119TH CONGRESS
1ST SESSION

S. 1875

To establish an interagency committee to harmonize regulatory regimes in the United States relating to cybersecurity, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 22, 2025

Mr. PETERS (for himself and Mr. LANKFORD) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To establish an interagency committee to harmonize regulatory regimes in the United States relating to cybersecurity, 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 ''Streamlining Federal Cybersecurity Regulations Act of 2025''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 3502 of title 44, United States Code.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Oversight and Government Reform of the House of Representatives;

(C) each committee of Congress with jurisdiction over the activities of a regulatory agency; and

(D) each committee of Congress with jurisdiction over the activities of a Sector Risk Management Agency with respect to a sector regulated by a regulatory agency.

(3) COMMITTEE.—The term ''Committee'' means the Harmonization Committee established under section 3(a).

(4) CYBERSECURITY REQUIREMENT.—The term ''cybersecurity requirement'' means a regulation or supervisory activity, including an examination or binding guidance, that includes administrative, tech-

nical, or physical requirements relating to information security, security of information technology or operational technology, cybersecurity, or cyber risk or resilience.

(5) HARMONIZATION.—

(A) DEFINITION.—The term ''harmonization'' means the process of aligning cybersecurity requirements issued by regulatory agencies such that the requirements consist of—

(i) a common set of minimum requirements that may apply across sectors and that can be updated periodically to address new or evolving risks relating to information security or cybersecurity; and

(ii) sector-specific requirements, which may include performance-based requirements, that—

(I) are necessary to address sector-specific risks that are not adequately addressed by the minimum requirements described in clause (i);

(II) are substantially similar, where appropriate, to other requirements in that sector or a similar sector; and

(III) align with international standards, where appropriate.

(B) RULE OF CONSTRUCTION.—Nothing in this definition shall be construed to exempt regulatory agencies from any otherwise applicable processes or laws relating to promulgating or amending regulations, including subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly known as the ''Administrative Procedure Act'').

(6) HEAD.—The term ''head'' includes, in the case of an agency directed by multiple individuals, such as a commission, a representative selected by such individuals from among such individuals.

(7) INDEPENDENT REGULATORY AGENCY.—The term ''independent regulatory agency'' has the meaning given that term in section 3502 of title 44, United States Code.

(8) RECIPROCITY.—The term ''reciprocity'' means the recognition or acceptance by 1 regulatory agency of an assessment, determination, examination, finding, or conclusion of another regulatory agency for determining that a regulated entity has complied with a cybersecurity requirement.

(9) REGULATORY AGENCY.—The term ''regulatory agency'' means—

(A) any independent regulatory agency that has the statutory authority to issue or enforce any mandatory cybersecurity requirement; or

(B) any other agency that has the statutory authority to issue or enforce any cybersecurity requirement.

(10) REGULATORY FRAMEWORK.—The term ''regulatory framework'' means the framework developed under section 3(e)(1).

(11) SECTOR RISK MANAGEMENT AGENCY.—The term ''Sector Risk Management Agency'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

SEC. 3. ESTABLISHMENT OF INTERAGENCY COMMITTEE TO HARMONIZE REGULATORY REGIMES IN THE UNITED STATES RELATING TO CYBERSECURITY.

(a) HARMONIZATION COMMITTEE.—

(1) IN GENERAL.—The National Cyber Director shall establish an interagency committee to be known as the Harmonization Committee to enhance the harmonization and reciprocity of cybersecurity

requirements that are applicable within the United States, including the formulation of baseline and sector-specific requirements that are risk-based.

(2) SUPPORT.—The National Cyber Director shall provide the Committee with administrative and management support as appropriate.

(b) MEMBERS.—

(1) IN GENERAL.—The Committee shall be composed of—

(A) the National Cyber Director;

(B) the head of each regulatory agency, including the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology;

(C) the head of the Office of Information and Regulatory Affairs of the Office of Management and Budget; and

(D) the head of other appropriate agencies, as determined by the chair of the Committee.

(2) PUBLICATION OF LIST OF MEMBERS.—The Committee shall maintain, on a publicly available website, a list of the agencies that are represented on the Committee as determined by the chair of the Committee, and shall update the list as members are added or removed.

(c) CHAIR.—The National Cyber Director shall be the chair of the Committee.

(d) CHARTER.—The Committee shall develop, deliver to Congress, and make publicly available a charter, which shall—

(1) include the processes and rules of the Committee; and

(2) detail—

(A) the objective and scope of the Committee; and

(B) other items as necessary.

