

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Streamlining Federal
5 Cybersecurity Regulations Act of 2025”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

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

4 (2) APPROPRIATE CONGRESSIONAL COMMIT-
5 TEES.—The term “appropriate congressional com-
6 mittees” means—

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

9 (B) the Committee on Oversight and Gov-
10 ernment Reform of the House of Representa-
11 tives;

12 (C) each committee of Congress with juris-
13 diction over the activities of a regulatory agen-
14 cy; and

15 (D) each committee of Congress with juris-
16 diction over the activities of a Sector Risk Man-
17 agement Agency with respect to a sector regu-
18 lated by a regulatory agency.

19 (3) COMMITTEE.—The term “Committee”
20 means the Harmonization Committee established
21 under section 3(a).

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

1 nical, or physical requirements relating to informa-
 2 tion security, security of information technology or
 3 operational technology, cybersecurity, or cyber risk
 4 or resilience.

5 (5) HARMONIZATION.—

6 (A) DEFINITION.—The term “harmoni-
 7 zation” means the process of aligning cyberse-
 8 curity requirements issued by regulatory agen-
 9 cies such that the requirements consist of—

10 (i) a common set of minimum require-
 11 ments that may apply across sectors and
 12 that can be updated periodically to address
 13 new or evolving risks relating to informa-
 14 tion security or cybersecurity; and

15 (ii) sector-specific requirements, which
 16 may include performance-based require-
 17 ments, that—

18 (I) are necessary to address sec-
 19 tor-specific risks that are not ade-
 20 quately addressed by the minimum re-
 21 quirements described in clause (i);

22 (II) are substantially similar,
 23 where appropriate, to other require-
 24 ments in that sector or a similar sec-
 25 tor; and

1 (III) align with international
2 standards, where appropriate.

3 (B) RULE OF CONSTRUCTION.—Nothing in
4 this definition shall be construed to exempt reg-
5 ulatory agencies from any otherwise applicable
6 processes or laws relating to promulgating or
7 amending regulations, including subchapter II
8 of chapter 5, and chapter 7, of title 5, United
9 States Code (commonly known as the “Admin-
10 istrative Procedure Act”).

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

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

19 (8) RECIPROCITY.—The term “reciprocity”
20 means the recognition or acceptance by 1 regulatory
21 agency of an assessment, determination, examina-
22 tion, finding, or conclusion of another regulatory
23 agency for determining that a regulated entity has
24 complied with a cybersecurity requirement.

1 (9) REGULATORY AGENCY.—The term “regu-
2 latory agency” means—

3 (A) any independent regulatory agency
4 that has the statutory authority to issue or en-
5 force any mandatory cybersecurity requirement;
6 or

7 (B) any other agency that has the statu-
8 tory authority to issue or enforce any cyberse-
9 curity requirement.

10 (10) REGULATORY FRAMEWORK.—The term
11 “regulatory framework” means the framework devel-
12 oped under section 3(e)(1).

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

17 **SEC. 3. ESTABLISHMENT OF INTERAGENCY COMMITTEE TO**
18 **HARMONIZE REGULATORY REGIMES IN THE**
19 **UNITED STATES RELATING TO CYBERSECU-**
20 **RITY.**

21 (a) HARMONIZATION COMMITTEE.—

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

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

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

7 (b) MEMBERS.—

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

10 (A) the National Cyber Director;

11 (B) the head of each regulatory agency, in-
12 cluding the Cybersecurity and Infrastructure
13 Security Agency and the National Institute of
14 Standards and Technology;

15 (C) the head of the Office of Information
16 and Regulatory Affairs of the Office of Manage-
17 ment and Budget; and

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

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

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

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

6 (1) include the processes and rules of the Com-
 7 mittee; and

8 (2) detail—

9 (A) the objective and scope of the Com-
 10 mittee; and

11 (B) other items as necessary.

12 (e) REGULATORY FRAMEWORK FOR HARMONI-
 13 ZATION.—

14 (1) IN GENERAL.—

15 (A) DEVELOPMENT.—Not later than 1
 16 year after the date of enactment of this Act, the
 17 Committee shall develop a regulatory frame-
 18 work for achieving harmonization of the cyber-
 19 security requirements of each regulatory agen-
 20 cy.

