AMENDMENT TO RULES COMM. PRINT 119–33
OFFERED BY MR. BIGGS OF ARIZONA

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

SEC. 15___. SECURE AND INTEROPERABLE DEFENSE COLLABORATION TECHNOLOGY.

(a) DEFINITIONS.—In this section:

(1) CHIEF INFORMATION OFFICER.—The term ''Chief Information Officer'' means the Chief Information Officer of the Department of Defense.

(2) COLLABORATION TECHNOLOGY.—The term ''collaboration technology'' means a software system or application that offers one or more primary collaboration technology features.

(3) DEPARTMENT.—The term ''Department'' means the Department of Defense.

(4) END-TO-END ENCRYPTION.—The term ''end-to-end encryption'' means communications encryption in which data is encrypted when being passed through a network such that no party, other than the sender and each intended recipient of the communication, can access the decrypted communication, regardless of the transport technology used

and the intermediaries or intermediate steps along the sending path.

(5) IDENTIFIED STANDARDS.—The term ''identified standards'' means the standard, or set of standards, identified under subsection (b)(2).

(6) INTEROPERABILITY.—The term ''interoperability'' has the meaning given the term in section 3601 of title 44, United States Code.

(7) OPEN STANDARD.—The term ''open standard'' means a standard, or a set of standards, that—

(A) is available for any individual to read and implement;

(B) does not impose any royalty or other fee for use; and

(C) can be certified for low or no cost to users of the standard or set of standards.

(8) PRIMARY COLLABORATION TECHNOLOGY FEATURE.—The term ''primary collaboration technology feature'' means a technology feature or function that—

(A) facilitates remote work or collaboration within the Department;

(B) facilitates the work or collaboration described in subparagraph (A) by providing

functionality that is core or essential, rather than ancillary or secondary; and

(C) is identified by the Chief Information Officer under subsection (b)(1).

(9) STANDARDS-COMPATIBLE COLLABORATION TECHNOLOGY.—The term ''standards-compatible collaboration technology'' means collaboration technology—

(A) each primary collaboration technology feature of which is compatible with the identified standards for such a primary collaboration technology feature; and

(B) that has demonstrated compliance under subsection (d)(2).

(10) VOLUNTARY CONSENSUS STANDARD.—The term ''voluntary consensus standard'' has the meaning given such term in Circular A–119 of the Office of Management and Budget entitled ''Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities'', issued in revised form on January 27, 2016.

(11) THIRD-PARTY HOSTING SERVER.—The term ''third-party hosting server'' means any com-

puter or software system which is not directly operated and managed by the Department.

(b) IDENTIFYING STANDARDS FOR DEFENSE COLLABORATION TECHNOLOGY.—

(1) IDENTIFICATION OF FEATURES.—Not later than 180 days after the date of the enactment of this Act, the Chief Information Officer shall, in consultation with such others as the Chief Information Officer considers relevant, identify a list of primary collaboration technology features, including—

(A) voice and video calling, including—

(i) calling between two individuals within the Department (including any agencies or departments within the Department); and

(ii) calling between not less than three individuals within the Department (including any agencies or departments within the Department);

(B) text-based messaging within the Department (including any agencies or departments within the Department);

(C) file sharing within the Department (including any agencies or departments within the Department);

(D) live document editing within the Department (including any agencies or departments within the Department);

(E) scheduling and calendaring within the Department (including any agencies or departments within the Department); and

(F) any other technology feature or function that the Chief Information Officer considers appropriate.

(2) IDENTIFICATION OF STANDARDS.—Not later than two years after the date of the enactment of this Act, the Chief Information Officer shall identify a standard, or set of standards, for collaboration technology used by the Department that—

(A) for each primary collaboration technology feature, specifies interoperability protocols, and any other protocol, format, requirement, or guidance required to create interoperable implementations of that feature, including—

(i) protocols for applications to specify and standardize security, including systems for—

(I) identifying and authenticating the individuals who are party to a communication or collaboration task;

(II) controlling the attendance and security settings of voice and video calls; and

(III) controlling access and editing rights for shared documents; and

(ii) protocols for any ancillary feature the Chief Information Officer identifies to support the core primary collaboration technology feature, including participation features available within video meetings;

(B) to the extent possible, is based on open standards;

(C) to the extent possible, is based on standards planned, developed, established, or coordinated using procedures consistent with those for voluntary consensus standards;

(D) subject to paragraph (3), uses end-to-end encryption technology;

(E) incorporates protocols, guidance, and requirements based on best practices for the cybersecurity of collaboration technology and collaboration technology features;

(F) to the extent practicable, integrates cybersecurity technology designed to protect communications from surveillance by foreign adversaries, including technology to protect communications metadata from traffic analysis, with requirements developed in consultation with such others as the Chief Information Officer considers relevant;

(G) to the extent practicable, is usable by, or offers options for, users with internet connections that have low-bandwidth or high-latency;

(H) subject to paragraph (5), with respect to the use of primary collaboration technology features, adds requirements to the identified standards that enables compliance with record retention and disclosure obligations, and permit internal lawful access for law enforcement purposes; and

(I) to the extent practicable, is compatible with all relevant information management rules, regulations, and policies, without the need for waivers or exceptions to such requirements.

