

.....
(Original Signature of Member)

117TH CONGRESS
2D SESSION

H. R.

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

IN THE HOUSE OF REPRESENTATIVES

Mr. KHANNA (for himself, Ms. MACE, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on

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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Quantum Computing
5 Cybersecurity Preparedness Act”.

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

7 (a) FINDINGS.—The Congress finds the following:

1 (1) Cryptography is essential for our national
2 security and the functioning of our economy.

3 (2) The most widespread encryption protocols
4 today rely on computational limits of classical com-
5 puters to provide cybersecurity.

6 (3) Quantum computers might one day have the
7 ability to push computational boundaries, allowing
8 us to solve problems that have been intractable thus
9 far, such as integer factorization, which is important
10 for encryption.

11 (4) The rapid progress of quantum computing
12 suggests the potential for adversaries to steal sen-
13 sitive encrypted data today using classical com-
14 puters, and wait until sufficiently powerful quantum
15 systems are available to decrypt it.

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

18 (1) a strategy for the migration of information
19 technology systems of the Federal Government to
20 post-quantum cryptography is needed; and

21 (2) the Governmentwide and industrywide ap-
22 proach to post-quantum cryptography should
23 prioritize developing applications, hardware intellec-
24 tual property (IP), and software that can be easily
25 updated to developing support cryptographic agility.

1 **SEC. 3. MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.**

2 (a) **MIGRATION AND ASSESSMENT.**—

3 (1) **MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.**—Not later than 1 year after the date on
4 which the Director of NIST has issued post-quantum cryptography standards, the Director of OMB,
5 in consultation with the Chief Information Officers Council, shall begin to prioritize the migration to
6 post-quantum cryptography and assessment of information technology systems of executive agencies that
7 does not use post-quantum cryptography, including digital signatures.
8
9
10
11
12

13 (2) **DESIGNATION OF SYSTEMS FOR MIGRATION.**—Not later than 1 year after the date on
14 which post-quantum cryptography standards have been set by NIST and on an ongoing basis there-
15 after, the Director of OMB, in consultation with the Chief Information Officers Council, shall designate
16 and prioritize for migration to post-quantum cryptography information technology systems of execu-
17 tive agencies based on the risk of systems that do not use post-quantum cryptography.
18
19
20
21
22

23 (b) **REPORT ON POST-QUANTUM CRYPTOGRAPHY.**—

24 Not later than 1 year after the date of the enactment of
25 this section, the Director of OMB shall submit to Congress
26 a report on the following:

1 (1) A strategy to address the risk posed by the
2 vulnerabilities of information technology systems of
3 executive agencies to weakened encryption due to the
4 potential and possible capability of a quantum com-
5 puter to breach such encryption.

6 (2) The funding necessary to secure such infor-
7 mation technology systems from the threat posed by
8 adversarial access to quantum computers.

9 (3) A description and analysis of ongoing co-
10 ordination efforts, including any framework and
11 timeline, with international standards development
12 organizations and consortia (such as the Inter-
13 national Organization for Standardization) to de-
14 velop standards for post-quantum cryptography, in-
15 cluding any Federal Information Processing Stand-
16 ards developed under chapter 35 of title 44, United
17 States Code.

18 (c) REPORT ON MIGRATION TO POST-QUANTUM
19 CRYPTOGRAPHY IN INFORMATION TECHNOLOGY SYS-
20 TEMS.—Not later than 1 year after the date on which the
21 Director of NIST has issued post-quantum cryptography
22 standards, and annually thereafter until the date that is
23 9 years after the date on which such standards are issued,
24 the Director of OMB shall submit to Congress a report

1 on the progress of the Federal Government in
2 transitioning to post-quantum cryptography standards.

3 (d) DEFINITIONS.—In this section:

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

10 (2) DIRECTOR OF NIST.—The term “Director
11 of NIST” means the Director of the National Insti-
12 tute for Standards and Technology.

13 (3) DIRECTOR OF OMB.—The term “Director of
14 OMB” means the Director of the Office of Manage-
15 ment and Budget.

16 (4) EXECUTIVE AGENCY.—The term “executive
17 agency” has the meaning given the term “Executive
18 agency” in section 105 of title 5, United States
19 Code.

20 (5) INFORMATION TECHNOLOGY.—The term
21 “information technology” has the meaning given
22 that term in section 11101 of title 40, United States
23 Code.

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

4 (A) is secure against decryption attempts
5 using a quantum computer or classical com-
6 puter; and

7 (B) can interoperate with existing commu-
8 nications protocols and networks.

9 (7) QUANTUM COMPUTER.—The term “quan-
10 tum computer” means a device for computation that
11 uses quantum mechanics like superposition and en-
12 tanglement to perform computational operations on
13 data.

14 (8) SUPERPOSITION.—The term “superposi-
15 tion” refers to the ability of quantum systems to
16 exist in two or more states simultaneously.

17 (9) ENTANGLEMENT.—The term “entangle-
18 ment” is a property where two or more quantum ob-
19 jects in a system can be intrinsically linked such
20 that the measurement of one dictates the possible
21 measurement outcomes for another, regardless of
22 how far apart the objects are.