118TH CONGRESS
1ST SESSION

S. _____

To establish standards for collaboration technology of the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish standards for collaboration technology of the Federal Government, 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 ''Secure and Interoperable Government Collaboration Technology Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of General Services.

(2) AGENCY.—The term ''agency''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes the Federal Election Commission.

(3) COLLABORATION TECHNOLOGY.—The term ''collaboration technology'' means a software system or application that offers 1 or more primary collaboration technology features.

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

(5) 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.

(6) IDENTIFIED STANDARDS.—The term ''identified standards'' means the standard, or set of standards, identified under section 3(b).

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

(8) OPEN STANDARD.—The term ''open standard'' means a voluntary consensus standard, or a set of voluntary consensus 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.

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

(A) facilitates remote work and collaboration within the Federal Government;

(B) facilitates the work and collaboration described in subparagraph (A) by providing functionality that is core or essential, rather than ancillary or secondary; and

(C) is identified by the Administrator under section 3(a).

(10) 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 section 5(b).

(11) VOLUNTARY CONSENSUS STANDARD.—The term ''voluntary consensus standard'' has the meaning given that 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.

(12) WORKING GROUP.—The term ''working group'' means the collaboration technology working group established under section 7(a).

SEC. 3. IDENTIFYING STANDARDS FOR GOVERNMENT COLLABORATION TECHNOLOGY.

(a) IDENTIFICATION OF FEATURES.—Not later than 180 days after the date of enactment of this Act, the Ad-

ministrator, in collaboration with the Director of the Office of Management and Budget and the Chief Information Officers Council, shall identify a list of primary collaboration technology features, including—

(1) voice and video calling, including—

(A) calling between 2 individuals; and

(B) calling between not less than 3 individuals;

(2) text-based messaging;

(3) file sharing;

(4) live document editing;

(5) scheduling and calendaring; and

(6) any other technology feature or function that the Administrator considers appropriate.

(b) IDENTIFICATION OF STANDARDS.—Not later than 2 years after the date of enactment of this Act, the Director shall identify a voluntary consensus standard, or set of voluntary consensus standards, for collaboration technology used by the Federal Government that—

(1) 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—

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

(i) identifying and authenticating the individuals 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

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

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

(3) subject to subsection (c), uses end-to-end encryption technology;

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

(5) to the extent practicable, integrates cybersecurity technology designed to protect communica-

tions from surveillance by foreign adversaries, including technology to protect communications metadata from traffic analysis, with requirements developed in consultation with the Secretary of Homeland Security, the Director of the National Security Agency, the Director of the Defense Advanced Research Projects Agency, the Director of the Intelligence Advanced Research Projects Activity, the Chief of Naval Research, and the President of the Open Technology Fund;

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

(7) subject to subsection (e), with respect to the use of primary collaboration technology features, enables agencies subject to Federal record-keeping requirements to comply with those requirements and section 552 of title 5, United States Code.

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

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

(2) END-TO-END ENCRYPTION NOT AVAILABLE.—Subject to paragraph (3), if the Administrator has identified an ancillary feature or function for a primary collaboration technology feature and the Director 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 Director 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.

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

(A) IN GENERAL.—Subject to subparagraph (B), the head of an agency shall ensure that, with respect to the use of standards-compatible collaboration technology that offers an ancillary technology feature or function described in paragraph (2) by the agency—

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

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

(B) EXCEPTION.—Subparagraph (A) shall not apply to an agency using a primary collabo-

ration technology feature with an ancillary feature or function described in paragraph (2) if—

(i) the head of the agency has enabled the use of the ancillary feature or function within the agency;

(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 head of the agency to collect aggregate statistics about the use of the options that are not end-to-end encrypted.

(4) ENCRYPTION STATUS TRANSPARENCY.—To the extent practicable, the Director 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.