(3) END-TO-END ENCRYPTION REQUIREMENTS.—

(A) IN GENERAL.—The end-to-end encryption technology selected as part of the identified standards under paragraph (2), to the extent practicable, shall ensure that collaboration and communications content data cannot be compromised if a third-party hosting server is compromised.

(B) END-TO-END ENCRYPTION NOT AVAILABLE.—Subject to subparagraph (C), if the Chief Information Officer has identified an ancillary feature or function for a primary collaboration technology feature and is unable to identify a standard, or set of standards, that uses end-to-end encryption and that is compatible with such ancillary feature or function, the Chief Information Officer may identify a standard or set of standards that does not utilize end-to-end encryption that may be used to support the ancillary feature or function.

(C) END-TO-END ENCRYPTION BY DEFAULT.—

(i) IN GENERAL.—Subject to clause (ii), the Chief Information Officer shall ensure that, with respect to the use of standards-compatible collaboration technology

that offers an ancillary technology feature or function described in subparagraph (B)—

(I) the ancillary feature or function is disabled by default; and

(II) the primary collaboration technology feature uses end-to-end encryption.

(ii) EXCEPTION.—Clause (i) shall not apply to the use of a primary collaboration technology feature with an ancillary feature or function described in subparagraph (B) if—

(I) the Chief Information Officer has enabled the use of the ancillary feature or function within the Department;

(II) each user of the ancillary feature or function has been notified of the additional cybersecurity and surveillance risks accompanying the use of the ancillary feature or function;

(III) each user of the ancillary feature or function has explicitly

opted into the use of the ancillary feature or function; and

(IV) the primary collaboration technology feature offers a means for the Chief Information Officer to collect aggregate statistics about the use of the options that are not end-to-end encrypted.

(D) ENCRYPTION STATUS TRANSPARENCY.—To the extent practicable, the Chief Information Officer shall identify protocols, guidance, or requirements to ensure that standards-compatible collaboration technology provides users the ability to easily see the encryption status of any collaboration feature in use.

(4) CONSIDERATIONS.—In identifying the identified standards, the Chief Information Officer shall consider secure, standards-based technologies adopted by a component or element of the Department, allies of the United States, State and local governments, and the private sector.

(5) COMPLIANCE WITH RECORD-KEEPING REQUIREMENTS.—The Chief Information Officer shall ensure, to the greatest extent practicable, that the

requirements added to the identified standards to achieve compliance with record retention and disclosure obligations, and to permit internal lawful access for law enforcement purposes—

(A) preserve the security benefits of end-to-end encryption, including that only specifically authorized personnel of the Department can access retained records of collaboration;

(B) avoid storing information, like plaintext messages or decryption keys, that would compromise the security of communications content data if a third-party hosting server were compromised;

(C) minimize other cybersecurity risks; and

(D) require that all users party to a communication be notified that the communications content data is being saved for archival purposes.

(6) WAIVER TO EXTEND DEADLINE FOR STANDARDS IDENTIFICATION.—

(A) IN GENERAL.—If the Chief Information Officer determines that it is infeasible to identify a standard for a particular primary collaboration technology feature not later than two years after the date of enactment of this Act,

the Chief Information Officer may issue a waiver to extend the deadline for the identification of such standard for the particular primary collaboration technology feature.

(B) WAIVER REQUIREMENTS.—A waiver described in subparagraph (A) shall include—

(i) the particular primary collaboration technology feature for which the waiver is issued; and

(ii) an explanation of the reason for which it is currently infeasible to identify a standard meeting the requirements under paragraph (2).

(C) WAIVER DURATION.—A waiver issued by the Chief Information Officer under subparagraph (A) shall be valid for one year.

(D) WAIVER RE-ISSUANCE.—The Chief Information Officer may re-issue a waiver under paragraph (1) for a primary collaboration technology feature not more than ten times.

(c) REQUIREMENT TO USE IDENTIFIED STANDARDS.—

(1) IN GENERAL.—On and after the date that is four years after the date on which the Chief Information Officer identifies the identified standards,

the head of a component or element of the Department may only procure collaboration technology if the collaboration technology is standards-compatible collaboration technology.

(2) EXCEPTION FOR PARTICULAR COLLABORATION SYSTEMS.—The following collaboration systems shall not be subject to the requirements under paragraph (1):

(A) Email.

(B) Voice services, as defined in section 227(e) of the Communications Act of 1934 (47 U.S.C. 227(e)).

(C) National security systems, as defined in section 11103(a) of title 40, United States Code.

(3) EXCEPTION FOR POST-PURCHASE CONFIGURATION.—If a software product or a device with a software operating system has built-in primary collaboration technology features that are not compatible with the identified standards, and the Chief Information Officer cannot procure the product or device with those primary collaboration technology features disabled before purchase, the Chief Information Officer may comply with this subsection by disabling the primary collaboration technology features

that are not compatible with the identified standards before provisioning the software product or device to an employee of the Department.

(4) CERTIFICATION FOR WAIVER.—

(A) CERTIFICATION.—The Chief Information Officer may issue a certification for waiver of the prohibition under paragraph (1) with respect to a particular collaboration technology.

