119TH CONGRESS
2D SESSION

S. _____

To establish a public-private working group to develop cybersecurity best practices for telecommunications carriers and related supply chain participants, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER (for himself and Mr. CRUZ) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish a public-private working group to develop cybersecurity best practices for telecommunications carriers and related supply chain participants, 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 ''Telecommunications Cybersecurity and Resilience Act''.

SEC. 2. DEFINITIONS.

In this Act :

(1) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Commerce for Communications and Information.

(2) ELIGIBLE ENTITY.—The term ''eligible entity'' means—

(A) a telecommunications carrier; or

(B) any other telecommunications sector or related supply chain stakeholder for which Industry Best Practices are developed under section 4.

(3) CISA.—The term ''CISA'' means the Cybersecurity and Infrastructure Security Agency.

(4) COMMISSION.—The term ''Commission'' means the Federal Communications Commission.

(5) CSRMA.—The term ''CSRMA'' means Communications Sector Risk Management Agency.

(6) CSRIC.—The term ''CSRIC'' means the Communications Security, Reliability, and Interoperability Council Federal advisory committee to the Commission.

(7) INDUSTRY BEST PRACTICES.—The term ''Industry Best Practices'' means voluntary cybersecurity frameworks and best practices for eligible entities described in section 4(a).

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

(9) NIST CSF.—The term ''NIST CSF'' means the latest version of the NIST Cybersecurity Framework.

(10) NSA.—The term ''NSA'' means the National Security Agency.

(11) NTIA.—The term ''NTIA'' means the National Telecommunications and Information Administration.

(12) ODNI.—The term ''ODNI'' means the Office of the Director of National Intelligence.

(13) ONCD.—The term ''ONCD'' means the Office of the National Cyber Director.

(14) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

(15) TELECOMMUNICATIONS CARRIER.—The term ''telecommunications carrier'' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(16) WORKING GROUP.—The term ''Working Group'' means the Telecommunications Cybersecurity Working Group established under section 3(a).

SEC. 3. TELECOMMUNICATIONS CYBERSECURITY WORKING GROUP.

(a) ESTABLISHMENT.—There is established, within NTIA, a public-private advisory body to be known as the ''Telecommunications Cybersecurity Working Group'' that shall—

(1) develop Industry Best Practices, including associated adoption instructions and materials as outlined in section 4;

(2) create a network of independent third-party assessors eligible to certify implementation and maintenance of best practices under section 5, including criteria for such assessors; and

(3) provide and advise on technical feedback and implementation guidance relating to Industry Best Practices developed pursuant to paragraph (1).

(b) MEMBERSHIP.—

(1) IN GENERAL.—The Working Group shall include representatives from NTIA, CISA, NIST, ODNI, ONCD, NSA, the Commission, and industry members appointed in accordance with paragraph (2).

(2) INITIAL APPOINTMENT OF INDUSTRY MEMBERS.—The Assistant Secretary shall appoint initial members of the Working Group that, to the extent practicable, represent the following stakeholder categories:

(A) National telecommunications carriers.

(B) Regional and rural telecommunications carriers, including small and medium-sized telecommunications providers.

(C) Communications sector suppliers, including network infrastructure and equipment manufacturers.

(D) Software and systems providers that offer cloud services, network management, or cybersecurity tools.

(E) State and local government communications or emergency network operators.

(F) Independent cybersecurity experts and representatives of academia.

(G) Other relevant supply chain stakeholders, as jointly determined by the co-chairs.

(3) TERMS AND VACANCIES OF INDUSTRY MEMBERS.—

(A) TERMS.—Each industry member of the Working Group shall serve 1 term of not

longer than 2 years and may be reappointed for 1 successive term.

(B) VACANCY REPLACEMENT.—The Working Group shall develop a vacancy replacement procedure that includes—

(i) for vacancies occurring due to the end of an industry member's term, a vote not later than 90 days before the last day of the industry member's term; and

(ii) for vacancies occurring under paragraph (4) or for any other reason, joint nomination of a replacement by the co-chairs from the same stakeholder category under paragraph (2), to the extent practicable, as the industry member creating the vacancy, subject to approval by a majority vote of the members of the Working Group.

