

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.

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 “The National Quantum
5 Cybersecurity Migration Strategy Act of 2025.”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) CRYPTOGRAPHY.—The term “cryptog-
2 raphy” has the meaning given such term in the Na-
3 tional Institute of Standards and Technology Special
4 Publication 1800–21B (relating to mobile device se-
5 curity) and the National Institute of Standards and
6 Technology Special Publication 800–59 (relating to
7 guidelines for identifying an information system as
8 a national security system).

9 (2) CLASSICAL COMPUTER.—The term “clas-
10 sical computer” means a device that accepts digital
11 data and manipulates the data based on a program
12 or sequence of instructions for how such data is to
13 be processed, and that encodes information in bi-
14 nary.

15 (3) QUANTUM COMPUTER.—The term “quan-
16 tum computer” means a computer that uses the col-
17 lective properties of quantum states, such as super-
18 position, interference, and entanglement, to perform
19 calculations.

20 (4) POST-QUANTUM CRYPTOGRAPHY.—The
21 term “post-quantum cryptography” means cryp-
22 tographic algorithms or methods that are not specifi-
23 cally vulnerable to attacks by either a quantum com-
24 puter or classical computer.

1 (5) **CRITICAL INFRASTRUCTURE.**—The term
2 “critical infrastructure” has the meaning given that
3 term in section 1016(e) of the Critical Infrastruc-
4 tures Protection Act of 2001 (42 U.S.C. 5195c(e)).

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

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

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

20 (a) **DUTIES OF SUBCOMMITTEE ON THE ECONOMIC**
21 **AND SECURITY IMPLICATIONS OF QUANTUM INFORMA-**
22 **TION SCIENCE.**—Not later than 180 days after the date
23 of the enactment of this Act, the Subcommittee on the
24 Economic and Security Implications of Quantum Informa-
25 tion Science, as established by section 105 of the National

1 Quantum Initiative Act (15 U.S.C. 8814a), in coordina-
2 tion with the Director of the National Institute of Stand-
3 ards and Technology and in consultation with the Quan-
4 tum Economic Development Consortium, shall develop a
5 National Quantum Cybersecurity Migration Strategy that
6 includes the following:

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

9 (2) Recommended standards for Federal agen-
10 cies to apply to determine whether a quantum com-
11 puter meets such definition, including—

12 (A) the characteristics of such computers;

13 and

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

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

21 (A) the critical functions of each agency;

22 and

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

1 (4) Performance measures for migration to
2 post-quantum cryptography to be used by each Fed-
3 eral agency for each of the following 4 stages of mi-
4 gration:

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

7 (B) Establishment of a baseline under-
8 standing of the data inventory.

9 (C) Planning and execution of post-quan-
10 tum cryptographic solutions, including ensuring
11 that data at rest and in motion is subject to ap-
12 propriate protections.

13 (D) Monitoring and evaluation of migra-
14 tion success and assessment of cryptographic
15 security.

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

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

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

3 (c) DUTIES OF THE OFFICE OF ELECTRONIC GOV-
4 ERNMENT.—Not later than 180 days after the date of the
5 enactment of this Act, the Administrator of the Office of
6 Electronic Government, in coordination with the Sub-
7 committee on the Economic and Security Implications of
8 Quantum Information Science, shall—

9 (1) survey the heads of Federal agencies for in-
10 formation relating to the cost of migration to post-
11 quantum cryptography by the Federal agencies, in-
12 cluding estimates for the personnel, equipment, and
13 time needed to fully implement post-quantum cryp-
14 tography, in alignment with the National Quantum
15 Cybersecurity Migration Strategy developed pursu-
16 ant to subsection (a);

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

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

22 (4) advise on how Federal agencies should en-
23 courage the adoption of post-quantum cryptography
24 by the private sector.

1 (d) REPORT TO CONGRESS.—Not later than 1 year
2 after the date of the enactment of this Act, the Director
3 of the Office of Management and Budget and the Sub-
4 committee on the Economic and Security Implications of
5 Quantum Information Science shall jointly submit to Con-
6 gress a report detailing their findings with respect to the
7 post-quantum migration assessments required under sub-
8 section (a)(3), the pilot program established pursuant to
9 subsection (b), and the survey on associated costs of exe-
10 cuting the migration required by subsection (c)(1).

11 (e) ASSESSMENT BY COMPTROLLER GENERAL.—Not
12 later than 1 year after the development of the National
13 Quantum Cybersecurity Migration Strategy under sub-
14 section (a), and annually thereafter, the Comptroller Gen-
15 eral of the United States shall submit to Congress an as-
16 sessment, using the performance measures described in
17 subsection (a)(4), of the progress made by each Federal
18 agency in migrating to post-quantum cryptography.

○