

118TH CONGRESS  
2D SESSION

**S.** \_\_\_\_\_

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

---

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

---



---

**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”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1           (1) AGENCY.—The term “agency” has the  
2 meaning given that term in section 551 of title 5,  
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 Ac-  
10 countability of the House of Representatives;

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

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

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

21           (4) CYBERSECURITY REQUIREMENT.—The term  
22 “cybersecurity requirement” means an administra-  
23 tive, technical, or physical safeguard, requirement,  
24 or supervisory activity, including regulations, guid-  
25 ance, bulletins or examinations, relating to informa-

1       tion security, information technology, cybersecurity,  
2       or cyber risk or resilience.

3           (5) HARMONIZATION.—

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

8           (i) a common set of minimum require-  
9       ments that apply across sectors and that  
10      can be updated periodically to address new  
11      or evolving risks relating to information se-  
12      curity or cybersecurity; and

13          (ii) sector-specific requirements  
14      that—

15           (I) are necessary to address sec-  
16      tor-specific risks that are not ade-  
17      quately addressed by the minimum re-  
18      quirements in clause (i); and

19           (II) are substantially similar,  
20      where appropriate, to other require-  
21      ments in that sector or a similar sec-  
22      tor.

23           (B) RULE OF CONSTRUCTION.—Nothing in  
24      this definition shall be construed to exempt reg-  
25      ulatory agencies from any otherwise applicable

1 processes or laws relating to updating regula-  
2 tions, including subchapter II of chapter 5, and  
3 chapter 7, of title 5, United States Code (com-  
4 monly known as the “Administrative Procedure  
5 Act”).

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

10 (7) RECIPROCITY.—The term “reciprocity”  
11 means the recognition or acceptance by 1 regulatory  
12 agency of an assessment, determination, examina-  
13 tion, finding, or conclusion of another regulatory  
14 agency for determining that a regulated entity has  
15 complied with a cybersecurity requirement.

16 (8) REGULATORY AGENCY.—The term “regu-  
17 latory agency” means—

18 (A) any independent regulatory agency  
19 that has the statutory authority to issue or en-  
20 force any mandatory cybersecurity requirement;  
21 or

22 (B) any other agency that has the statu-  
23 tory authority to issue or enforce any cyberse-  
24 curity requirement.



1 (C) the head of the Office of Information  
2 and Regulatory Affairs of the Office of Manage-  
3 ment and Budget; and

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

6 (2) PUBLICATION OF LIST OF MEMBERS.—The  
7 Committee shall maintain a list of the agencies that  
8 are represented on the Committee on a publicly  
9 available website.

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

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

15 (1) include the processes and rules of the Com-  
16 mittee; and

17 (2) detail—

18 (A) the objective and scope of the Com-  
19 mittee; and

20 (B) other items as necessary.

21 (e) REGULATORY FRAMEWORK FOR HARMONI-  
22 ZATION.—

23 (1) IN GENERAL.—

24 (A) FRAMEWORK.—Not later than 1 year  
25 after the date of enactment of this Act, the

1           Committee shall develop a regulatory frame-  
2           work for achieving harmonization of the cyber-  
3           security requirements of each regulatory agen-  
4           cy.

5                   (B) FACTORS.—In developing the frame-  
6           work under subparagraph (A), the Committee  
7           shall account for existing sector-specific cyber-  
8           security requirements that are identified as  
9           unique or critical to a sector.

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

12                   (A) establishing a reciprocal compliance  
13           mechanism for minimum requirements relating  
14           to information security or cybersecurity for en-  
15           tities regulated by more than 1 regulatory agen-  
16           cy;

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

21                   (C) developing recommendations for updat-  
22           ing regulations, guidance, and examinations to  
23           address overly burdensome, inconsistent, or con-  
24           tradictory cybersecurity requirements identified

1 under subparagraph (B) to achieve harmoni-  
2 zation.

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

6 (f) PILOT PROGRAM ON IMPLEMENTATION OF REGU-  
7 LATORY FRAMEWORK.—

8 (1) IN GENERAL.—Not fewer than 3 regulatory  
9 agencies, selected by the Committee, shall carry out  
10 a pilot program to implement the regulatory frame-  
11 work established under subsection (e) with respect to  
12 not fewer than 3 cybersecurity requirements.

13 (2) PARTICIPATION BY REGULATORY AGENCIES  
14 AND REGULATED ENTITIES.—

15 (A) REGULATORY AGENCIES.—Participa-  
16 tion in the pilot program by a regulatory agen-  
17 cy shall be voluntary and subject to the consent  
18 of the regulatory agency following selection by  
19 the Committee under paragraph (1).