(d) CONSULTATION AND ADDITIONAL CONSIDERATIONS.—In identifying the identified standards, the Director shall—

(1) consult with the Director of the Office of Management and Budget, the Administrator, the Secretary of Homeland Security, the Director of National Intelligence, the National Association of State Chief Information Officers, the Sergeant at Arms of the Senate, the Chief Administrative Officer of the House of Representatives, the Federal Communications Commission, the National Telecommunications and Information Administration, the Director of the Administrative Office of the United States Courts, and the Archivist of the United States; and

(2) consider other secure, standards-based technologies adopted by allies of the United States, State and local governments, and the private sector.

(e) COMPLIANCE WITH RECORD-KEEPING REQUIREMENTS.—The Director shall ensure that requirements added to the identified standards to achieve compliance with Federal record-keeping requirements—

(1) are designed in consultation with the Archivist of the United States; and

(2) to the greatest extent practicable—

(A) preserve the security benefits of end-to-end encryption;

(B) avoid storing information, like plaintext messages or decryption keys, that would compromise the security of communications content data if a 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.

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

(1) IN GENERAL.—If the Director determines that it is infeasible to identify a standard for a particular primary collaboration technology feature not later than 2 years after the date of enactment of this Act, the Director may issue a waiver to extend the deadline for the identification of such standard for the particular primary collaboration technology feature.

(2) WAIVER REQUIREMENTS.—A waiver described in paragraph (1) shall include—

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

(B) an explanation of the reason for which it is currently infeasible to identify a standard meeting the requirements under subsection (b).

(3) WAIVER DURATION.—A waiver issued by the Director under paragraph (1) shall be valid for 1 year.

(4) WAIVER RE-ISSUANCE.—The Director may re-issue a waiver under paragraph (1) for a primary collaboration technology feature not more than 10 times.

SEC. 4. REQUIREMENT TO USE IDENTIFIED STANDARDS.

(a) IN GENERAL.—

(1) INTEGRATION.—Not later than 4 years after the date on which the Director identifies the identified standards—

(A) the Federal Acquisition Regulatory Council shall integrate compatibility with the identified standards as part of Federal Acquisition Regulation for collaboration technology products that offer 1 or more primary collaboration technology features; and

(B) the Secretary of Homeland Security shall develop technical guidance for agencies on selecting and configuring standards-compatible collaboration technology.

(2) PROHIBITION ON PROCUREMENT.—Effective 4 years after the date on which the Director identifies the identified standards, the head of an agency may not procure collaboration technology that is not standards-compatible collaboration technology.

(b) EXCEPTION FOR PARTICULAR COLLABORATION SYSTEMS.—The following collaboration systems shall not be subject to the requirements under subsection (a):

(1) Email.

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

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

(c) 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 head of an agency cannot procure the product or device with those primary collaboration tech-

nology features disabled before purchase, the head of the agency may comply with this section 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 agency.

(d) CERTIFICATION FOR WAIVER.—

(1) CERTIFICATION.—The head of an agency may issue a certification for waiver of the prohibition under subsection (a)(2) with respect to a particular collaboration technology.

(2) REQUIREMENT.—A certification under paragraph (1) shall cite not less than 1 specific reason for which the agency is unable to procure standards-compatible collaboration technology that meets the needs of the agency.

(3) SUBMISSION.—The head of an agency shall submit to the congressional committees of jurisdiction of the agency a copy of each certification issued under paragraph (1).

(4) ACCESSIBLE POSTING.—The head of an agency shall post a copy of each certification issued under paragraph (1) at a standardized location on the website of the agency specified by the Director of the Office of Management and Budget.

(5) DURATION; RENEWAL.—A certification with respect to a particular collaboration technology under this subsection shall result in a waiver of the prohibition for that particular collaboration technology under subsection (a)(2) that—

(A) shall be valid for a 4-year period; and

(B) may be renewed by the head of the agency.

SEC. 5. ATTESTATION OF COMPLIANCE AND INTEROPERABILITY TEST RESULTS.

