Calendar No. 655

118TH CONGRESS *2d Session*	SENATE	REPORT 118–254

STREAMLINING FEDERAL CYBERSECURITY REGULATIONS ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 4630

TO ESTABLISH AN INTERAGENCY COMMITTEE TO HARMONIZE REGULATORY REGIMES IN THE UNITED STATES RELATING TO CYBERSECURITY, AND FOR OTHER PURPOSES

DECEMBER 2, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

59–010 WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA R. BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A. FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 655

118TH CONGRESS *2d Session* | SENATE | REPORT 118–254

STREAMLINING FEDERAL CYBERSECURITY REGULATIONS ACT

DECEMBER 2, 2024.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 4630]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4630) to establish an interagency committee to harmonize regulatory regimes in the United States relating to cybersecurity, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 4630, the *Streamlining Federal Cybersecurity Regulations Act*, requires the National Cyber Director to establish an interagency committee to be known as the Harmonization Committee to enhance the harmonization of cybersecurity requirements from United States federal agencies. Not later than one year after the date of enactment of this bill, the Harmonization Committee shall develop a regulatory framework for achieving harmonization of the

cybersecurity requirements of each regulatory agency. In addition, after the Committee is established, federal agencies will be required to consult with the Harmonization Committee prior to updating or issuing new cybersecurity requirements.

The regulatory framework developed by the Harmonization Committee shall contain processes for establishing reciprocal compliance mechanisms, identifying unnecessary cybersecurity regulations, and developing recommendations for updating regulations and guidance. The framework shall also account for existing sector-specific cybersecurity requirements that are identified as unique or critical to a sector. Upon completion of the regulatory framework, the Committee shall publish the regulatory framework in the Federal Register and conduct a pilot program to harmonize at least three cybersecurity regulations. Additionally, the Harmonization Committee is required to report to Congress annually on the progress of its work in formulating the framework, conducting the pilot program, and consultations with other federal agencies.

II. Background and Need for the Legislation

Malicious cyber actors from around the globe regularly attack a variety of targets in the United States, in both the public and private sectors. The federal government's ability to respond to these attacks and the bad actors who perpetrate them is limited by cyber capabilities and responsibilities that are often siloed by various federal agencies. A variety of legal frameworks across the U.S. and the globe leads to confusion and inefficiency, and this haphazard application of cyber procedures and regulations puts citizens and businesses at risk.[1] Cyberattacks and cybercrime have reached unprecedented levels, leaving individuals, industries, and governments scrambling to ensure the safety and security of their networks.[2] Currently, a cyberattack occurs every 39 seconds and is estimated to increase in frequency to every 2 seconds by 2031.[3] The Federal Bureau of Investigation stated in its Internet Crime Complaint Center (IC3) 2023 report that Americans lost $12.5 billion to cybercrime in 2023, a $9 billion, or 350% increase in just five years.[4]

In response to cybersecurity vulnerabilities, federal regulators in the United States have turned to cybersecurity oversight to ensure that essential operations continue and entities in their regulated sector can protect themselves from cyberattacks.[5] However, the fractured landscape of government regulations often serves as an obstacle to effective regulation.[6] From 2020 to mid-2024, according

[1] *Why Develop Thoughtful Cyber Policies When Disjointed Activities and Remaining Vulnerable Feel Good?*, Forbes (July 29, 2020) (www.forbes.com/sites/amityoran1/2020/07/28/why-develop-thoughtful-cyber-policies-when-disjointed-activities-and-remaining-vulnerable-feel-good/).

[2] *Check Point Research Reports Highest Increase of Global Cyber Attacks*, Check Point (July 16, 2024) (blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks).

[3] *Cybersecurity statistics in 2024*, USA Today (Feb. 26, 2024) (www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics).

[4] Federal Bureau of Investigation, San Francisco Media Office, *FBI Releases Internet Crime Report* (April 4, 2024).

[5] Transportation Security Administration, TSA Updates, Renews Cybersecurity Requirements for Pipeline Owners, Operators, (July 26, 2023) (www.tsa.gov/news/press/releases/2023/07/26/tsa-updates-renews-cybersecurity-requirements-pipeline-owners).