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

23 (3) SELECTION OF CYBERSECURITY REQUIRE-  
24 MENTS.—Cybersecurity requirements selected for the  
25 pilot program under paragraph (1) shall contain



1 substantially similar or substantially related require-  
2 ments such that not fewer than 2 of the selected cy-  
3 bersecurity requirements govern the same regulated  
4 entity with substantially similar or substantially re-  
5 lated requirements relating to information security  
6 or cybersecurity.

7 (4) WAIVERS.—Notwithstanding any provision  
8 of subchapter II of chapter 5, and chapter 7, of title  
9 5, United States Code (commonly known as the  
10 “Administrative Procedure Act”) and subject to the  
11 consent of any participating regulated entity, in im-  
12 plementing the pilot program under paragraph (1),  
13 a regulatory agency participating in the pilot pro-  
14 gram shall have the authority to issue waivers and  
15 establish alternative procedures for regulated entities  
16 participating in the pilot program with respect to  
17 the cybersecurity requirements included under the  
18 pilot program.

19 (g) CONSULTATION WITH THE COMMITTEE.—

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

22 (A) before prescribing any cybersecurity  
23 requirement, the head of a regulatory agency  
24 shall consult with the Committee regarding

1 such requirement and the regulatory framework  
2 established under subsection (e); and

3 (B) independent regulatory agencies, when  
4 updating any existing cybersecurity requirement  
5 or issuing a potential new cybersecurity require-  
6 ment, shall consult the Committee during the  
7 development of the updated cybersecurity re-  
8 quirement or the new cybersecurity requirement  
9 to ensure that the requirement is aligned to the  
10 greatest extent possible with the regulatory  
11 framework.

12 (2) DETERMINATION.—Following a consultation  
13 under paragraph (1), the Committee shall make a  
14 determination in writing to the agency, in coordina-  
15 tion with the Office of Management and Budget as  
16 necessary, that shall—

17 (A) include to what degree the proposed  
18 cybersecurity requirement or update to the cy-  
19 bersecurity requirement aligns with the regu-  
20 latory framework; and

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

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 under subsection (e)  
3 and the implementation of the pilot program under sub-  
4 section (f).

5 (i) REPORTS.—

6 (1) ANNUAL REPORT.—Not later than 12  
7 months after the date of enactment of this Act, and  
8 annually thereafter, the Committee shall submit to  
9 the appropriate congressional committees a report  
10 detailing—

11 (A) member participation; and

12 (B) the application of the regulatory  
13 framework, once developed, on cybersecurity re-  
14 quirements, including consultations or discus-  
15 sions with regulators.

16 (2) PILOT PROGRAM REPORT.—Not later than  
17 12 months after the date on which the pilot program  
18 begins, the Committee shall submit to the appro-  
19 priate congressional committees a report detailing—

20 (A) the cybersecurity requirements selected  
21 for the program, including the reasons that the  
22 regulatory agency and cybersecurity require-  
23 ment were selected;

24 (B) the information learned from the pro-  
25 gram;

1 (C) any obstacles encountered during the  
2 program; and

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

6 **SEC. 4. STATUS UPDATES ON INCIDENT REPORTING.**

7 (a) STATUS UPDATE ON MEMORANDA OF AGREE-  
8 MENT.—Not later than 180 days after the date of enact-  
9 ment of this Act, and not less frequently than every 180  
10 days thereafter, the Director of the Cybersecurity and In-  
11 frastructure Security Agency shall provide to the appro-  
12 priate congressional committees a status update on the de-  
13 velopment and implementation of memoranda of agree-  
14 ment between agencies required under section 104(a)(5)  
15 of the Cyber Incident Reporting for Critical Infrastructure  
16 Act of 2022 (6 U.S.C. 681g(a)(5)).

17 (b) STATUS UPDATE ON EFFORTS OF THE CYBER  
18 INCIDENT REPORTING COUNCIL.—Not later than 180  
19 days after the date of enactment of this Act, and not less  
20 frequently than every 180 days thereafter, the Secretary  
21 of Homeland Security shall provide to the appropriate con-  
22 gressional committees a status update on the efforts of  
23 the Cyber Incident Reporting Council established under  
24 section 2246 of the Homeland Security Act of 2002 (6  
25 U.S.C. 681f).

1 **SEC. 5. RULE OF CONSTRUCTION.**

2 Nothing in this Act shall be construed—

3 (1) to expand or alter the existing regulatory  
4 authorities of any agency, including any independent  
5 regulatory agency, except for exemptions under sec-  
6 tion 3(f) to implement the pilot program established  
7 under that section;

8 (2) to provide any such agency any new or ad-  
9 ditional regulatory authorities; or

10 (3) to address security incident reporting re-  
11 quirements subject to coordination by the Cyber In-  
12 cident Reporting Council established under section  
13 2246 of the Homeland Security Act of 2022 (6  
14 U.S.C. 681f), except for the required status updates  
15 under section 4.