(4) REMOVAL.—Any member that fails to comply with the conflict of interest policy adopted pursuant to subsection (c)(4) shall be removed from the Working Group.

(5) CO-CHAIRS.—The Working Group shall have 2 co-chairs, of which—

(A) 1 shall be the Assistant Secretary; and

(B) 1 shall be selected by a majority vote among a quorum of the industry members appointed in accordance with paragraph (2).

(6) MEMBER ACCESS TO CLASSIFIED INFORMATION.—

(A) ACCESS.—

(i) IN GENERAL.—Not later than 60 days after the date on which a member is first selected to the Working Group and before the member is granted access to any classified information necessary to participate in a closed session pursuant to subsection (c)(6), the Assistant Secretary shall determine, for the purposes of the Working Group, if the member should be restricted from reviewing, discussing, or possessing classified information.

(ii) MANAGEMENT.—Access to classified materials shall be managed in accordance with Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or any subsequent corresponding Executive Order.

(B) PROTECTION OF INFORMATION.—A member of the Working Group granted access

to classified information shall protect the classified information in accordance with the applicable requirements for the particular level of classification of the information.

(C) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to affect the security clearance of a member of the Working Group or the authority of a Federal agency to provide a member of the Working Group access to classified information.

(c) PROCEDURES.—

(1) DESIGNATED FEDERAL OFFICER.—The Assistant Secretary shall designate a Federal officer or employee to serve as the Designated Federal Officer of the Working Group, consistent with the requirements of chapter 10 of title 5, United States Code (commonly known as the ''Federal Advisory Committee Act'').

(2) INITIAL MEETING AND BYLAWS.—Not later than 120 days after the date of enactment of this Act, the Working Group shall convene and establish bylaws that—

(A) govern quorum and voting rules;

(B) set deliverable timelines and meeting schedules; and

(C) create procedures for recommending third-party certification assessors, including conflict-of-interest protocols.

(3) OPERATING PROCEDURES.—Unless otherwise specified, the Working Group shall adopt written procedures governing its meetings, consistent with chapter 10 of title 5, United States Code, that include—

(A) requirements for public notice of meetings and the maintenance of records and minutes;

(B) decision-making by majority vote of those present and voting, or in accordance with the voting rules established in the bylaws;

(C) authorization for the establishment of subgroups as necessary, subject to the approval of the co-chairs; and

(D) approval of the meeting agendas by the co-chair described in subsection (b)(5)(A), in consultation with the co-chair described in subsection (b)(5)(B) and the Designated Federal Officer of the Working Group to ensure compliance with applicable laws.

(4) CONFLICT-OF-INTEREST POLICY.—

(A) IN GENERAL.—The Working Group shall adopt and enforce a written conflict of interest policy to ensure that members have a fiduciary responsibility to the Working Group, a duty to report conflicts of interest, including the appearance of a conflict of interest, and do not participate in deliberations or votes from which they personally or their employer would directly and materially benefit.

(B) REQUIRED DISCLOSURES.—The policy under subparagraph (A) shall require each member to publicly disclose all relevant financial and employment relationships and include recusal procedures in the event of a conflict.

(C) RECORDS.—The Designated Federal Officer of the Working Group shall maintain records of disclosures under subparagraph (B) and make summaries of the disclosures available to NTIA.

(5) THREAT INFORMATION ACCESS.—ODNI, in coordination with other appropriate Federal entities, shall ensure that the Working Group has access to relevant cybersecurity threat information, including through closed or classified briefings for members eligible to receive such information, when appropriate.

(6) CLOSED SESSIONS.—Notwithstanding section 1009 of title 5, United States Code, the Working Group may hold closed or restricted-access sessions when the Assistant Secretary determines that the matters to be discussed involve any of the following:

(A) Classified information.

(B) Sensitive cybersecurity vulnerabilities.

(C) Threat information.

(D) Proprietary business information.

