

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Quantum Readiness
5 and Innovation Act of 2025”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) APPROPRIATE CONGRESSIONAL COMMIT-
2 TEES.—The term “appropriate congressional com-
3 mittees” means—

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

6 (B) the Committee on Energy and Com-
7 merce of the House of Representatives.

8 (2) CLASSICAL COMPUTER; QUANTUM COM-
9 PUTER.—The terms “classical computer” and
10 “quantum computer” have the meanings given such
11 terms in section 3 of the Quantum Computing Cy-
12 bersecurity Preparedness Act (Public Law 117–260;
13 6 U.S.C. 1526 note).

14 (3) CRITICAL INFRASTRUCTURE SECTORS.—
15 The term “critical infrastructure sectors” means the
16 critical infrastructure sectors defined in the National
17 Security Memorandum on “Critical Infrastructure
18 Security and Resilience” (NSM–22), dated April 30,
19 2024.

20 (4) HIGH-IMPACT SYSTEM.—The term “high-
21 impact system” means a Federal information system
22 that holds sensitive information, the loss of which
23 would be categorized as high impact under Federal
24 Information Processing Standards Publication 199
25 (relating to standards for security categorization of

1 Federal information and information systems), as in
2 effect on the day before the date of the enactment
3 of this Act.

4 (5) POST-QUANTUM CRYPTOGRAPHY.—The
5 term “post-quantum cryptography”—

6 (A) means those cryptographic algorithms
7 or methods that are assessed not to be specifi-
8 cally vulnerable to attack by either a quantum
9 computer or classical computer; and

10 (B) includes—

11 (i) the lattice-based digital signature
12 algorithm specified in National Institute of
13 Standards and Technology Federal Infor-
14 mation Processing Standards Publication
15 204 (dated August 13, 2024; relating to
16 Module-Lattice-Based Digital Signature
17 Standard), or any successor standard;

18 (ii) the module-lattice-based key en-
19 capsulation mechanism specified in Na-
20 tional Institute of Standards and Tech-
21 nology Federal Information Processing
22 Standards Publication 203 (dated August
23 13, 2024; relating to Module-Lattice-Based
24 Key-Encapsulation Mechanism Standard),
25 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

1 guidance that is specifically tailored for critical infrastruc-
2 ture sectors.

3 (b) REQUIREMENT.—The guidance established pur-
4 suant to subsection (a) shall include standards and selec-
5 tion criteria to guide the procurement and deployment of
6 commercial solutions for an entity seeking to upgrade to
7 post-quantum cryptography.

8 (c) DISSEMINATION OF GUIDANCE.—

9 (1) IN GENERAL.—The Director of the National
10 Institute of Standards and Technology shall make
11 available to entities in the private sector the guid-
12 ance established under subsection (a).

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

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

18 (1) IN GENERAL.—If an industry sector rep-
19 resentative, who is part of the Quantum Economic
20 Development Consortium, decides to carry out an
21 assessment of the adoption by the industry sector of
22 the guidance established under subsection (a), the
23 Director of the National Institute of Standards and
24 Technology shall offer to collaborate on such assess-
25 ment with such representative.

1 (2) TECHNICAL ASSISTANCE AND INTEROPER-
 2 ABILITY FRAMEWORKS.—If requested by the rep-
 3 resentative described in paragraph (1), the Director
 4 of the National Institute of Standards and Tech-
 5 nology shall support the assessment by providing—

6 (A) technical and administrative support;

7 (B) test beds to support the assessment;

8 and

9 (C) interoperability frameworks.

10 (3) COORDINATION ASSISTANCE.—The Director
 11 of the National Institute of Standards and Tech-
 12 nology may support an assessment described in
 13 paragraph (1) by coordinating between stakeholders
 14 as the Director considers necessary.

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

17 (a) NATIONAL QUANTUM CYBERSECURITY UPGRADE
 18 STRATEGY.—Not later than 360 days after the date of
 19 the enactment of this Act, the Director of the Office of
 20 Science and Technology Policy, in coordination with the
 21 Director of the National Institute of Standards and Tech-
 22 nology and in consultation with the Quantum Economic
 23 Development Consortium, shall develop a National Quan-
 24 tum Cybersecurity Upgrade Strategy that includes the fol-
 25 lowing:

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

3 (2) Recommended standards to apply to deter-
4 mine whether a quantum computer meets such defi-
5 nition, including—

6 (A) the characteristics of such computers;
7 and

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

12 (3) Guidelines for assessing the urgency of up-
13 grading to post-quantum cryptography for each Fed-
14 eral agency relative to—

15 (A) the critical functions of each agency;
16 and

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

20 (4) Recommended performance measures for
21 upgrading to post-quantum cryptography for the fol-
22 lowing tasks:

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

1 (i) the adoption of hardware inte-
2 grating quantum-resistant cryptographic
3 algorithms; and

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

10 (B) Establishment of a baseline under-
11 standing of the data inventory, including
12 through the use of automated tools to identify
13 assets.

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

18 (D) Monitoring and evaluating the success
19 of the upgrade and assessing the security of the
20 system.

21 (5) A plan for implementing the above perform-
22 ance measures, including evaluating and monitoring
23 entities that are at high risk of quantum attacks, in-
24 cluding sector risk management agencies.

25 (b) POST-QUANTUM VOLUNTARY PILOT PROGRAM.—

1 (1) IN GENERAL.—Not later than 360 days
2 after the date of the enactment of this Act, the Di-
3 rector of the Office of Science and Technology Policy
4 shall establish a pilot program to provide planning,
5 technical, and any other support the Director con-
6 siders appropriate to any covered entity that elects
7 to participate in the program for the purpose of up-
8 grading the systems of such covered entity to post-
9 quantum cryptography.

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

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

16 (A) not later than 18 months after the
17 date of the establishment of the program, not
18 fewer than 1 high-impact system of any covered
19 entity participating in the program shall be up-
20 graded to post-quantum cryptography in ac-
21 cordance with the recommended performance
22 measures described in subsection (a)(4); and

23 (B) upon completion of the initial upgrade
24 under subparagraph (A), the head of the cov-
25 ered entity may upgrade—

- 1 (i) 1 additional system in accordance
2 with such performance measures; or
3 (ii) 2 or more systems in accordance
4 with such performance measures if the
5 head notifies the Director before initiating
6 such upgrade.

7 (4) PILOT PROGRAM REPORTS.—

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

13 (i) an initial report not later than 180
14 days after the date on which the initial up-
15 grade is completed under paragraph
16 (3)(A); and

17 (ii) an updated report annually until
18 such date as the Director considers appro-
19 priate.

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

22 (i) the actions of the head of the cov-
23 ered entity in carrying out the program;
24 and

1 (ii) any planning, technical, or other
2 support that the Director provided to the
3 head of the covered entity through the pro-
4 gram.

5 (5) COVERED ENTITY DEFINED.—In this sub-
6 section, the term “covered entity” means—

7 (A) a sector risk management agency;

8 (B) a Federal agency; or

9 (C) a mission partner of a Federal agency.

10 (c) REPORT TO CONGRESS.—Not later than 360 days
11 after the date of the enactment of this Act, the Director
12 of the Office of Science and Technology Policy shall sub-
13 mit to the appropriate congressional committees a report
14 that includes the National Quantum Cybersecurity Up-
15 grade Strategy developed under subsection (a) and a de-
16 scription of the pilot program established pursuant to sub-
17 section (b)(1).

○