AMENDMENT TO RULES COMM. PRINT 119–33
OFFERED BY MR. NEHLS OF TEXAS

In title XV, subtitle A, add at the end the following:

SEC. 15___. INTERIM DATA PROTECTION MEASURES FOR THE DEPARTMENT OF DEFENSE.

(a) DATA PROTECTION REVIEW.—The Secretary of Defense shall ensure that, not later than 45 days after the date of the enactment of this Act, each portfolio acquisition executive initiates a narrow, expeditious review of each program of record assigned to such executive to determine whether it is feasible and practicable to incorporate into the program of record cryptographic protection described in subsection (b) in a manner that does not require replacement, modification, or augmentation of existing chips, cryptographic cards, radios, hardware security modules, or other physical components.

(b) CRYPTOGRAPHIC PROTECTION.—The cryptographic protection described in this subsection is utility-based, software-only data packet level cryptographic protection that—

(1) advances data protection for the program of record toward the migration to post quantum cryptography on or before December 31, 2030, as di-

rected in the memorandum of the Chief Information Officer dated November 18, 2025 (relating to ''Preparing for Migration to Post Quantum Cryptography'');

(2) is, or is compatible with, a lattice-based, symmetric, asymmetric, or hybrid cipher capable of providing security strength of or exceeding Advanced Encryption Standard with a 256-bit key (AES-256), including post-quantum security key encapsulation at greater than 1024-bit and digital signature mechanisms and other parameters defined by the Chief Information Officer;

(3) is capable of directly combining cryptographic key material with access controls and authorization constraints or policies controlled by the Department of Defense, a multi-factor key for user identity management and device authentication through the encryption process at the data or key level, and can guarantee provenance between the sender and the receiver of data;

(4) provides capability for variable symmetric encryption strengths of at least 512-bit with minimal degradation of encryption decryption speed; and

(5) provides full key custody and control to the data owner within the Department of Defense, con-

sistent key sovereignty, including no requirement for key escrow, replication, derivation, or retention of cryptographic keys by third-party vendors.

(c) APPROVAL.—Software providing the cryptographic protection described in subsection (b) shall be approved by the Chief Information Officer of the Department of Defense before it is deployed in any program of record.

(d) FUTURE PROGRAMS OF RECORD.—The Secretary of Defense shall ensure that each program of record established after the date of the enactment of this Act incorporates cryptographic protection described in subsection (b) from inception, to the extent it is feasible and practicable to do so.

(e) POOLED IMPLEMENTATION.—The Chief Information Officer is authorized to direct pooled acquisitions of licenses for cryptographic protection described in subsection (b) for use by programs of record across one or more programs in one or more military departments or other elements of the Department.

(f) VENDOR LOCK.—The Secretary of Defense shall ensure, in acquiring any cryptographic protection described in subsection (b), that the Department retains the legal and technical capability to decrypt, access, and mi-

grate its encrypted data upon termination of the contract, without cost and without extending the contract.

(g) MULTI-YEAR TERM.—A contract for cryptographic protection described in subsection (b) may have a multi-year term if the contract contains a clause for the Department of Defense to opt out of the contract every two years.

(h) RELATIONSHIP TO EXISTING GUIDANCE.—The Secretary of Defense shall ensure that this section is implemented in a manner that is consistent with, and seeks to advance, the zero-trust initiatives and classified network protection requirements of the Department of Defense.

☒