21 (B) CONTENTS.—The regulatory frame-
 22 work developed under clause (i) shall—

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

1 (ii) outline common approaches and
2 language for applying cybersecurity re-
3 quirements promulgated or amended fol-
4 lowing passage of this Act.

5 (C) PUBLIC COMMENT.—The process for
6 developing such regulatory framework shall in-
7 clude the opportunity for public comment and
8 consultation with industry experts and other
9 stakeholders.

10 (D) FACTORS.—In developing the frame-
11 work under subparagraph (A), the Committee
12 shall account for existing sector-specific cyber-
13 security requirements that are identified as
14 unique or critical to a sector.

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

17 (A) establishing a reciprocal compliance
18 mechanism for minimum requirements relating
19 to information security or cybersecurity for en-
20 tities regulated by more than 1 regulatory agen-
21 cy;

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

1 (C) developing recommendations for updat-
2 ing regulations, guidance, and examinations to
3 address overly burdensome, inconsistent, or con-
4 tradictory cybersecurity requirements identified
5 under subparagraph (B) to achieve harmoni-
6 zation; and

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

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

13 (f) PILOT PROGRAM ON IMPLEMENTATION OF REGU-
14 LATORY FRAMEWORK.—

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

24 (2) DURATION.—The duration of the pilot pro-
25 gram shall be determined by the Harmonization

1 Committee in coordination with the pilot program
2 participants.

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

5 (A) REGULATORY AGENCIES.—Participa-
6 tion in the pilot program by a regulatory agen-
7 cy shall be voluntary and subject to the consent
8 of the regulatory agency following selection by
9 the Committee under paragraph (1).

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

13 (4) SELECTION OF CYBERSECURITY REQUIRE-
14 MENTS.—Cybersecurity requirements selected for the
15 pilot program under paragraph (1) shall contain
16 substantially similar or substantially related require-
17 ments such that not fewer than 2 of the selected cy-
18 bersecurity requirements govern the same regulated
19 entity with substantially similar or substantially re-
20 lated requirements relating to information security
21 or cybersecurity.

22 (5) WAIVERS.—

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

1 monly known as the “Administrative Procedure
2 Act”) and subject to the consent of any partici-
3 pating regulated entity, in implementing the
4 pilot program under paragraph (1), a regu-
5 latory agency participating in the pilot program
6 shall have the authority, as the regulatory agen-
7 cy determines appropriate, to both issue waivers
8 and establish alternative procedures for regu-
9 lated entities participating in the pilot program
10 with respect to the cybersecurity requirements
11 included under the pilot program.

12 (B) COMPLIANCE.—A regulated entity that
13 notifies a regulatory agency of the entity’s par-
14 ticipation in a pilot program shall be deemed in
15 compliance with the waived requirements to the
16 extent that the entity complies with require-
17 ments of the pilot program.

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

22 (6) SUBSEQUENT PILOT PROGRAM.—The Com-
23 mittee may only authorize an additional pilot pro-
24 gram after the later of—

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

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

6 (7) SUNSET.—The pilot program shall termi-
7 nate on the date that is 7 years after the date on
8 which the pilot program began under paragraph (1).

9 (g) CONSULTATION WITH THE COMMITTEE.—

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

12 (A) except when an exigent circumstance
13 described in paragraph (3) exists, before pro-
14 mulgating or amending a cybersecurity require-
15 ment, a regulatory agency shall consult with the
16 Committee regarding such requirement and the
17 regulatory framework;

18 (B) independent regulatory agencies, when
19 promulgating or amending a cybersecurity re-
20 quirement, shall consult the Committee during
21 the development of the updated cybersecurity
22 requirement or the new cybersecurity require-
23 ment to ensure that the requirement is aligned
24 to the greatest extent possible with the regu-
25 latory framework; and

1 (C) such consultation should be integrated
2 with existing interagency review and input proc-
3 esses administered by the Office of Information
4 and Regulatory Affairs of the Office of Manage-
5 ment and Budget.