(e) REGULATORY FRAMEWORK FOR HARMONIZATION.—

(1) IN GENERAL.—

(A) DEVELOPMENT.—Not later than 1 year after the date of enactment of this Act, the Committee shall develop a regulatory framework for achieving harmonization of the cybersecurity requirements of each regulatory agency.

(B) CONTENTS.—The regulatory framework developed under clause (i) shall—

(i) include a common set of baseline cybersecurity requirements across sectors; and

(ii) outline common approaches and language for applying cybersecurity requirements promulgated or amended following passage of this Act.

(C) PUBLIC COMMENT.—The process for developing such regulatory framework shall include the opportunity for public comment and consultation with industry experts and other stakeholders.

(D) FACTORS.—In developing the framework under subparagraph (A), the Committee shall account for existing sector-specific cybersecurity requirements that are identified as unique or critical to a sector.

(2) MINIMUM REQUIREMENTS.—The framework shall contain, at a minimum, processes for—

(A) establishing a reciprocal compliance mechanism for minimum requirements relating to information security or cybersecurity for entities regulated by more than 1 regulatory agency;

(B) identifying cybersecurity requirements that are overly burdensome, inconsistent, or contradictory, as determined by the Committee;

(C) developing recommendations for updating regulations, guidance, and examinations to address overly burdensome, inconsistent, or contradictory cybersecurity requirements identified under subparagraph (B) to achieve harmonization; and

(D) drafting baseline requirements and regulatory language for covered agencies to use, as appropriate.

(3) PUBLICATION.—Upon completion of the regulatory framework, the Committee shall publish the regulatory framework in the Federal Register.

(f) PILOT PROGRAM ON IMPLEMENTATION OF REGULATORY FRAMEWORK.—

(1) IN GENERAL.—Not later than 90 days after the publication of the framework developed under subsection (e), not fewer than 3 regulatory agencies but not more than 5 regulatory agencies, selected by the Committee, shall carry out a pilot program to implement the regulatory framework with respect to not fewer than 3 cybersecurity requirements but not more than 6 cybersecurity requirements, with at least 1 requirement from each regulatory agency.

(2) DURATION.—The duration of the pilot program shall be determined by the Harmonization

Committee in coordination with the pilot program participants.

(3) PARTICIPATION BY REGULATORY AGENCIES AND REGULATED ENTITIES.—

(A) REGULATORY AGENCIES.—Participation in the pilot program by a regulatory agency shall be voluntary and subject to the consent of the regulatory agency following selection by the Committee under paragraph (1).

(B) REGULATED ENTITIES.—Participation in the pilot program by a regulated entity shall be voluntary.

(4) SELECTION OF CYBERSECURITY REQUIREMENTS.—Cybersecurity requirements selected for the pilot program under paragraph (1) shall contain substantially similar or substantially related requirements such that not fewer than 2 of the selected cybersecurity requirements govern the same regulated entity with substantially similar or substantially related requirements relating to information security or cybersecurity.

(5) WAIVERS.—

(A) IN GENERAL.—Notwithstanding any provision of subchapter II of chapter 5, and chapter 7, of title 5, United States Code (com-

monly known as the ''Administrative Procedure Act'') and subject to the consent of any participating regulated entity, in implementing the pilot program under paragraph (1), a regulatory agency participating in the pilot program shall have the authority, as the regulatory agency determines appropriate, to both issue waivers and establish alternative procedures for regulated entities participating in the pilot program with respect to the cybersecurity requirements included under the pilot program.

(B) COMPLIANCE.—A regulated entity that notifies a regulatory agency of the entity's participation in a pilot program shall be deemed in compliance with the waived requirements to the extent that the entity complies with requirements of the pilot program.

(C) TERMINATION.—Waivers issued and alternative procedures established under this paragraph shall terminate on the date on which the pilot program terminates.

(6) SUBSEQUENT PILOT PROGRAM.—The Committee may only authorize an additional pilot program after the later of—

(A) the date of the conclusion of all of the initial pilot programs under paragraph (1); and

(B) the date of submission of all reports required under subsection (i) for each initial pilot program.

(7) SUNSET.—The pilot program shall terminate on the date that is 7 years after the date on which the pilot program began under paragraph (1).

