

Calendar No. 655

118TH CONGRESS
2D SESSION**S. 4630****[Report No. 118-254]**

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

JULY 8, 2024

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

DECEMBER 2, 2024

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

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”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **AGENCY.**—The term “agency” has the
4 meaning given that term in section 551 of title 5,
5 United States Code.

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

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

11 (B) the Committee on Oversight and Ac-
12 countability of the House of Representatives;

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

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

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

23 (4) **CYBERSECURITY REQUIREMENT.**—The term
24 “cybersecurity requirement” means an administra-
25 tive, technical, or physical safeguard, requirement,
26 or supervisory activity, including regulations, guid-

1 ance, bulletins or examinations, relating to informa-
 2 tion security, information technology, cybersecurity,
 3 or cyber risk or resilience.

4 (5) HARMONIZATION.—

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

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

14 (ii) sector-specific requirements
 15 that—

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

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

24 (B) RULE OF CONSTRUCTION.—Nothing in
 25 this definition shall be construed to exempt reg-

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

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

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

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

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

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

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

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

8 **SEC. 3. ESTABLISHMENT OF INTERAGENCY COMMITTEE TO**
9 **HARMONIZE REGULATORY REGIMES IN THE**
10 **UNITED STATES RELATING TO CYBERSECU-**
11 **RITY.**

12 (a) HARMONIZATION COMMITTEE.—

13 (1) IN GENERAL.—The National Cyber Director
14 shall establish an interagency committee to be
15 known as the Harmonization Committee to enhance
16 the harmonization of cybersecurity requirements
17 that are applicable within the United States.

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

21 (b) MEMBERS.—

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

24 (A) the National Cyber Director;

25 (B) the head of each regulatory agency;

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 (e) 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; or10 (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 4.16 **SECTION 1. SHORT TITLE.**17 *This Act may be cited as the “Streamlining Federal*
18 *Cybersecurity Regulations Act”.*19 **SEC. 2. DEFINITIONS.**20 *In this Act:*21 (1) *AGENCY.*—*The term “agency” has the mean-*
22 *ing given that term in section 551 of title 5, United*
23 *States Code.*24 (2) *APPROPRIATE CONGRESSIONAL COMMIT-*
25 *TEES.*—*The term “appropriate congressional commit-*
26 *tees” means—*

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

3 (B) *the Committee on Oversight and Ac-*
4 *countability of the House of Representatives;*

5 (C) *each committee of Congress with juris-*
6 *isdiction over the activities of a regulatory agency;*
7 *and*

8 (D) *each committee of Congress with juris-*
9 *isdiction over the activities of a Sector Risk Man-*
10 *agement Agency with respect to a sector regu-*
11 *lated by a regulatory agency.*

12 (3) *COMMITTEE.—The term “Committee” means*
13 *the Harmonization Committee established under sec-*
14 *tion 3(a).*

15 (4) *CYBERSECURITY REQUIREMENT.—The term*
16 *“cybersecurity requirement” means an administra-*
17 *tive, technical, or physical safeguard, requirement, or*
18 *supervisory activity, including regulations, guidance,*
19 *bulletins, or examinations, relating to information se-*
20 *curity, information technology, cybersecurity, or cyber*
21 *risk or resilience.*

22 (5) *HARMONIZATION.—*

23 (A) *DEFINITION.—The term “harmoni-*
24 *zation” means the process of aligning cybersecu-*

1 *riety requirements issued by regulatory agencies*
2 *such that the requirements consist of—*

3 *(i) a common set of minimum require-*
4 *ments that apply across sectors and that*
5 *can be updated periodically to address new*
6 *or evolving risks relating to information se-*
7 *curity or cybersecurity; and*

8 *(ii) sector-specific requirements, which*
9 *may include performance-based require-*
10 *ments, that—*

11 *(I) are necessary to address sector-*
12 *specific risks that are not adequately*
13 *addressed by the minimum require-*
14 *ments described in clause (i); and*

15 *(II) are substantially similar,*
16 *where appropriate, to other require-*
17 *ments in that sector or a similar sec-*
18 *tor.*

19 *(B) RULE OF CONSTRUCTION.—Nothing in*
20 *this definition shall be construed to exempt regu-*
21 *latory agencies from any otherwise applicable*
22 *processes or laws relating to updating regula-*
23 *tions, including subchapter II of chapter 5, and*
24 *chapter 7, of title 5, United States Code (com-*

1 *monly known as the “Administrative Procedure*
2 *Act”*).