(E) Other information exempt from public disclosure under section 552 of title 5, United States Code.

(d) TRANSPARENCY AND COMMUNICATION.—The Assistant Secretary shall—

(1) publish Industry Best Practices, implementation guidance, and criteria for third-party assessors;

(2) publish on the website of NTIA and submit to the relevant congressional committees the bylaws, membership, and procedures of the Working Group; and

(3) publish a memorandum of understanding (or equivalent written coordination instrument) among NTIA, CISA (acting through the CSRMA),

NIST, and the Commission describing roles, coordination, and non-duplication procedures under this Act.

(e) TERMINATION OF ADVISORY COMMITTEE.—Section 1013(a) of title 5, United States Code, shall not apply with respect to the Working Group.

SEC. 4. DEVELOPMENT OF INDUSTRY BEST PRACTICES FOR CYBERSECURITY.

(a) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Working Group shall, in consultation with the heads of NTIA, CISA, NIST, ODNI, ONCD, NSA, and the Commission, develop and maintain cybersecurity best practices (and corresponding implementation guidance), referred to in this Act as ''Industry Best Practices'', for telecommunications carriers and other eligible entities that—

(1) are for carriers and communications sector suppliers and the telecommunications sector to elect to implement and maintain;

(2) are issued and maintained by CISA, acting through the CSRMA, with NTIA serving as the convener and administrative home for the Working Group;

(3) apply, as appropriate, to communications sector suppliers and other supply chain participants,

which may participate as eligible entities for purposes of certification under section 5;

(4) focus solely on identifying, responding to, mitigating, preventing, and remediating cybersecurity incidents and vulnerabilities;

(5) are risk-based and consistent with other Federal cybersecurity risk management frameworks, including CISA sector guidance, the NIST Cybersecurity Framework, the NIST Risk Management Framework, and relevant cybersecurity guidance developed pursuant to Executive Order 14028 (44 U.S.C. 3551 note; relating to improving the nation's cybersecurity), including those for communications subsectors, and any relevant successor guidance;

(6) may account for, as appropriate, relevant cybersecurity requirements and certifications of a current member of the North Atlantic Treaty Organization, a major non-NATO ally (as designated under section 517 of the Foreign Assistance Act of 1961 (22 U.S.C. 2321k)), or a member of the Five Eyes countries (as defined in section 1606(c) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (10 U.S.C. 2271 note)), including as relevant to interoperability or avoiding unnecessary duplication;

(7) avoid duplication of existing cybersecurity risk management processes; and

(8) reflect available threat intelligence, Federal cybersecurity advisories, and technological developments at the time of development or update.

(b) INDUSTRY BEST PRACTICES CONTENTS.—The Industry Best Practices may include –

(1) application of security updates to network devices, as available;

(2) the timely decommissioning, or implementation of secure alternative mitigations, of network devices owned by and under the control and management of the telecommunications carrier that no longer receive updates by the original equipment manufacturer to address identified security vulnerabilities in the network device;

(3) the creation and maintenance of configuration management practices for the hardware, software, or firmware, or a combination thereof, of network devices owned by or under the control and management of the telecommunications carrier including, at a minimum, a baseline configuration and configuration management plan that align with internal security policies and NIST CSF 2.0 industry best practices;

(4) implementation of appropriate multi-factor authentication, or identity control and access management measures; and

(5) other such practices as established by the Working Group.

(c) REVIEW AND UPDATE.—The Working Group shall review and update Industry Best Practices (and corresponding implementation guidance) not less frequently than once every 2 years, and interim updates may be made in response to significant cybersecurity incidents or material changes in threat conditions if determined necessary by the Working Group, to reflect evolving cybersecurity risks and technologies.

(d) USE OF EXISTING BODIES.—In carrying out this section, the Working Group may consult with other public-private advisory councils and relevant information-sharing organizations, as well as any Federal entities, including the Commission, NTIA, and CISA, that the Working Group determines may be capable of providing meaningful insight with respect to the development of Industry Best Practices (and corresponding implementation guidance).

