AMENDMENT TO H.R. 8462

OFFERED BY MR. OBERNOLTE OF CALIFORNIA

Insert after section 24 the following:

SEC. 25. INTERIM POST QUANTUM CRYPTOGRAPHY MEASURES.

(a) AUTHORIZATION FOR FEDERAL ENTITIES.—

(1) IN GENERAL.—The Chief Information Officer (or functional equivalent) for each Federal entity may directly procure interim post quantum cryptographic software and initiate upgrades to deploy such software on any Federal device of such entity that stores, uses, transmits, and receives digital information if the following requirements are met:

(A) The software is the best available cryptographic software in terms of functionality and bit strength needed for Federal entity use cases as determined by the Chief Information Officer (or functional equivalent).

(B) The software is compatible with the existing or planned Federal cybersecurity framework, policy, and governance of the Federal entity and is not limited to any product, service, or solution identified in the document

entitled ''Post Quantum Cryptography Buyer's Guide (Version 1.0)'' and published by the General Services Administration in June 2025, or any successor guide.

(C) Any contractor that provides the software certifies before entering into a contract that any such software provided is interim post quantum cryptographic software.

(D) The software and the contract for the software do not include a vendor lock for the Federal entity but may be procured under a multi-year term contract if the contract contains a clause for the Federal entity to opt out of the contract every 2 years.

(2) DEADLINE TO COMPLETE UPGRADE.—The Chief Information Officer (or functional equivalent) for each Federal entity may procure the interim post quantum cryptographic software under paragraph (1) as soon as practicable, and the installation of such software shall be completed within 36 months after the date of the enactment of this section or as soon as practicable.

(b) DEFINITIONS.—In this section:

(1) CRYPTOGRAPHIC SOFTWARE.—The term ''cryptographic software'' means cryptographic in-

structions or programs, including a crypto system, for data-packet-level encryption, through which cleartext data is never exposed in memory, logs, caches, or network transport outside of authorized cryptographic boundaries and decryption of such data only occurs in authorized execution contexts, that do not require replacement, modification, or augmentation of chips, cryptographic cards, radios, hardware security modules, or other physical components.

(2) FEDERAL ENTITY.—The term ''Federal entity'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code, and any other entity of the Federal Government funded in whole or part by the Federal Government.

(3) INTERIM POST QUANTUM CRYPTOGRAPHIC SOFTWARE.—The term ''interim post quantum cryptographic software'' means cryptographic software that meets the following requirements:

(A) Is developed in the United States.

(B) Is able to protect data in storage, transit, and use.

(C) Includes a lattice-based, symmetric, asymmetric, or hybrid cipher or crypto system

capable of providing security strength that is equivalent to or exceeds AES–256, or any successor standard.

(D) Is able to meet the following:

(i) NIST Federal Information Processing Standard 140–3 (entitled ''Security Requirements for Cryptographic Modules'') or a successor standard.

(ii) NIST Federal Information Processing Standard 202 (entitled ''SHA–3 Standard: Permutation-Based Hash and Extendable-Output Functions''), 203 (entitled ''Module-Lattice-Based Key-Encapsulation Mechanism Standard''), or 204 (entitled ''Module-Lattice-Based Digital Signature Standard''), or successor standards.

(E) Is able to meet post quantum security margins, as defined by the Director of NIST.

(F) Is able to steganographically embed access controls, authorization policies, and a multi-factor key for user identity and device authorization at the data or key level through the encryption process.

(G) Is able to guarantee data provenance.

(H) Is able to be used with little or no performance degradation.

(I) Is capable of widespread system deployment for Federal entities, with little or no system disruption.

(J) Is able to rotate keys and transition cryptographic algorithms securely over the air, including in degraded, denied, or electronic environments, without system disruption, hardware replacement, or physical access to endpoints.

(K) Provides to the Federal entity at issue full key custody and control and consistent key sovereignty, including no required key escrow, replication, derivation, or retention of cryptographic keys by a third-party contractor or cloud service provider.

(4) NIST.—The term ''NIST'' means the National Institute of Standards and Technology.

(5) VENDOR LOCK.—The term ''vendor lock'' means a contractual or technical dependency on the cryptographic software or technology of a supplier, such that data encrypted using such software or technology, as the case may be, cannot, without cost or the extension of a license, be decrypted, accessed,

or migrated by the Federal entity at issue after a contract for such software expires.