I

118TH CONGRESS
1ST SESSION

H. R. 5759

To amend the National Quantum Initiative Act and the Cyber Security Research and Development Act to advance the rapid deployment of post quantum cybersecurity standards across the United States economy, support United States cryptography research, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 27, 2023

Mr. JACKSON of North Carolina (for himself and Ms. TENNEY) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

A BILL

To amend the National Quantum Initiative Act and the Cyber Security Research and Development Act to advance the rapid deployment of post quantum cybersecurity standards across the United States economy, support United States cryptography research, 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 ''Post Quantum Cybersecurity Standards Act''.

SEC. 2. NIST CRYPTOGRAPHY PROGRAMS AND NSF CRYPTOGRAPHY RESEARCH.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CRYPTOGRAPHY PROGRAMS.—The National Quantum Initiative Act is amended—

(1) in section 2 (15 U.S.C. 8801)—

(A) by redesignating paragraphs (4), (5), (6), (7), the first paragraph (8) (relating to the definition of ''Subcommittee on Economic and Security Implications''), and the second paragraph (8) (relating to the definition of ''Subcommittee on Quantum Information Science'') as paragraphs (5), (7), (8), (9), (11), and (12), respectively;

(B) by inserting after paragraph (3) the following new paragraph:

''(4) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e))'';

(C) by inserting after paragraph (5), as so redesignated, the following new paragraph:

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

(D) by inserting after paragraph (9), as so redesignated, the following new paragraph:

''(10) 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).''; and

(2) in section 201 (15 U.S.C. 8831), by—

(A) redesignating subsection (c) as subsection (d); and

(B) inserting after subsection (b) the following new subsection:

''(c) POST QUANTUM CRYPTOGRAPHY DEPLOYMENT.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology, in consultation with the Secretary of Homeland Security and the heads of sector risk management agencies, as appropriate, shall promote the voluntary adoption and deployment of post-quantum cryptography standards, including by—

''(A) disseminating and making publicly available guidance and resources to help organi-

zations adopt and deploy post-quantum cryptography standards;

"(B) providing technical assistance, as practicable, to entities that are high risk of quantum cryptoanalytic attacks, such as entities determined to be critical infrastructure or digital infrastructure providers; and

"(C) conducting such other activities as determined necessary by the Director to promote the adoption and deployment of post-quantum cryptography standards across the United States.

"(2) GRANT PROGRAM.—

"(A) IN GENERAL.—Subject to the availability of appropriations and after the date on which the Director of National Institute of Standards and Technology has issued post-quantum cryptography standards under paragraph (1), the Director may establish a program to identify and provide technical assistance through the award of grants to entities that are at high risk of quantum cryptoanalytic attacks, including by granting funds, in adopting such post-quantum cryptographic standards

and remediating quantum-related vulnerabilities.

''(B) USE OF FUNDS.—Grants awarded to entities under this subsection may be used to cover reasonable costs, up to a specified amount established by the Director of the National Institute of Standards and Technology, of activities to adopt post-quantum cryptographic standards and remediate quantum-related vulnerabilities.

''(C) GUIDANCE.—The Director of the National Institute of Standards and Technology may develop, and periodically update, guidance, including eligibility, application disclosure requirements, grant amount and duration, and any additional requirements regarding the award of grants under this paragraph.

''(D) CONSULTATION.—If the program described in this paragraph is established, the Director of the National Institute of Standards and Technology shall consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, the heads of other Sector Specific Agencies and risk management agencies, and

appropriate representatives of private sector entities, including nonprofit organizations, to share information regarding the program and guidance developed under subparagraph (C).''.

(b) NATIONAL SCIENCE FOUNDATION CRYPTOGRAPHY RESEARCH.—Subsection (a)(1)(A) of section 4 of the Cyber Security Research and Development Act (15 U.S.C. 7403) is amended by inserting '', including post-quantum cryptography'' before the semicolon.

○