOR RISK MANAGEMENT AGENCY.—The term ''sector risk management agency'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

SEC. 3. STRATEGY FOR FEDERAL AGENCY MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.

(a) DUTIES OF SUBCOMMITTEE ON THE ECONOMIC AND SECURITY IMPLICATIONS OF QUANTUM INFORMATION SCIENCE.—Not later than 180 days after the date of the enactment of this Act, the Subcommittee on the Economic and Security Implications of Quantum Information Science, as established by section 105 of the National

Quantum Initiative Act (15 U.S.C. 8814a), in coordination with the Director of the National Institute of Standards and Technology and in consultation with the Quantum Economic Development Consortium, shall develop a National Quantum Cybersecurity Migration Strategy that includes the following:

(1) A definition of a cryptographically relevant quantum computer.

(2) Recommended standards for Federal agencies to apply to determine whether a quantum computer meets such definition, including—

(A) the characteristics of such computers; and

(B) the particular point at which such computers are capable of attacking real world cryptographic systems that classical computers are unable to attack.

(3) An assessment of the urgency for migration to post-quantum cryptography for each Federal agency relative to—

(A) the critical functions of each agency; and

(B) the risk each agency faces should a cryptographically relevant quantum computer attack a system operated by the agency.

(4) Performance measures for migration to post-quantum cryptography to be used by each Federal agency for each of the following 4 stages of migration:

(A) Preparation for migration to post-quantum cryptography.

(B) Establishment of a baseline understanding of the data inventory.

(C) Planning and execution of post-quantum cryptographic solutions, including ensuring that data at rest and in motion is subject to appropriate protections.

(D) Monitoring and evaluation of migration success and assessment of cryptographic security.

(5) A plan for evaluating and monitoring entities that are at high risk of quantum cryptographic attacks, including entities determined to be providers of critical infrastructure.

(b) POST-QUANTUM PILOT PROGRAM.—Not later than 180 days after the date of the enactment of this Act, the Subcommittee on the Economic and Security Implications of Quantum Information Science shall establish a post-quantum pilot program that requires each sector risk management agency to upgrade not less than one high-

impact system to post-quantum cryptography not later than January 1, 2027.

(c) DUTIES OF THE OFFICE OF ELECTRONIC GOVERNMENT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Office of Electronic Government, in coordination with the Subcommittee on the Economic and Security Implications of Quantum Information Science, shall—

(1) survey the heads of Federal agencies for information relating to the cost of migration to post-quantum cryptography by the Federal agencies, including estimates for the personnel, equipment, and time needed to fully implement post-quantum cryptography, in alignment with the National Quantum Cybersecurity Migration Strategy developed pursuant to subsection (a);

(2) verify that the information provided under paragraph (1) is realistic and fiscally sound;

(3) identify the funding and resources necessary for Federal agencies to carry out the migration to post-quantum cryptography; and

(4) advise on how Federal agencies should encourage the adoption of post-quantum cryptography by the private sector.

(d) REPORT TO CONGRESS.—Not later than 1 year after the date of the enactment of this Act, the Director of the Office of Management and Budget and the Subcommittee on the Economic and Security Implications of Quantum Information Science shall jointly submit to Congress a report detailing their findings with respect to the post-quantum migration assessments required under subsection (a)(3), the pilot program established pursuant to subsection (b), and the survey on associated costs of executing the migration required by subsection (c)(1).

(e) ASSESSMENT BY COMPTROLLER GENERAL.—Not later than 1 year after the development of the National Quantum Cybersecurity Migration Strategy under subsection (a), and annually thereafter, the Comptroller General of the United States shall submit to Congress an assessment, using the performance measures described in subsection (a)(4), of the progress made by each Federal agency in migrating to post-quantum cryptography.

○