

Calendar No. 635

117TH CONGRESS
2D SESSION**S. 4592****[Report No. 117–251]**

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

IN THE SENATE OF THE UNITED STATES

JULY 21, 2022

Ms. HASSAN (for herself, Mr. PORTMAN, Ms. ROSEN, Mr. TILLIS, Mr. YOUNG, and Mr. HEINRICH) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 13, 2022

Reported by Mr. PETERS, with an amendment

[Insert the part printed in italic]

A BILL

To encourage the migration of Federal Government information technology systems to quantum-resistant 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Quantum Computing
3 Cybersecurity Preparedness Act”.

4 **SEC. 2. FINDINGS; SENSE OF CONGRESS.**

5 (a) FINDINGS.—Congress finds the following:

6 (1) Cryptography is essential for the national
7 security of the United States and the functioning of
8 the economy of the United States.

9 (2) The most widespread encryption protocols
10 today rely on computational limits of classical com-
11 puters to provide cybersecurity.

12 (3) Quantum computers might one day have the
13 ability to push computational boundaries, allowing
14 us to solve problems that have been intractable thus
15 far, such as integer factorization, which is important
16 for encryption.

17 (4) The rapid progress of quantum computing
18 suggests the potential for adversaries of the United
19 States to steal sensitive encrypted data today using
20 classical computers, and wait until sufficiently pow-
21 erful quantum systems are available to decrypt it.

22 (b) SENSE OF CONGRESS.—It is the sense of Con-
23 gress that—

24 (1) a strategy for the migration of information
25 technology systems of the Federal Government to
26 post-quantum cryptography is needed; and

1 (2) the governmentwide and industrywide ap-
2 proach to post-quantum cryptography should
3 prioritize developing applications, hardware intellec-
4 tual property, and software that can be easily up-
5 dated to support cryptographic agility.

6 **SEC. 3. DEFINITIONS.**

7 In this Act:

8 (1) CLASSICAL COMPUTER.—The term “clas-
9 sical computer” means a device that accepts digital
10 data and manipulates the information based on a
11 program or sequence of instructions for how data is
12 to be processed and encodes information in binary
13 bits that can either be 0s or 1s.

14 (2) DIRECTOR OF CISA.—The term “Director of
15 CISA” means the Director of the Cybersecurity and
16 Infrastructure Security Agency.

17 (3) DIRECTOR OF NIST.—The term “Director
18 of NIST” means the Director of the National Insti-
19 tute of Standards and Technology.

20 (4) DIRECTOR OF OMB.—The term “Director of
21 OMB” means the Director of the Office of Manage-
22 ment and Budget.

23 (5) EXECUTIVE AGENCY.—The term “executive
24 agency” has the meaning given the term “Executive

1 agency” in section 105 of title 5, United States
2 Code.

3 (6) INFORMATION TECHNOLOGY.—The term
4 “information technology” has the meaning given the
5 term in section 3502 of title 44, United States Code.

6 (7) POST-QUANTUM CRYPTOGRAPHY.—The
7 term “post-quantum cryptography” means a cryp-
8 tographic system that—

9 (A) is secure against decryption attempts
10 using a quantum computer or classical com-
11 puter; and

12 (B) can interoperate with existing commu-
13 nications protocols and networks.

14 (8) QUANTUM COMPUTER.—The term “quan-
15 tum computer” means a computer that uses the col-
16 lective properties of quantum states to perform cal-
17 culations.

18 **SEC. 4. INVENTORY OF CRYPTOGRAPHIC SYSTEMS; MIGRA-**
19 **TION TO POST-QUANTUM CRYPTOGRAPHY.**

20 (a) INVENTORY.—

21 (1) ESTABLISHMENT.—Not later than 180 days
22 after the date of enactment of this Act, the Director
23 of OMB shall establish, by rule or binding guidance,
24 a requirement for each executive agency to establish

1 and maintain an inventory of each cryptographic
2 system in use by the agency.

3 (2) ADDITIONAL CONTENT IN RULE OR BIND-
4 ING GUIDANCE.—In the rule or binding guidance es-
5 tablished by paragraph (1), the Director of OMB
6 shall include, in addition to the requirement de-
7 scribed under that paragraph—

8 (A) a description of information technology
9 to be prioritized for migration to post-quantum
10 cryptography;

11 (B) a description of the information re-
12 quired to be reported pursuant to subsection
13 (b); and

14 (C) a process for evaluating progress on
15 migrating information technology to post-quantum
16 cryptography, which shall be automated to
17 the greatest extent practicable.