[6] Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government (September 19, 2023) (https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf).

to the Federal Register, regulators published 48 final rules, or an average of ten rules a year, covering adjustments to minimum cybersecurity standards, increased reporting requirements for vulnerabilities, cyber incidents, and other cybersecurity requirements.[7] Most commonly, a cybersecurity regulation sets out a particular standard or practice for a specific industry that addresses a significant cybersecurity threat. For example, in December 2023, the Farm Credit Administration updated and revised its rules for a broader cyber risk focus and to codify the requirement for each Farm Credit System institution to implement a comprehensive, written cyber risk management program consistent with the specific profile and complexity of the institution's operations.[8]

Agency rule-promulgation has provided industries with guidance, but also has created an array of protocols and industry requirements that may be onerous and repetitive, causing inefficiencies, while also raising costs for business.[9] In addition, as each organization creates their own varying levels of compliance with the regulations, it causes confusion between and among federal, local and state agencies, and creates obstacles to battling malicious cyber activity.[10]

Moreover, much of this regulatory work has been done in response to incidents, threats, or new commercial products, without discussion or consideration for entities who are overseen by multiple overlapping regulators. These redundancies may lead to cybersecurity teams spending up to 70% of their time on compliance rather than security.[11] The Office of the National Cyber Director (ONCD) published a 2024 report regarding overlapping and redundant regulations, which found lack of harmonization harms outcomes, increases costs, and increases administrative burdens. The report detailed a lack of harmonization across and within agencies of the federal government, but also between state and federal regulators. As an example, the Department of Homeland Security (DHS) and its components of the Transportation Security Administration, Cybersecurity and Infrastructure Security Agency, and the Coast Guard all have responsibility as it pertains to the oil and natural gas sectors. The report found that even within the abovementioned components of DHS, those regulations were duplicative and conflicting, and created an unnecessary administrative burden.[12]

In a Senate Homeland Security and Governmental Affairs Committee hearing in 2024, ONCD testified that since the Committee's

---

[7] The Federal Register, Home Page (www.federalregister.gov/documents/search?conditions%5Bterm%5D=cybersecurity%2BAND%2Bregulation) (accessed Sept. 11, 2024).

[8] Farm Credit Administration, 88 FR 85825, (Dec. 11, 2023).

[9] Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* (September 19, 2023) (www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf); Office of the National Cyber Director, *Cybersecurity Regulatory Harmonization RFI Summary* (June 2024) (www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf).

[10] Government Accountability Office, *Efforts Initiated to Harmonize Regulations, but Significant Work Remains* (June 5, 2024) (GAO–24–107602).

[11] Bank Policy Institute, Briefing with Majority and Minority Staff of Senate Homeland Security and Government Affairs Committee (May 29, 2024); Chamber of Commerce, Briefing with Majority and Minority Staff of Senate Homeland Security and Government Affairs Committee (May 29, 2024).

[12] Office of the National Cyber Director, *Cybersecurity-regulatory-harmonization-RFI-summary* (June 2024) (www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf).

last hearing on this topic in 2017, the "efforts to confront cyber threats aggressively have not been anchored in a comprehensive policy framework for regulatory harmonization" even though "effective cybersecurity regulations minimize the cost and burden of compliance while maximizing their cybersecurity risk reduction effect."[13] For example, the Government Accountability Office reported that four federal agencies had established cybersecurity requirements for states to secure their data, but these requirements had conflicting parameters in up to 79% of the requirements.[14] The President's National Security Telecommunications Advisory Committee (NSTAC) has also emphasized the danger of proliferating cybersecurity requirements and a lack of alignment to consensus standards causing resources to be diverted from improving security. While some limited progress has been made, the 2023 NSTAC report highlighted that a government office with congressional support is needed to provide the legal foundation to forge partnerships and help bring regulators and non-regulators closer.[15]

Since its inception, ONCD has worked to improve cybersecurity writ large across the nation through the development of the President's National Cybersecurity Strategy (NCS) that was issued on March 2, 2023, and the NCS Implementation Plan on July 13, 2023.[16] Recognizing the importance of addressing the harmonization problem, according to NCS, ONCD has tackled harmonization of the larger body of cybersecurity regulation with the goal to have effective regulations to "minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets."[17] ONCD's work on harmonization, however, is limited to only voluntary streamlining of regulations by executive branch agencies.