(e) PUBLICATION AND GUIDANCE ACCESS.—

(1) IN GENERAL.—The Assistant Secretary shall publish Industry Best Practices (and corresponding implementation guidance) on the website

of NTIA, to promote transparency and encourage voluntary alignment across the telecommunications sector.

(2) GUIDANCE.—

(A) WITHHOLDING FOR CYBERSECURITY.—The Assistant Secretary, in consultation with the head of CISA, may withhold detailed implementation guidance from public release to mitigate cybersecurity risks, provided that the implementation guidance is made available to eligible entities and eligible cybersecurity assessors for purposes of certification under section 5.

(B) EXEMPTION FROM DISCLOSURE.—Detailed implementation guidance withheld under subparagraph (A) is exempt from disclosure under section 552(b)(3) of title 5, United States Code.

(C) NO USE FOR REGULATORY ENFORCEMENT.—No information disclosed by an eligible entity for the purposes of informing guidance published or disclosed pursuant to this paragraph may be used in any regulatory proceeding or enforcement action.

(D) RULE OF CONSTRUCTION (NO NEW COMMISSION AUTHORITY).—Nothing in this Act shall be construed to expand the authority of the Commission to promulgate or enforce cybersecurity regulations, or to require adoption of Industry Best Practices, which eligible entities may elect to adopt.

(E) NO ADVERSE INFERENCE.—No regulatory agency may draw any inferences from an eligible entity choosing not to adopt Industry Best Practices or implementation guidance.

SEC. 5. CYBERSECURITY CERTIFICATION REQUIREMENTS FOR ELIGIBLE ENTITIES.

(a) ELIGIBLE ASSESSOR CRITERIA AND PUBLICATION.—

(1) DEVELOPMENT AND APPROVAL OF CRITERIA.—

(A) DEVELOPMENT OF CRITERIA.—The Working Group shall determine, and the Assistant Secretary shall approve, criteria for independent third-party cybersecurity assessors.

(B) DOCUMENTATION.—In developing the criteria under subparagraph (A), the Working Group shall publish the assessment criteria and general methodology to be used by eligible cy-

bersecurity assessors, except for information the Assistant Secretary determines should be withheld to mitigate cybersecurity risks.

(2) PUBLICATION OF ELIGIBLE CYBERSECURITY ASSESSORS.—The Assistant Secretary shall—

(A) establish an evaluation process and assessment standard for designating eligible cybersecurity assessors;

(B) publish a list of eligible cybersecurity assessors designated pursuant to subparagraph (A) that a telecommunications carrier, or other eligible entity for which Industry Best Practices were developed, may elect to evaluate the telecommunication carrier's or eligible entity's implementation of Industry Best Practices and that may issue a proposed certification; and

(C) establish conditions under which to revoke or suspend the designation as an eligible cybersecurity assessor.

(3) PROHIBITION ON CERTAIN ASSESSORS.—No entity owned or controlled by a telecommunications carrier may be designated as an eligible cybersecurity assessor under this subsection.

(b) CERTIFICATION AND APPROVAL PROCESS.—

(1) APPROVAL OF CERTIFICATION.—

(A) SUBMISSION.—

(i) IN GENERAL.—A telecommunications carrier or other eligible entity that elects to have an eligible cybersecurity assessor evaluate the telecommunication carrier or eligible entity and receives a proposed certification may submit the proposed certification to the Assistant Secretary for approval.

(ii) FORMAT OF SUBMISSIONS.—The Assistant Secretary may require submissions of the proposed certification under clause (i) to be submitted in machine readable format in the Open Security Controls Assessment Language architecture developed by NIST, or a successor framework.

(B) CONTENTS OF SUBMISSION.—A submission under subparagraph (A) shall include—

(i) the full assessment report prepared by the eligible cybersecurity assessor;

(ii) documentation of the Industry Best Practices against which the telecommunications carrier or other eligible entity was evaluated; and

(iii) the disclosures required under subsection (c)(4).