3 (6) *INDEPENDENT REGULATORY AGENCY.—The*
4 *term “independent regulatory agency” has the mean-*
5 *ing given that term in section 3502 of title 44, United*
6 *States Code.*

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

13 (8) *REGULATORY AGENCY.—The term “regu-*
14 *latory agency” means—*

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

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

21 (9) *REGULATORY FRAMEWORK.—The term “reg-*
22 *ulatory framework” means the framework developed*
23 *under section 3(e)(1).*

24 (10) *SECTOR RISK MANAGEMENT AGENCY.—The*
25 *term “Sector Risk Management Agency” has the*

1 *meaning given that term in section 2200 of the*
2 *Homeland Security Act of 2002 (6 U.S.C. 650).*

3 **SEC. 3. ESTABLISHMENT OF INTERAGENCY COMMITTEE TO**
4 **HARMONIZE REGULATORY REGIMES IN THE**
5 **UNITED STATES RELATING TO CYBERSECU-**
6 **RITY.**

7 *(a) HARMONIZATION COMMITTEE.—*

8 *(1) IN GENERAL.—The National Cyber Director*
9 *shall establish an interagency committee to be known*
10 *as the Harmonization Committee to enhance the har-*
11 *monization of cybersecurity requirements that are ap-*
12 *licable within the United States.*

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

16 *(b) MEMBERS.—*

17 *(1) IN GENERAL.—The Committee shall be com-*
18 *posed of—*

19 *(A) the National Cyber Director;*

20 *(B) the head of each regulatory agency;*

21 *(C) the head of the Office of Information*
22 *and Regulatory Affairs of the Office of Manage-*
23 *ment and Budget; and*

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

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

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

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

11 (1) *include the processes and rules of the Com-*
12 *mittee; and*

13 (2) *detail—*

14 (A) *the objective and scope of the Com-*
15 *mittee; and*

16 (B) *other items as necessary.*

17 (e) *REGULATORY FRAMEWORK FOR HARMONI-*
18 *ZATION.*—

19 (1) *IN GENERAL.*—

20 (A) *FRAMEWORK.*—Not later than 1 year
21 after the date of enactment of this Act, the Com-
22 mittee shall develop a regulatory framework for
23 achieving harmonization of the cybersecurity re-
24 quirements of each regulatory agency.

1 (B) *FACTORS.*—*In developing the frame-*
2 *work under subparagraph (A), the Committee*
3 *shall account for existing sector-specific cyberse-*
4 *curity requirements that are identified as unique*
5 *or critical to a sector.*

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

8 (A) *establishing a reciprocal compliance*
9 *mechanism for minimum requirements relating*
10 *to information security or cybersecurity for enti-*
11 *ties regulated by more than 1 regulatory agency;*

12 (B) *identifying cybersecurity requirements*
13 *that are overly burdensome, inconsistent, or con-*
14 *tradictory, as determined by the Committee; and*

15 (C) *developing recommendations for updat-*
16 *ing regulations, guidance, and examinations to*
17 *address overly burdensome, inconsistent, or con-*
18 *tradictory cybersecurity requirements identified*
19 *under subparagraph (B) to achieve harmoni-*
20 *zation.*

21 (3) *PUBLICATION.*—*Upon completion of the regu-*
22 *latory framework, the Committee shall publish the*
23 *regulatory framework in the Federal Register for pub-*
24 *lic comment.*

1 (f) *PILOT PROGRAM ON IMPLEMENTATION OF REGU-*
2 *LATORY FRAMEWORK.*—

3 (1) *IN GENERAL.*—*Not fewer than 3 regulatory*
4 *agencies, selected by the Committee, shall carry out a*
5 *pilot program to implement the regulatory framework*
6 *with respect to not fewer than 3 cybersecurity require-*
7 *ments.*

8 (2) *PARTICIPATION BY REGULATORY AGENCIES*
9 *AND REGULATED ENTITIES.*—

10 (A) *REGULATORY AGENCIES.*—*Participa-*
11 *tion in the pilot program by a regulatory agency*
12 *shall be voluntary and subject to the consent of*
13 *the regulatory agency following selection by the*
14 *Committee under paragraph (1).*

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

18 (3) *SELECTION OF CYBERSECURITY REQUIRE-*
19 *MENTS.*—*Cybersecurity requirements selected for the*
20 *pilot program under paragraph (1) shall contain sub-*
21 *stantially similar or substantially related require-*
22 *ments such that not fewer than 2 of the selected cyber-*
23 *security requirements govern the same regulated enti-*
24 *ty with substantially similar or substantially related*

1 *requirements relating to information security or cy-*
2 *bersecurity.*

3 (4) *WAIVERS.—Notwithstanding any provision*
4 *of subchapter II of chapter 5, and chapter 7, of title*
5 *5, United States Code (commonly known as the “Ad-*
6 *ministrative Procedure Act”)* and subject to the con-
7 *sent of any participating regulated entity, in imple-*
8 *menting the pilot program under paragraph (1), a*
9 *regulatory agency participating in the pilot program*
10 *shall have the authority to issue waivers and establish*
11 *alternative procedures for regulated entities partici-*
12 *pating in the pilot program with respect to the cyber-*
13 *security requirements included under the pilot pro-*
14 *gram.*

15 (5) *SUBSEQUENT PILOT PROGRAM.—The Com-*
16 *mittee may only authorize an additional pilot pro-*
17 *gram after the later of—*

18 (A) *the date of the conclusion of all 3 initial*
19 *pilot programs under paragraph (1); and*

