119TH CONGRESS
1ST SESSION

S. 3312

To require the Director of the National Institute of Standards and Technology to develop guidance for upgrading information systems to post-quantum cryptography, and for other purposes.

IN THE SENATE OF THE UNITED STATES

DECEMBER 2, 2025

Mr. PETERS (for himself and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To require the Director of the National Institute of Standards and Technology to develop guidance for upgrading information systems 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 ''Quantum Readiness and Innovation Act of 2025''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Committee on Energy and Commerce of the House of Representatives.

(2) CLASSICAL COMPUTER; QUANTUM COMPUTER.—The terms ''classical computer'' and ''quantum computer'' have the meanings given such terms in section 3 of the Quantum Computing Cybersecurity Preparedness Act (Public Law 117–260; 6 U.S.C. 1526 note).

(3) CRITICAL INFRASTRUCTURE SECTORS.—The term ''critical infrastructure sectors'' means the critical infrastructure sectors defined in the National Security Memorandum on ''Critical Infrastructure Security and Resilience'' (NSM–22), dated April 30, 2024.

(4) 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.

(5) POST-QUANTUM CRYPTOGRAPHY.—The term ''post-quantum cryptography''—

(A) means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a quantum computer or classical computer; and

(B) includes—

(i) the lattice-based digital signature algorithm specified in National Institute of Standards and Technology Federal Information Processing Standards Publication 204 (dated August 13, 2024; relating to Module-Lattice-Based Digital Signature Standard), or any successor standard;

(ii) the module-lattice-based key encapsulation mechanism specified in National Institute of Standards and Technology Federal Information Processing Standards Publication 203 (dated August 13, 2024; relating to Module-Lattice-Based Key-Encapsulation Mechanism Standard), or any successor standard; and

(iii) any cryptographic algorithm or method implemented in accordance with National Institute of Standards and Technology Federal Information Processing Standard Publication 140–3 (dated March 22, 2019; relating to Security Requirements for Cryptographic Modules), or any successor standard, operating within a zero trust architecture as described in National Institute of Standards and Technology Special Publication 800–207 (dated August 2020; relating to Zero Trust Architecture), or any successor standard.

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

SEC. 3. GUIDANCE ON UPGRADING TO POST-QUANTUM CRYPTOGRAPHY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology, in consultation with the Director of the Office of Science and Technology Policy, shall establish guidance for upgrading information systems to post-quantum cryptography, including

guidance that is specifically tailored for critical infrastructure sectors.

(b) REQUIREMENT.—The guidance established pursuant to subsection (a) shall include standards and selection criteria to guide the procurement and deployment of commercial solutions for an entity seeking to upgrade to post-quantum cryptography.

(c) DISSEMINATION OF GUIDANCE.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall make available to entities in the private sector the guidance established under subsection (a).

(2) SPECIAL PUBLICATIONS.—The Director may satisfy the requirement under paragraph (1) through the publication of Special Publications.

(d) COORDINATION AND ASSISTANCE FOR INDUSTRY-LED ASSESSMENTS OF ADOPTION OF GUIDANCE.—

(1) IN GENERAL.—If an industry sector representative, who is part of the Quantum Economic Development Consortium, decides to carry out an assessment of the adoption by the industry sector of the guidance established under subsection (a), the Director of the National Institute of Standards and Technology shall offer to collaborate on such assessment with such representative.

(2) TECHNICAL ASSISTANCE AND INTEROPERABILITY FRAMEWORKS.—If requested by the representative described in paragraph (1), the Director of the National Institute of Standards and Technology shall support the assessment by providing—

(A) technical and administrative support;

(B) test beds to support the assessment; and

(C) interoperability frameworks.

(3) COORDINATION ASSISTANCE.—The Director of the National Institute of Standards and Technology may support an assessment described in paragraph (1) by coordinating between stakeholders as the Director considers necessary.

SEC. 4. STRATEGY FOR FEDERAL AGENCY UPGRADE TO POST-QUANTUM CRYPTOGRAPHY.

(a) NATIONAL QUANTUM CYBERSECURITY UPGRADE STRATEGY.—Not later than 360 days after the date of the enactment of this Act, the Director of the Office of Science and Technology Policy, 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 Upgrade Strategy that includes the following:

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

(2) Recommended standards 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 systems that classical computers are unable to attack.

(3) Guidelines for assessing the urgency of upgrading 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) Recommended performance measures for upgrading to post-quantum cryptography for the following tasks:

(A) Preparation for upgrading to post-quantum cryptography, including—

(i) the adoption of hardware integrating quantum-resistant cryptographic algorithms; and

(ii) the deployment of software-only post-quantum cryptography overlays that meet or exceed security standards set forth in the Federal Information Processing Standards issued by the National Institute of Standards and Technology.

(B) Establishment of a baseline understanding of the data inventory, including through the use of automated tools to identify assets.

(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 evaluating the success of the upgrade and assessing the security of the system.

(5) A plan for implementing the above performance measures, including evaluating and monitoring entities that are at high risk of quantum attacks, including sector risk management agencies.

(b) POST-QUANTUM VOLUNTARY PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 360 days after the date of the enactment of this Act, the Director of the Office of Science and Technology Policy shall establish a pilot program to provide planning, technical, and any other support the Director considers appropriate to any covered entity that elects to participate in the program for the purpose of upgrading the systems of such covered entity to post-quantum cryptography.

(2) HIGH RISK ENTITIES.—The Director shall encourage any covered entity that is at high risk of quantum attack to participate in the pilot program established under paragraph (1).

(3) REQUIREMENTS.—Under the pilot program established under paragraph (1)—

(A) not later than 18 months after the date of the establishment of the program, not fewer than 1 high-impact system of any covered entity participating in the program shall be upgraded to post-quantum cryptography in accordance with the recommended performance measures described in subsection (a)(4); and

(B) upon completion of the initial upgrade under subparagraph (A), the head of the covered entity may upgrade—

(i) 1 additional system in accordance with such performance measures; or

(ii) 2 or more systems in accordance with such performance measures if the head notifies the Director before initiating such upgrade.

(4) PILOT PROGRAM REPORTS.—

(A) IN GENERAL.—For each covered entity participating in the program established under paragraph (1), the Director, in coordination with the head of such entity, shall submit to the appropriate congressional committees—

(i) an initial report not later than 180 days after the date on which the initial upgrade is completed under paragraph (3)(A); and

(ii) an updated report annually until such date as the Director considers appropriate.

(B) ELEMENTS.—Each report submitted under subparagraph (A) shall describe—

(i) the actions of the head of the covered entity in carrying out the program; and

(ii) any planning, technical, or other support that the Director provided to the head of the covered entity through the program.

(5) COVERED ENTITY DEFINED.—In this subsection, the term ''covered entity'' means—

(A) a sector risk management agency;

(B) a Federal agency; or

(C) a mission partner of a Federal agency.

(c) REPORT TO CONGRESS.—Not later than 360 days after the date of the enactment of this Act, the Director of the Office of Science and Technology Policy shall submit to the appropriate congressional committees a report that includes the National Quantum Cybersecurity Upgrade Strategy developed under subsection (a) and a description of the pilot program established pursuant to subsection (b)(1).

○