Currently, the other federal entities working to harmonize cybersecurity regulations are the Cybersecurity Forum for Independent and Executive Branch Regulators led by the Federal Communications Commission and the Cyber Incident Reporting Council led by the DHS. However, these bodies were primarily created for information sharing and voluntary collaboration, and they cannot independently compel agencies to make changes aimed at harmonizing regulations.[18] ONCD's ability to compel harmonization is limited to

---

[13] Senate Homeland Security and Governmental Affairs Committee, *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization*, 118th Cong. (June 5, 2024) (S. Hrg. 118–353); Senate Homeland Security and Governmental Affairs Committee, Testimony Submitted for the Record of Assistant National Cyber Director Programs Nicholas Leiserson, Office of the National Cyber Director, *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization*, 118th Cong. (June 5, 2024) (S. Hrg. 118–353).

[14] Senate Homeland Security and Governmental Affairs Committee, Testimony Submitted for the Record of Director David Hinchman, Government Accountability Office, *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization*, 118th Cong. (June 5, 2024) (S. Hrg. 118–353); *TSA Has Screwed This Up: Pipeline Cyber Rules Hitting Major Hurdles*, Politico (Mar. 17, 2022) (www.politico.com/news/2022/03/17/tsa-has-screwed-this-up-pipeline-cyber-rules-hitting-major-hurdles-00017893).

[15] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President: Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem* (Feb. 21, 2023) (www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf).

[16] The White House, Office of the National Cyber Director, (www.whitehouse.gov/oncd/) (accessed May 28, 2023).

[17] The White House, *National Cybersecurity Strategy Implementation Plan* (July 13, 2023) (www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/).

[18] Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* (September 19, 2023) (www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20-

executive branch agencies currently, however, ONCD has been working to encourage independent regulatory agencies to voluntarily harmonize.[19] This bill would build on ONCD's current voluntary work by compelling all federal agencies, including independent regulatory agencies, to commit to working on harmonization and participate in the Harmonization Committee. Beyond the United States, establishing a clear process for harmonization can be translated to other partner and allied nations—further streamlining cybersecurity regulations around the world and allowing companies and organizations to shift resources from compliance to cybersecurity operations and improving the cybersecurity landscape for all.

III. Legislative History

Senator Gary Peters (D–MI) introduced S. 4630, the *Streamlining Federal Cybersecurity Regulations Act*, on July 8, 2024, with Senator James Lankford (R–OK) as original cosponsor. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 4630 at a business meeting on July 31, 2024. At the business meeting, Senator Peters offered a substitute amendment to the bill, as well as a modification to the substitute amendment. The Peters substitute amendment, as modified, required the Harmonization Committee membership list to be publicly posted and regularly updated, clarified subsequent pilot programs, and clarified that the Congressional annual reports must include information on nonparticipation in Committee activities and any determinations made on cyber requirements. The Committee adopted the modification to the Peters substitute amendment and the underlying substitute by unanimous consent with Senators Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Blumenthal, Butler, Paul, Lankford and Scott present. The Committee adopted the Peters substitute amendment, as modified, by unanimous consent with Senators Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Blumenthal, Butler, Paul, Lankford and Scott present.

The bill, as amended by the Peters substitute amendment as modified, was ordered reported favorably by roll call vote of 10 yeas to 1 nay, with Senators Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Blumenthal, Butler, Lankford, and Scott voting in the affirmative, and Senator Paul voting in the negative. Senators Johnson, Romney, Hawley, and Marshall voted yea by proxy, for the record only.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section establishes the short title of the bill as the "Streamlining Federal Cybersecurity Regulations Act."