(a) INTEROPERABILITY TEST.—Not later than 1 year after the date on which the Director identifies the identified standards, the Director shall identify third-party online interoperability test suites, including not less than 1 free test suite, or develop a free online interoperability test suite if no suitable third-party test suite can be identified, which shall—

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

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

(b) 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 Administrator—

(1) an attestation that includes an affirmation that—

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

(i) uses the relevant standard or standards from the identified standards 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

(B) the collaboration technology enables the head of an agency to disable the ability of users to use modes of the collaboration technology that are not compatible with the identified standards; and

(2) interoperability test results described in subsection (a)(2) that demonstrate interoperability with the identified standards for each primary collaboration technology feature the collaboration technology offers.

(c) PUBLICATION OF STANDARDS-COMPATIBLE COLLABORATION TECHNOLOGY VENDORS.—Upon a review of the materials submitted under subsection (b), the Administrator shall publish on the website of the General Services Administration a list of each collaboration technology that the Administrator has determined to be a standards-compatible collaboration technology.

(d) RULE OF CONSTRUCTION.—Nothing in this section 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.

SEC. 6. CYBERSECURITY REVIEWS OF COLLABORATION TECHNOLOGY PRODUCTS.

(a) IN GENERAL.—Not later than 4 years after the date on which the Director identifies the identified standards, using the authority under section 3553(b)(7) of title 44, United States Code, the Secretary of Homeland Security shall conduct security reviews of collaboration technology products used within the Federal Government, to

identify any cybersecurity vulnerability or threat relating to those collaboration technology products.

(b) SELECTION AND PRIORITIZATION.—With respect to collaboration technology products selected for security reviews under subsection (a), the Secretary of Homeland Security shall determine the number of products, the specific products, and the prioritization of products for security review, considering factors including—

(1) the number of agencies using a collaboration technology product;

(2) the total number of users across agencies using a collaboration technology product; and

(3) an estimation of the likelihood of a particular agency or a collaboration technology product being targeted for hacking.

(c) REPORT.—Not later than 30 days after the date on which the Secretary of Homeland Security conducts security reviews under subsection (a), the Secretary of Homeland Security shall submit a report on the results of the security reviews to—

(1) the Committee on Homeland Security and Governmental Affairs of the Senate;

(2) the Committee on Homeland Security of the House of Representatives; and

(3) the relevant congressional committees of jurisdiction of the agencies using the reviewed technology products.

SEC. 7. COLLABORATION TECHNOLOGY WORKING GROUP AND UPDATES TO IDENTIFIED STANDARDS.

(a) WORKING GROUP.—Not later than 60 days after the date of enactment of this Act, the Administrator, in collaboration with the Director of the Office of Management and Budget, shall establish a collaboration technology working group that produces biennial updates to the list of primary collaboration technology features identified under section 3(a).

(b) COLLECTION OF AGENCY FEEDBACK.—During the 10-year period following the date on which the Director identifies the identified standards, not less frequently than once every 2 years, the working group shall develop a report that compiles feedback solicited from agencies, including—

(1) with respect to agencies using standards-compatible collaboration technology, areas of improvement of the identified standards and desired features; and

(2) with respect to agencies not using standards-compatible collaboration technology, barriers to the adoption of standards-compatible collaboration

technology, including the reasons cited in all certifications issued under section 4(c).

(c) SUBMISSION OF AGENCY FEEDBACK.—Not later than 30 days after the date on which a report under subsection (b) is completed, the working group shall submit such report to the Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Government Reform of the House of Representatives.

(d) INCORPORATION OF REQUESTED FEATURES AND REQUIREMENTS.—To the extent practicable, the Director shall update the identified standards to incorporate features and requirements identified—

(1) by the working group under subsection (a); and

(2) in the reports submitted under subsection (c).

(e) UPDATES TO IDENTIFIED STANDARDS.—The Director may update the identified standards based on evolutions in collaboration technology feature offerings, cybersecurity best practices, or any other factor the Director determines.

SEC. 8. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed to limit the ability of—

(1) agencies to communicate with non-government entities using standards-compatible collaboration technology; or

(2) non-government entities to use the identified standards or standards-compatible collaboration technology.