(C) TIMEFRAME FOR DECISION.—Upon receipt of a proposed certification for approval, the Assistant Secretary shall, within 30 days, determine whether the submission is complete and, not later than 90 days after the date of such determination, approve or disapprove the complete proposed certification.

(D) DISAPPROVAL OF CERTIFICATION.—In the event that the Assistant Secretary disapproves a proposed certification under this paragraph, the Assistant Secretary shall inform the eligible entity of the basis for the disapproval.

(E) RIGHT TO CURE AND APPEAL.—

(i) RIGHT TO CURE.—An eligible entity the proposed certification of which was disapproved by the Assistant Secretary shall have 30 days to resubmit the proposed certification, during which period no adverse action shall be taken by the Assistant Secretary against the eligible entity on the basis of lacking a certification.

(ii) RIGHT TO APPEAL.—

(I) IN GENERAL.—An eligible entity described in clause (i) may appeal the disapproval to the Assistant Secretary.

(II) PROCESS.—The Assistant Secretary shall establish the manner and form in which appeals under this clause shall be heard and shall render a decision on any such appeal not later than 90 days after the date of the initiation of the appeal.

(2) EFFECT OF CERTIFICATION.—A certified telecommunications carrier or other eligible entity shall, in any Federal or State Court, be entitled to an affirmative defense that approval of a certification under paragraph (1) constitutes due care or reasonableness for mitigating, preventing, and remediating cybersecurity incidents and vulnerabilities, unless the telecommunications carrier or other eligible entity is found to have acted with gross negligence, willful misconduct, or have not materially implemented and maintained the Industry Best Practices consistent with the approved certification.

(3) TIMING; LATER CHANGE.—The defense under paragraph (2) shall apply if the eligible entity

was certified and in compliance with the Industry Best Practices in effect at the time of the incident, notwithstanding—

(A) subsequent revisions to Industry Best Practices; or

(B) subsequent expiration, subsequent suspension, or non-renewal of the certification.

(4) CONFLICT PREEMPTION.—No State or political subdivision of a State may establish, maintain, prescribe, continue, or enforce any law, rule, regulation, or requirement imposing a duty, standard, requirement, or liability or enforcing standards for cybersecurity that are inconsistent with this Act with respect to a certified eligible entity.

(c) CERTIFICATION REQUIREMENTS.—Each approved certification under subsection (b)(1) shall—

(1) be valid for a period of not more than 2 years;

(2) be renewable through comprehensive reassessment;

(3) include documentation of implementation and maintenance of the applicable Industry Best Practices at the time of certification;

(4) require disclosure of any direct financial interest or material business relationship between the assessor and the entity being assessed;

(5) include a description of the assessment methodology and criteria used; and

(6) be subject to revocation by the Assistant Secretary if the assessor is found to have issued invalid or false certifications.

(d) WHISTLEBLOWER PROTECTION.—

(1) IN GENERAL.—No eligible cybersecurity assessor or telecommunications carrier with an approved or pending certification, or any officer, employee, contractor, subcontractor, or agent of such company, may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the employee to provide information to, cause information to be provided to, or otherwise assist in an investigation by an agency, entity, or person described in paragraph (2),relating to any conduct that the employee reasonably believes reflects non-compliance with or gross misrepresentation relating to the certification standard established by the Working Group.

(2) AGENCY, ENTITY, OR PERSON DESCRIBED.—An agency, entity, or person described in this paragraph is—

(A) a Federal regulatory or law enforcement agency;

(B) any Member of Congress or any committee of Congress; or

(C) a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct).

(e) ROUTINE IMPLEMENTATION AND MAINTENANCE OBLIGATION.—A certified eligible entity shall routinely implement and maintain cybersecurity practices aligned with Industry Best Practices, as updated, during the period of certification.

(f) EARLY REASSESSMENT.—

(1) AUTHORITY.—

(A) IN GENERAL.—Upon any of the grounds described in paragraph (2), the Assistant Secretary may direct an eligible cybersecurity assessor to conduct, or may on the Assistant Secretary's own initiative commission by an alternative eligible cybersecurity assessor, an early reassessment of a certified eligible entity

and may, upon a written finding of credible evidence of material failure to implement or maintain the Industry Best Practices, suspend the approved certification of the eligible entity pending successful completion of the reassessment.