Federal%20Government.pdf); *Cybersecurity Regulators Forum Aims to Develop 'Shared Lexicon' for Minimum Requirements*, Inside Cybersecurity (August 1, 2024) (insidecybersecurity.com/daily-news/cybersecurity-regulators-forum-aims-develop-shared-lexicon-minimum-requirements); Government Accountability Office, *Efforts Initiated to Harmonize Regulations, but Significant Work Remains* (June 5, 2024) (GAO–24–107602).

[19] *Id.*

Section 2. Definitions

This section defines the terms "agency", "appropriate congressional committees", "committee", "cybersecurity requirement", "harmonization" "independent regulatory agency", "reciprocity", "regulatory agency" "regulatory framework" and "sector risk management agency".

Section 3. Establishment of interagency committee to harmonize regulatory regimes in the United States relating to cybersecurity

Subsection (a) requires the National Cyber Director to establish an interagency committee to be known as the Harmonization Committee to enhance the harmonization of cybersecurity requirements. Additionally, it requires the National Cyber Director to support the committee with administrative management support.

Subsection (b) delineates the committee composition, including the National Cyber Director, head of each regulatory agency, the head of the Office of Information and Regulatory Affairs, and the heads of other appropriate agencies. It further requires the Committee maintain a publicly available website listing the agencies that are represented on the Committee.

Subsection (c) names the chair as the National Cyber Director.

Subsection (d) discusses the development of a charter, which is delivered to Congress and made publicly available. This charter will include the processes and rules as well as the objective and scope of the committee.

Subsection (e) provides the regulatory framework for harmonization, including the establishment of a reciprocal compliance mechanism, the identification of cybersecurity requirements that are overly burdensome, inconsistent or contradictory, and the development of recommendations. It also requires the framework be published in the Federal Register for public comment.

Subsection (f) explains the pilot program implementation, in which no fewer than three (3) regulatory agencies, selected by the committee, carry out the program to implement the framework of subsection (e). It further provides for additional pilot programs following the completion of the initial pilot program.

Subsection (g) discusses the requirement for the heads of regulatory agencies to consult with the committee regarding the establishment or updating of cybersecurity requirements.

Subsection (h) outlines the necessity for the Committee to consult with appropriate Sector Risk Management Agencies, and with members of industry and critical infrastructure as appropriate in the development of the regulatory framework under subsection (e) and the implementation of the pilot program under subsection (f).

Subsection (i) outlines the reporting requirements, including an annual report and a pilot program report.

Section 4: Status updates on Incident Reporting

Subsection (a) requires a status update be provided to congress no later than 180 days after the enactment of this act, and not less than every 180 days thereafter.

Subsection (b) requires annual briefings to 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.

Section 5: Rule of construction

This section states nothing in this act shall alter or expand existing regulatory authorities of any agency.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

S. 4630, Streamlining Federal Cybersecurity Regulations Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 31, 2024

By Fiscal Year, Millions of Dollars	2024	2024-2029	2024-2034
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	5	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2035?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2035?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 4630 would require the National Cyber Director to create policy guidance for federal agencies to reduce duplicative or contradictory cybersecurity regulations. Under the bill, the director would establish an interagency committee to study federal cyber regulations, identify regulations that are overly burdensome on the private sector, and recommend changes to such regulations. S. 4630 also would require the director to implement a pilot program to assess the new policy guidance at three or more federal agencies and to report to the Congress on the results of those efforts. For purposes of this estimate, CBO assumes the bill will be enacted in 2025.

Using information about the cost of similar interagency committees, CBO estimates that staff salaries and other administrative expenses necessary to operate the committee that would be established by S. 4630 would cost $4 million over the 2024–2029 period. CBO also estimates that satisfying the reporting requirements of S. 4630 would cost $1 million over the 2024–2029 period. In total, implementing S. 4630 would cost $5 million over the 2024–2029 pe-

riod, CBO estimates. Any spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

* * * * * * *

Subchapter XVIII—Cybersecurity and Infrastructure Security Agency

* * * * * * *

PART D—CYBER INCIDENT REPORTING

* * * * * * *

SEC. 681f. CYBER INCIDENT REPORTING COUNCIL

(a) * * *

(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.*

[(b)] *(c)* * * *

* * * * * * *

○