AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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.

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".~~

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5, 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 Accountability 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 an administrative, technical, or physical safeguard, requirement, or supervisory activity, including regulations, guid-

ance, bulletins or examinations, relating to information security, information 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 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 that—

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

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

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

ulatory agencies from any otherwise applicable processes or laws relating to updating regulations, including subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly known as the ''Administrative Procedure Act'').

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

(7) 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.

(8) 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.

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

(10) 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 of cybersecurity requirements that are applicable within the United States.

(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;

(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 a list of the agencies that are represented on the Committee on a publicly available website.

(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) FRAMEWORK.—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) 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; and

(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.

(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 fewer than 3 regulatory agencies, selected by the Committee, shall carry out a pilot program to implement the regulatory framework established under subsection (c) with respect to not fewer than 3 cybersecurity requirements.

(2) 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.

(3) 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.

(4) WAIVERS.—Notwithstanding any provision of subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly 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 to 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.

(g) CONSULTATION WITH THE COMMITTEE.—

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

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

such requirement and the regulatory framework established under subsection (c); and

(B) independent regulatory agencies, when updating any existing cybersecurity requirement or issuing a potential new 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.

(2) DETERMINATION.—Following a consultation under paragraph (1), the Committee shall make a determination in writing to the agency, in coordination with the Office of Management and Budget as necessary, that shall—

(A) include to what degree the proposed cybersecurity requirement or update to the cybersecurity requirement aligns with the regulatory framework; and

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

(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 under subsection (e) and the implementation of the pilot program under subsection (f).

(i) REPORTS.—

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

(A) member participation; and

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

(2) PILOT PROGRAM REPORT.—Not later than 12 months after the date on which the pilot program begins, the Committee shall submit to the appropriate congressional committees a report detailing—

(A) the cybersecurity requirements selected for the program, including the reasons that the regulatory agency and cybersecurity requirement were selected;

(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. STATUS UPDATES ON INCIDENT REPORTING.

(a) STATUS UPDATE ON MEMORANDA OF AGREEMENT.—Not later than 180 days after the date of enactment of this Act, and not less frequently than every 180 days thereafter, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate congressional committees a status update on the development and implementation of memoranda of agreement between agencies required under section 104(a)(5) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (6 U.S.C. 681g(a)(5)).

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

~~SEC. 5. RULE OF CONSTRUCTION.~~

~~Nothing in this Act shall be construed—~~

~~(1) to expand or alter the existing regulatory 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 regulatory authorities; or~~

~~(3) to address security incident reporting requirements subject to coordination by the Cyber Incident Reporting Council established under section 2246 of the Homeland Security Act of 2022 (6 U.S.C. 681f), except for the required status updates under section 4.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Streamlining Federal Cybersecurity Regulations Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given that term in section 551 of title 5, 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 Accountability 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 an administrative, technical, or physical safeguard, requirement, or supervisory activity, including regulations, guidance, bulletins, or examinations, relating to information security, information technology, cybersecurity, or cyber risk or resilience.

(5) HARMONIZATION.—

(A) DEFINITION.—The term "harmonization" means the process of aligning cybersecu-

rity requirements issued by regulatory agencies such that the requirements consist of—

(i) a common set of minimum requirements that 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); and

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

(B) RULE OF CONSTRUCTION.—Nothing in this definition shall be construed to exempt regulatory agencies from any otherwise applicable processes or laws relating to updating regulations, including subchapter II of chapter 5, and chapter 7, of title 5, United States Code (com-

monly known as the "Administrative Procedure Act").

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

(7) 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.

(8) 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.

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

(10) 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 of cybersecurity requirements that are applicable within the United States.

(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;

(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, 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) FRAMEWORK.—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) 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; and

(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.

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

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

(1) IN GENERAL.—Not fewer than 3 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.

(2) 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.

(3) 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.

(4) WAIVERS.—Notwithstanding any provision of subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly 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 to 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.

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

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

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

(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 prescribing any cybersecurity requirement, the head of a regulatory agency shall consult with the Committee regarding such requirement and the regulatory framework; and

(B) independent regulatory agencies, when updating any existing cybersecurity requirement or issuing a potential new 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.

(2) DETERMINATION.—Following a consultation under paragraph (1), the Committee shall make a determination in writing to the agency, in coordination with the Office of Management and Budget as necessary, that shall—

(A) include to what degree the proposed cybersecurity requirement or update to the cybersecurity requirement aligns with the regulatory framework; and

(B) provide a list of recommendations to improve the cybersecurity requirement and align it 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 appropriate 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, the Committee shall submit to the appropriate congressional committees a report detailing—

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

(B) the application of the regulatory framework, once developed, on cybersecurity require-

ments, including consultations or discussions with regulators; and

(C) any determination made under subsection (g)(2).

(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. STATUS UPDATES ON INCIDENT REPORTING.

(a) STATUS UPDATE ON MEMORANDA OF AGREEMENT.—Not later than 180 days after the date of enactment of this Act, and not less frequently than every 180 days thereafter, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate congressional committees a status update on the development and implementation of documented agreements between agencies required under section 104(a)(5) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (6 U.S.C. 681g(a)(5)).

(b) YEARLY BRIEFING ON ACTIVITIES OF THE CYBER INCIDENT REPORTING COUNCIL.—Section 2246 of the Homeland Security Act of 2002 (6 U.S.C. 681f) is amended—

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

(2) by inserting after subsection (a) the following:

"(b) Not later than 1 year after the date of enactment of the Streamlining Federal Cybersecurity Regulations Act, and not less frequently than every 1 year thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the activities of the Cyber Incident Reporting Council.".

SEC. 5. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed—

(1) to expand or alter the existing regulatory 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; or

(2) to provide any such agency any new or additional regulatory authorities.

Calendar No. 655

118TH CONGRESS
2D 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