20 (B) *the date of submission of all reports re-*
21 *quired under subsection (i) for each initial pilot*
22 *program.*

23 (g) *CONSULTATION WITH THE COMMITTEE.—*

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

1 (A) *except when an exigent circumstance*
2 *described in paragraph (3) exists, before pre-*
3 *scribing any cybersecurity requirement, the head*
4 *of a regulatory agency shall consult with the*
5 *Committee regarding such requirement and the*
6 *regulatory framework; and*

7 (B) *independent regulatory agencies, when*
8 *updating any existing cybersecurity requirement*
9 *or issuing a potential new cybersecurity require-*
10 *ment, shall consult the Committee during the de-*
11 *velopment of the updated cybersecurity require-*
12 *ment or the new cybersecurity requirement to en-*
13 *sure that the requirement is aligned to the great-*
14 *est extent possible with the regulatory framework.*

15 (2) *DETERMINATION.*—*Following a consultation*
16 *under paragraph (1), the Committee shall make a de-*
17 *termination in writing to the agency, in coordination*
18 *with the Office of Management and Budget as nec-*
19 *essary, that shall—*

20 (A) *include to what degree the proposed cy-*
21 *bersecurity requirement or update to the cyberse-*
22 *curity requirement aligns with the regulatory*
23 *framework; and*

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

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

8 (h) *CONSULTATION WITH SECTOR RISK MANAGEMENT*
9 *AGENCIES.*—*The Committee shall consult with appropriate*
10 *Sector Risk Management Agencies in the development of the*
11 *regulatory framework and the implementation of the pilot*
12 *program under subsection (f) and shall consult with mem-*
13 *bers of industry and critical infrastructure, as appropriate,*
14 *for the development of the regulatory framework and pilot*
15 *program.*

16 (i) *REPORTS.*—

17 (1) *ANNUAL REPORT.*—*Not later than 1 year*
18 *after the date of enactment of this Act, and annually*
19 *thereafter, the Committee shall submit to the appro-*
20 *priate congressional committees a report detailing—*

21 (A) *member participation, including the ra-*
22 *tionale for any nonparticipation by Committee*
23 *members;*

24 (B) *the application of the regulatory frame-*
25 *work, once developed, on cybersecurity require-*

1 *ments, including consultations or discussions*
2 *with regulators; and*

3 *(C) any determination made under sub-*
4 *section (g)(2).*

5 *(2) PILOT PROGRAM REPORT.—Not later than 1*
6 *year after the date on which a pilot program under*
7 *subsection (f) begins, the Committee shall submit to*
8 *the appropriate congressional committees a report de-*
9 *tailing—*

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

12 *(i) the reasons that the regulatory*
13 *agency and cybersecurity requirement were*
14 *selected;*

15 *(ii) a list of the pilot programs consid-*
16 *ered by the Committee; and*

17 *(iii) the rationale for selecting the pilot*
18 *program;*

19 *(B) the information learned from the pro-*
20 *gram;*

21 *(C) any obstacles encountered during the*
22 *program; and*

23 *(D) an assessment of the applicability of ex-*
24 *panding the program to other agencies and cy-*
25 *bersecurity requirements.*

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

2 (a) *STATUS UPDATE ON MEMORANDA OF AGREE-*
3 *MENT.*—Not later than 180 days after the date of enactment
4 of this Act, and not less frequently than every 180 days
5 thereafter, the Director of the Cybersecurity and Infrastruc-
6 ture Security Agency shall provide to the appropriate con-
7 gressional committees a status update on the development
8 and implementation of documented agreements between
9 agencies required under section 104(a)(5) of the Cyber Inci-
10 dent Reporting for Critical Infrastructure Act of 2022 (6
11 U.S.C. 681g(a)(5)).

12 (b) *YEARLY BRIEFING ON ACTIVITIES OF THE CYBER*
13 *INCIDENT REPORTING COUNCIL.*—Section 2246 of the
14 Homeland Security Act of 2002 (6 U.S.C. 681f) is amend-
15 ed—

16 (1) by redesignating subsection (b) as subsection
17 (c); and

18 (2) by inserting after subsection (a) the fol-
19 lowing:

20 “(b) Not later than 1 year after the date of enactment
21 of the Streamlining Federal Cybersecurity Regulations Act,
22 and not less frequently than every 1 year thereafter, the Sec-
23 retary shall brief the Committee on Homeland Security and
24 Governmental Affairs of the Senate and the Committee on
25 Homeland Security of the House of Representatives on the
26 activities of the Cyber Incident Reporting Council.”.

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

2 *Nothing in this Act shall be construed—*

3 *(1) to expand or alter the existing regulatory au-*
4 *thorities 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; or*

8 *(2) to provide any such agency any new or addi-*
9 *tional regulatory authorities.*

Calendar No. 655

118TH CONGRESS
2^D SESSION

S. 4630

[Report No. 118-254]

A BILL

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

DECEMBER 2, 2024

Reported with an amendment