(g) CONSULTATION WITH THE COMMITTEE.—

(1) IN GENERAL.—Notwithstanding any other provision of law—

(A) except when an exigent circumstance described in paragraph (3) exists, before promulgating or amending a cybersecurity requirement, a regulatory agency shall consult with the Committee regarding such requirement and the regulatory framework;

(B) independent regulatory agencies, when promulgating or amending a cybersecurity requirement, shall consult the Committee during the development of the updated cybersecurity requirement or the new cybersecurity requirement to ensure that the requirement is aligned to the greatest extent possible with the regulatory framework; and

(C) such consultation should be integrated with existing interagency review and input processes administered by the Office of Information and Regulatory Affairs of the Office of Management and Budget.

(2) CONSULTATION REPORT.—Following a consultation under paragraph (1), the Committee, in coordination with the Office of Management and Budget as necessary, shall provide to the agency a report that shall be advisory in nature and shall—

(A) include to what degree the proposed cybersecurity requirement or update to the cybersecurity requirement aligns with the regulatory framework, taking into consideration the authorities of the agency; and

(B) provide a list of recommendations to improve the cybersecurity requirement and to align the cybersecurity requirement with the regulatory framework.

(3) EXIGENT CIRCUMSTANCES.—In the case of an exigent circumstance where an agency is authorized by law to act expeditiously, the agency shall notify the Committee as soon as possible.

(h) CONSULTATION WITH SECTOR RISK MANAGEMENT AGENCIES.—The Committee shall consult with ap-

propriate Sector Risk Management Agencies in the development of the regulatory framework and the implementation of the pilot program under subsection (f) and shall consult with members of industry and critical infrastructure, as appropriate, for the development of the regulatory framework and pilot program.

(i) REPORTS.—

(1) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter until the date on which the pilot program terminates, the Committee shall submit to the appropriate congressional committees a report including—

(A) information about member participation in Committee activities, including the rationale for any nonparticipation by Committee members;

(B) information about the application of the regulatory framework, once developed, on cybersecurity requirements, including consultations or discussions with regulators;

(C) a general summary of reports made under subsection (g)(2); and

(D) an analysis of the efficiency of the regulatory framework.

(2) PILOT PROGRAM REPORT.—Not later than 1 year after the date on which a pilot program under subsection (f) begins, the Committee shall submit to the appropriate congressional committees a report detailing—

(A) the cybersecurity requirements selected for the program, including—

(i) the reasons that the regulatory agency and cybersecurity requirement were selected;

(ii) a list of the pilot programs considered by the Committee; and

(iii) the rationale for selecting the pilot program;

(B) the information learned from the program;

(C) any obstacles encountered during the program; and

(D) an assessment of the applicability of expanding the program to other agencies and cybersecurity requirements.

SEC. 4. COORDINATION WITH FEDERAL AGENCIES AND INTERNATIONAL BODIES.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Office

of Management and Budget shall, in consultation with the Committee, issue guidance to Federal agencies, including the Cyber Incident Reporting Council, on coordination with the Committee.

(b) GUIDANCE.—

(1) IN GENERAL.—Not later than 1 year after the completion of the initial pilot program and submission of the pilot program report, the Director of the Office of Management and Budget shall, in coordination with the Committee, issue guidance to all agencies to ensure cybersecurity requirements are consistent with the framework developed under subsection (e), incorporating the results and lessons learned from the pilot program.

(2) CONTENTS.—The guidance issued under paragraph (1) shall, at a minimum—

(A) include updates to the regulatory review process, as appropriate, for proposed cybersecurity requirements;

(B) provide draft regulatory language for covered agencies to use when preparing cybersecurity requirements;

(C) provide guidance and procedures for covered agencies to resolve inconsistencies with the framework; and

(D) provide a template for covered agencies on how to use the guidance, including recommended procedures for implementation.

(c) REPORTING.—All agencies shall report to appropriate congressional committees on the status of implementing the guidance issued under subsection (a).

(d) ASSISTANCE.—

(1) FOREIGN ENTITIES.—The Committee, with the concurrence of the Secretary of State, and in coordination with the National Institute of Standards and Technology, may provide expertise or technical assistance on harmonization and reciprocity of cyber requirements to a foreign government, an international organization, or an international entity, as appropriate.

(2) LOCAL ENTITIES.—The Committee may provide expertise or technical assistance on harmonization and reciprocity of cyber requirements to State, local, Tribal, and territorial governments, as appropriate.

SEC. 5. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed—

(1) to expand or alter the existing authorities of any agency, including any independent regulatory agency, except for exemptions under section 3(f) to

implement the pilot program established under that section;

(2) to provide any such agency any new or additional authorities, except for exemptions under section 3(f) to implement the pilot program established under that section; or

(3) to affect, augment, or diminish the authority of the Secretary of State or any other officer of the Federal Government.

○