18 (3) PERIODIC UPDATES.—The Director of OMB
19 shall update the rule or binding guidance established
20 by paragraph (1) as the Director determines nec-
21 essary.

22 (b) AGENCY REPORTS.—Not later than 1 year after
23 the date of enactment of this Act, and on an ongoing basis
24 thereafter, the head of each executive agency shall provide
25 to the Director of OMB, the Director of CISA, and the

1 National Cyber Director an inventory of all information
2 technology in use by the executive agency that is vulner-
3 able to decryption by quantum computers, prioritized pur-
4 suant to the guidance issued under subsection (a)(2).

5 (c) MIGRATION AND ASSESSMENT.—

6 (1) MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.—Not later than 1 year after the date on
7 which the Director of NIST has issued post-quantum cryptography standards, the Director of OMB
8 shall issue guidance requiring each executive agency
9 to develop a plan to migrate information technology
10 of the agency to post-quantum cryptography.

13 (2) DESIGNATION OF SYSTEMS FOR MIGRATION.—Not later than 90 days after the date on
14 which the guidance required by paragraph (1) has
15 been issued, the Director of OMB shall issue guid-
16 ance for *executive* agencies to—

18 (A) designate information technology to be
19 migrated to post-quantum cryptography; and

20 (B) prioritize information technology des-
21 ignated under subparagraph (A), on the basis
22 of the amount of risk posed by decryption by
23 quantum computers to that technology, for mi-
24 gration to post-quantum cryptography.

1 (d) INTEROPERABILITY.—The Director of OMB shall
2 ensure that the designations and prioritizations made
3 under subsection (c)(2) are assessed and coordinated to
4 ensure interoperability.

5 (e) REPORT ON POST-QUANTUM CRYPTOGRAPHY.—
6 Not later than 15 months after the date of enactment of
7 this Act, the Director of OMB shall submit to Congress
8 a report on the following:

9 (1) A strategy to address the risk posed by the
10 vulnerabilities of information technology systems of
11 executive agencies to weakened encryption due to the
12 potential and possible capability of a quantum com-
13 puter to breach that encryption.

14 (2) The amount of funding needed by executive
15 agencies to secure the information technology sys-
16 tems described in paragraph (1) from the risk posed
17 by an adversary of the United States using a quan-
18 tum computer to breach the encryption of informa-
19 tion technology systems.

20 (3) A description of Federal civilian executive
21 branch coordination efforts led by the National In-
22 stitute of Standards and Technology, including
23 timelines, to develop standards for post-quantum
24 cryptography, including any Federal Information
25 Processing Standards developed under chapter 35 of

1 title 44, United States Code, as well as standards
2 developed through voluntary, consensus standards
3 bodies such as the International Organization for
4 Standardization.

5 (f) REPORT ON MIGRATION TO POST-QUANTUM
6 CRYPTOGRAPHY IN INFORMATION TECHNOLOGY SYS-
7 TEMS.—Not later than 1 year after the date on which the
8 Director of OMB issues guidance under subsection (c)(2),
9 and annually thereafter until the date that is 5 years after
10 the date on which post-quantum cryptographic standards
11 are issued, the Director of OMB shall submit to Congress,
12 with the report submitted pursuant to section 3553(c) of
13 title 44, United States Code, a report on the progress of
14 executive agencies in adopting post-quantum cryptography
15 standards.

16 **SEC. 5. DETERMINATION OF BUDGETARY EFFECTS.**

17 The budgetary effects of this Act, for the purpose of
18 complying with the Statutory Pay-As-You-Go Act of 2010,
19 shall be determined by reference to the latest statement
20 titled “Budgetary Effects of PAYGO Legislation” for this
21 Act, submitted for printing in the Congressional Record
22 by the Chairman of the House Budget Committee, pro-
23 vided that such statement has been submitted prior to the
24 vote on passage.

Calendar No. 635

117TH CONGRESS
2D Session

S. 4592

[Report No. 117-251]

A BILL

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

DECEMBER 13, 2022

Reported with an amendment