Peters-Blackburn 1 (Modified)

AMENDMENT NO._____ Calendar No._____

Purpose: To require the Director of the National Institute of Standards and Technology to develop guidance for upgrading information systems to post-quantum cryptography.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

S. 3597

To reauthorize the National Quantum Initiative Act, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. PETERS (for himself and Mrs. BLACKBURN)

Viz:

Strike paragraphs (1) and (2) of subsection (e) of section 201 of the National Quantum Initiative Act (15 U.S.C. 8831), as amended by section 12, and insert the following:

"(1) DEFINITIONS.—In this subsection:

"(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(i) the Committee on Commerce, Science, and Transportation of the Senate; and

"(ii) the Committee on Energy and Commerce of the House of Representatives.

"(B) CLASSICAL COMPUTER; QUANTUM COMPUTER.—The terms 'classical computer' and 'quantum computer' have the meanings given such terms in section 3 of the Quantum Computing Cybersecurity Preparedness Act (Public Law 117–260; 6 U.S.C. 1526 note).

"(C) CRITICAL INFRASTRUCTURE SECTORS.—The term 'critical infrastructure sectors' means the critical infrastructure sectors defined in the National Security Memorandum on 'Critical Infrastructure Security and Resilience' (NSM–22), dated April 30, 2024.

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

"(i) 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

"(ii) includes—

"(I) the lattice-based digital signature algorithm specified in National Institute of Standards and Technology Federal Information Processing Standards Publication 204 (dated August 13, 2024; relating to Module-Lattice-Based Digital Signature Standard), or any successor standard;

"(II) the module-lattice-based key encapsulation mechanism specified in National Institute of Standards and Technology Federal Information Processing Standards Publication 203 (dated August 13, 2024; relating to Module-Lattice-Based Key-Encapsulation Mechanism Standard), 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.

"(E) 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).

"(2) GUIDANCE ON UPGRADING TO POST-QUANTUM CRYPTOGRAPHY.—

"(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Director of the National Institute of Standards and Technology, in consultation with the Director of the Office of Science and Technology Policy, the Secretary of Homeland Security, and the head of any other agency the Director of the National Institute of Standards and Technology considers appropriate,

shall establish guidance for upgrading information systems to post-quantum cryptography, including guidance that is specifically tailored for critical infrastructure sectors.

"(B) DISSEMINATION OF GUIDANCE.—

"(i) IN GENERAL.—The Director of the National Institute of Standards and Technology shall make available to entities in the private sector the guidance established under subparagraph (A).

"(ii) SPECIAL PUBLICATIONS.—The Director may satisfy the requirement under clause (i) through the publication of Special Publications.

"(3) STRATEGY FOR FEDERAL AGENCY UPGRADE TO POST-QUANTUM CRYPTOGRAPHY.—

"(A) NATIONAL QUANTUM CYBERSECURITY UPGRADE STRATEGY.—The Secretary of Commerce, in coordination with the Director of the Office of Science and Technology Policy and in consultation with the Quantum Economic Development Consortium and the head of any other agency the Secretary of Commerce considers appropriate, shall develop a National

Quantum Cybersecurity Upgrade Strategy that includes the following:

"(i) A definition of a cryptographically relevant quantum computer.

"(ii) Recommended standards to apply to determine whether a quantum computer meets such definition, including—

"(I) the characteristics of such computers; and

"(II) the particular point at which such computers are capable of attacking real world systems that classical computers are unable to attack.

"(iii) Guidelines for assessing the urgency of upgrading to post-quantum cryptography for each Federal agency relative to—

"(I) the critical functions of each agency; and

"(II) the risk each agency faces should a cryptographically relevant quantum computer attack a system operated by the agency.

"(iv) Recommended performance measures for upgrading to post-quantum cryptography for the following tasks:

"(I) Preparation for upgrading to post-quantum cryptography, including—

"(aa) the adoption of hardware integrating quantum-resistant cryptographic algorithms; and

"(bb) the deployment of software-only post-quantum cryptography overlays that meet or exceed security standards set forth in the Federal Information Processing Standards issued by the National Institute of Standards and Technology.

"(II) Establishment of a baseline understanding of the data inventory, including through the use of automated tools to identify assets.

"(III) Planning and execution of post-quantum cryptographic solutions, including ensuring that data at rest

and in motion is subject to appropriate protections.

"(IV) Monitoring and evaluating the success of the upgrade and assessing the security of the system.

"(v) A plan for implementing the above performance measures, including evaluating and monitoring entities that are at high risk of quantum attacks, including sector risk management agencies.

"(B) REPORT TO CONGRESS.—Not later than 360 days after the date of the enactment of this subsection, the Director of the National Institute of Standards and Technology shall submit to the appropriate congressional committees a report that includes the National Quantum Cybersecurity Upgrade Strategy developed under subparagraph (A).

"(4) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize the development or implementation of any rulemaking or regulatory action for non-Federal entities.".