6 (2) CONSULTATION REPORT.—Following a con-
7 sultation under paragraph (1), the Committee, in co-
8 ordination with the Office of Management and
9 Budget as necessary, shall provide to the agency a
10 report that shall be advisory in nature and shall—

11 (A) include to what degree the proposed
12 cybersecurity requirement or update to the cy-
13 bersecurity requirement aligns with the regu-
14 latory framework, taking into consideration the
15 authorities of the agency; and

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

20 (3) EXIGENT CIRCUMSTANCES.—In the case of
21 an exigent circumstance where an agency is author-
22 ized by law to act expeditiously, the agency shall no-
23 tify the Committee as soon as possible.

24 (h) CONSULTATION WITH SECTOR RISK MANAGE-
25 MENT AGENCIES.—The Committee shall consult with ap-

1 appropriate Sector Risk Management Agencies in the devel-
2 opment of the regulatory framework and the implementa-
3 tion of the pilot program under subsection (f) and shall
4 consult with members of industry and critical infrastruc-
5 ture, as appropriate, for the development of the regulatory
6 framework and pilot program.

7 (i) REPORTS.—

8 (1) ANNUAL REPORT.—Not later than 1 year
9 after the date of enactment of this Act, and annually
10 thereafter until the date on which the pilot program
11 terminates, the Committee shall submit to the ap-
12 propriate congressional committees a report includ-
13 ing—

14 (A) information about member participa-
15 tion in Committee activities, including the ra-
16 tionale for any nonparticipation by Committee
17 members;

18 (B) information about the application of
19 the regulatory framework, once developed, on
20 cybersecurity requirements, including consulta-
21 tions or discussions with regulators;

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

24 (D) an analysis of the efficiency of the reg-
25 ulatory framework.

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

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

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

11 (ii) a list of the pilot programs consid-
12 ered by the Committee; and

13 (iii) the rationale for selecting the
14 pilot program;

15 (B) the information learned from the pro-
16 gram;

17 (C) any obstacles encountered during the
18 program; and

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

22 **SEC. 4. COORDINATION WITH FEDERAL AGENCIES AND**
23 **INTERNATIONAL BODIES.**

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

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

5 (b) GUIDANCE.—

6 (1) IN GENERAL.—Not later than 1 year after
7 the completion of the initial pilot program and sub-
8 mission of the pilot program report, the Director of
9 the Office of Management and Budget shall, in co-
10 ordination with the Committee, issue guidance to all
11 agencies to ensure cybersecurity requirements are
12 consistent with the framework developed under sub-
13 section (e), incorporating the results and lessons
14 learned from the pilot program.

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

17 (A) include updates to the regulatory re-
18 view process, as appropriate, for proposed cy-
19 bersecurity requirements;

20 (B) provide draft regulatory language for
21 covered agencies to use when preparing cyberse-
22 curity requirements;

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

1 (D) provide a template for covered agen-
2 cies on how to use the guidance, including rec-
3 ommended procedures for implementation.

4 (c) REPORTING.—All agencies shall report to appro-
5 priate congressional committees on the status of imple-
6 menting the guidance issued under subsection (a).

7 (d) ASSISTANCE.—

8 (1) FOREIGN ENTITIES.—The Committee, with
9 the concurrence of the Secretary of State, and in co-
10 ordination with the National Institute of Standards
11 and Technology, may provide expertise or technical
12 assistance on harmonization and reciprocity of cyber
13 requirements to a foreign government, an inter-
14 national organization, or an international entity, as
15 appropriate.

16 (2) LOCAL ENTITIES.—The Committee may
17 provide expertise or technical assistance on harmoni-
18 zation and reciprocity of cyber requirements to
19 State, local, Tribal, and territorial governments, as
20 appropriate.

21 **SEC. 5. RULE OF CONSTRUCTION.**

22 Nothing in this Act shall be construed—

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

1 implement the pilot program established under that
2 section;

3 (2) to provide any such agency any new or ad-
4 ditional authorities, except for exemptions under sec-
5 tion 3(f) to implement the pilot program established
6 under that section; or

7 (3) to affect, augment, or diminish the author-
8 ity of the Secretary of State or any other officer of
9 the Federal Government.

○