(B) RESPONSIBILITY FOR COSTS ASSOCIATED WITH ASSESSMENT.—If an assessment conducted pursuant to subparagraph (A) determines that the eligible entity has materially failed to implement or maintain the Industry Best Practices, the eligible entity shall be responsible for all costs associated with performing the assessment.

(2) GROUNDS FOR REASSESSMENT.—The grounds described in this paragraph include—

(A) a substantial revision to Industry Best Practices;

(B) a telecommunications carrier or other eligible entity experiences a significant cyber-incident, as defined by Presidential Policy Directive–41 (July 26, 2016; relating to United States cyber incident coordination); and

(C) the Assistant Secretary receives credible information that—

(i) any of the contents submitted to the Assistant Secretary under subsection (b)(1) to approve a certification were false or fraudulent; or

(ii) an eligible entity has failed to routinely implement and maintain cybersecurity practices in accordance with subsection (e).

(3) GOOD FAITH PROTECTION.—A certified telecommunications carrier or other eligible entity shall not have its certification under subsection (b) revoked solely due to an early reassessment under this subsection, unless and until the early reassessment produces a final determination that the eligible entity—

(A) materially failed to implement or maintain the Industry Best Practices the entity elected to adopt through the certification process; or

(B) has engaged in gross negligence or willful misconduct.

SEC. 6. REPORTING REQUIREMENTS.

(a) ANNUAL REPORT.—Not later than 1 year after the publication of any Industry Best Practices developed under section 4, and annually thereafter, the Assistant

Secretary, in consultation with the Working Group, shall submit to the relevant congressional committees and publish a public version on the website of NTIA a report that includes—

(1) an overview of the development of Industry Best Practices, and any updates or modifications of Industry Best Practices;

(2) data on participation of eligible entities in the certification process;

(3) a summary of early reassessment activity, if any;

(4) an assessment of the adoption of Industry Best Practices; and

(5) the effectiveness of Industry Best Practices and certification in enhancing cybersecurity across the telecommunications sector.

(b) EVENT-TRIGGERED REPORT.—Not later than 90 days after a substantial revision to Industry Best Practices or a significant cyber-incident, as defined in Presidential Policy Directive–41 (July 26, 2016; relating to United States cyber incident coordination), affecting the telecommunications sector, the Assistant Secretary, in consultation with the Working Group, shall submit to Congress a report that includes, to the greatest extent practicable, the consensus views and recommendations of the

Working Group to improve cybersecurity across the telecommunications sector.

SEC. 7. RULES OF CONSTRUCTION.

Nothing in this Act shall be construed to—

(1) grant any regulatory authority to any Federal agency;

(2) expand or otherwise alter obligations or authorities under the Communications Act of 1934 (47 U.S.C. 151 et seq.), the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601 et seq.), the Secure Equipment Act of 2021 (47 U.S.C. 1601 note), or any other Federal law;

(3) prohibit the Working Group from consulting with or referencing the work product of Federal advisory committees subject to chapter 10 of title 5, United States Code, including the President's National Security Telecommunications Advisory Committee, CSRIC, and the Commission's Technological Advisory Council;

(4) require adoption of Industry Best Practices or implementation guidance, or authorize any regulatory requirement of adoption;

(5) displace or replace the functions of any Federal advisory council or information-sharing agreement;

(6) grant regulatory authority to the Commission, or any other Federal body; or

(7) authorize, expand, or imply any Federal authority to supervise, direct, mandate, regulate, audit, or otherwise oversee the cybersecurity operations, risk-management programs, technical controls, or network security practices of any telecommunications carrier or other eligible entity, except as expressly permitted for the development, publication, and voluntary certification of Industry Best Practices under this Act.

SEC. 8. SEVERABILITY.

If any provision of this Act, or its application to any person or circumstance, is held to be unconstitutional, the remainder of this Act, and the application of the provision to any other person or circumstance, shall not be affected.