(B) REQUIREMENT.—A certification under subparagraph (A) shall cite not less than one specific reason, which shall not be a generalized national security claim, for which the Department is unable to procure standards-compatible collaboration technology that meets the needs of the Department.

(C) SUBMISSION.—The Chief Information Officer shall submit to the congressional defense committees a copy of each certification issued under subparagraph (A).

(D) PUBLISHING.—

(i) ACCESSIBLE POSTING.—The Chief Information Officer shall publish a copy of each certification issued under subparagraph (A) on the website of the Department.

(ii) NATIONAL SECURITY.—The Secretary of Defense may waive the requirement of subclause (i) on a case-by-case basis if the Secretary certifies, in writing, to the congressional defense committees that publicly posting the waiver described in subparagraph (A) would harm the national security of the United States.

(E) DURATION; RENEWAL.—A certification with respect to a particular collaboration technology under this paragraph shall result in a waiver of the prohibition for that particular collaboration technology under paragraph (1)(B) that—

(i) shall be valid for a four-year period; and

(ii) may be renewed by the Chief Information Officer, after conducting a new assessment of available standards-collaboration technology.

(d) ATTESTATION OF COMPLIANCE AND INTEROPERABILITY TEST RESULTS.—

(1) INTEROPERABILITY TEST.—Not later than one year after the date on which the Chief Information Officer identifies the identified standards, the

Chief Information Officer shall identify third-party online interoperability test suites, including not less than one free test suite, or develop a free online interoperability test suite if no suitable third-party test suite can be identified, which shall—

(A) enable any entity to test whether an implementation of a primary collaboration technology feature has interoperability with the identified standards; and

(B) offer an externally-shareable version of the interoperability test results that can be provided as part of a demonstration of compliance under paragraph (2).

(2) DEMONSTRATION OF COMPLIANCE.—In order to demonstrate that a collaboration technology is a standards-compatible collaboration technology, the provider of the collaboration technology shall provide to the Chief Information Officer—

(A) an attestation that includes an affirmation that—

(i) each primary collaboration technology feature of the collaboration technology, by default—

(I) uses the relevant standard or standards from the identified stand-

ards for the primary collaboration technology feature to interoperate with other instances of standards-compatible collaboration technology; and

(II) follows all guidance and requirements from the identified standards that is applicable to the primary collaboration technology feature; and

(ii) the collaboration technology enables the Chief Information Officer to disable the ability of users to use modes of the collaboration technology that are not compatible with the identified standards; and

(B) interoperability test results described in paragraph (1)(B) that demonstrate interoperability with the identified standards for each primary collaboration technology feature the collaboration technology offers.

(3) PUBLICATION OF STANDARDS-COMPATIBLE COLLABORATION TECHNOLOGY VENDORS.—Upon a review of the materials submitted under paragraph (2), the Chief Information Officer shall publish on the website of the Department a list of each collabo-

ration technology that the Chief Information Officer has determined to be a standards-compatible collaboration technology.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require a collaboration technology vendor to directly test the interoperability of a primary collaboration technology feature with the product of another collaboration technology vendor.

(e) CYBERSECURITY REVIEWS OF COLLABORATION TECHNOLOGY PRODUCTS.—

(1) IN GENERAL.—Not later than four years after the date on which the Chief Information Officer identifies the identified standards, the Chief Information Officer shall conduct security reviews of collaboration technology products used within the Department, to identify any cybersecurity vulnerability or threat relating to those collaboration technology products.

(2) SELECTION AND PRIORITIZATION.—With respect to collaboration technology products selected for security reviews under paragraph (1), the Chief Information Officer shall determine the number of products, the specific products, and the prioritization

of products for security review, considering factors including—

(A) the total number of users across the Department using a collaboration technology product; and

(B) an estimation of the likelihood of a collaboration technology product being targeted for hacking.

(3) REPORT.—Not later than 30 days after the date on which the Chief Information Officer conducts security reviews under paragraph (1), the Chief Information Officer shall submit to the congressional defense committees a report on the results of the security reviews.

(f) UPDATES TO IDENTIFIED STANDARDS.—

(1) SOLICITATION OF FEEDBACK.—The Chief Information Officer shall regularly solicit feedback from within the Department to identify areas of improvement of the identified standards, desired collaboration technology features, and barriers to the adoption of standards-compatible collaboration technology.

(2) UPDATES AUTHORIZED.—The Chief Information Officer may update the identified standards based on feedback received under paragraph (1),

evolutions in collaboration technology feature offerings, cybersecurity best practices, or any other factor the Chief Information Officer determines.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed—

(1) to limit the ability of the Department to communicate with other entities using standards-compatible collaboration technology;

(2) to limit the ability of other entities to use the identified standards or standards-compatible collaboration technology;

(3) to limit the ability of the Department to apply, implement, and enforce other information management policies, regulations, and requirements with respect to standards-compatible collaboration technology;

(4) to affect any of the authorities of the Director of National Intelligence or the Office of the Director of National Intelligence; or

(5) to affect information technology-related procurement for the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

☒