Calendar No. 587

117TH CONGRESS *2nd Session*	SENATE	REPORT 117–228

INTRAGOVERNMENTAL CYBERSECURITY INFORMATION SHARING ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 4000

TO REQUIRE THE ESTABLISHMENT OF CYBERSECURITY INFORMATION SHARING AGREEMENTS BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND CONGRESS, AND FOR OTHER PURPOSES

DECEMBER 5, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

39–010 WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 587

117TH CONGRESS
2d Session

SENATE

REPORT
117–228

INTRAGOVERNMENTAL CYBERSECURITY INFORMATION SHARING ACT

DECEMBER 5, 2022.—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. 4000]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4000), to require the establishment of cybersecurity information sharing agreements between the Department of Homeland Security and Congress, 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. 4000, the *Intragovernmental Cybersecurity Information Sharing Act*, improves intra-branch cybersecurity by requiring the President of the United States to enter into an agreement with the Sergeant at Arms and Doorkeeper of the United States Senate and the Chief Administrative Officer of the United States House of Representatives to ensure robust collaboration between the executive branch and Congress on federal cybersecurity. This bill will empower cybersecurity professionals in each branch to work together,

outside of the Congressional oversight context, to protect federal networks and systems. The bill lists some examples of what such an agreement may include, but defers to the parties to set the bounds of the agreement.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Cyber criminals and state actors, such as Russia and China, present potent security threats.[1] Cyber-attacks disrupt critical infrastructure sectors and government networks, including those used by Congressional staff.[2] Recent large-scale targets for cyberattacks include information technology companies such as SolarWinds, food suppliers like JBS meatpacking, and critical infrastructure, including Colonial Pipeline.[3] Moreover, studies by cybersecurity firms estimate that attacks on the public sector cost taxpayers millions of dollars.[4]

It is clear that the federal government and its partners in the private sector remain vulnerable to cyberattacks by foreign and criminal adversaries. The Cybersecurity and Infrastructure Security Agency (CISA) encourages stakeholders, including critical infrastructure owners and operators and the federal government, "to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical infrastructure." [5] While entities such as the Federal Acquisition Security Council already exist to create a "combined information-sharing environment" between executive federal agencies with regard to supply chain security, there is no such collaboration be-

---

[1] Senate Committee on Homeland Security and Governmental Affairs, Testimony Submitted for the Record of Secretary Alejandro N. Mayorkas, Homeland Security Department, *Hearing on Resources and Authorities Needed to Protect and Secure the Homeland,* 117th Cong. (May 4, 2022).

[2] Senate Committee on Homeland Security and Governmental Affairs, Testimony for the Record of Secretary Alejandro N. Mayorkas, Homeland Security Department, *Hearing on a Review of the Fiscal Year 2022 Budget Requests for the Department of Homeland Security,* 117th Cong. (July 27, 2021) (The United States "faces growing cyber threats from nation states and criminal groups alike. [The Department of Homeland Security has] discovered several intrusion campaigns impacting the federal government."); See Senate Committee on Homeland Security and Governmental Affairs, Statement of Director Christopher A. Wray, Federal Bureau of Investigation, *Hearing on Worldwide Threats* at 5–9, 117th Cong. (Sept. 21, 2021); Also see *Congress Zooms in on Cybersecurity After Banner Year of Attacks,* The Hill (Dec. 28, 2021) (https://thehill.com/policy/cybersecurity/587165-congress-zooms-in-on-cybersecurity-after-banner-year-of-attacks/); Senators Gary Peters, Ron Johnson, Ron Wyden, and Tom Cotton: *Peters, Colleagues Press to Strengthen Technology Supply Chain and Protect National Security* (Oct. 10, 2019); Letter from Chairman Ron Johnson, Ranking Member Gary Peters, and Senators Tom Cotton and Ron Wyden to Director Mick Mulvaney, Office of Management and Budget (Oct. 9, 2019); *Russians Targeted Senate and Conservative Think Tanks, Microsoft Says*, CNN (Aug. 22, 2018) (https://www.cnn.com/2018/08/21/politics/microsoft-russia-american-politicians/index.html).

[3] Senate Committee on Homeland Security and Governmental Affairs, Testimony Submitted for the Record of Federal Chief Information Security Officer Christopher J. DeRusha, Office of Budget and Management, *Hearing on Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective,* 117th Cong. (Mar. 18, 2021); Senate Committee on Homeland Security and Governmental Affairs, Emerging Threats and Spending Oversight Subcommittee, Opening Statement of Chairwoman Maggie Hassan, *Hearing on Addressing Emerging Cybersecurity Threats to State and Local Government,* 117th Cong. (June 17, 2021); Senate Committee on Homeland Security and Governmental Affairs, Testimony Submitted for the Record of Joseph Blount, President and Chief Executive Officer of Colonial Pipeline Company, *Hearing on Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack,* 117th Cong. (June 8, 2021).

[4] Hassan, *supra* note 3; See Cybersecurity and Infrastructure Security Agency, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Oct. 26, 2020).

[5] Cybersecurity & Infrastructure Security Agency, *Sharing Cyber Event Information: Observe, Act, Report* (Apr. 2022); See also *House Passes Cybersecurity Bill*, The Hill (Apr. 22, 2015) (https://thehill.com/blogs/floor-action/house/239756-house-passes-cybersecurity-bill/) (Prior legislation to ensure the sharing of cyberattack information was "the biggest step the country [could] take to thwart hackers. Lawmakers, government officials and most industry groups argue more data will help both sides understand their attackers and bolster network defenses that have been repeatedly compromised.").

tween Congress and executive federal agencies in either information technology supply chain security or broader cybersecurity.[6]

Currently, executive federal agencies and the intelligence community often regard requests for cybersecurity information from the security components of the House and Senate as Congressional oversight requests, rather than security collaboration requests, leading to delays in intra-branch communication on security matters that can threaten the federal government's cybersecurity.[7] This legislation would streamline the federal government's preparations for, and responses to, cyberattacks by promoting operational collaboration between the branches. The shared information will be useful for filling gaps in each branch's awareness, deploying assistance to those impacted by a cyberattack, and analyzing trends.[8] With the branches working more closely to identify and assess cyber threats, the federal government will be better positioned to prevent and respond to cyberattacks.

III. LEGISLATIVE HISTORY

Senators Rob Portman (R–OH), Amy Klobuchar (D–MN), Roy Blunt (R–MO), and Gary Peters (D–MI) introduced S. 4000, the Intragovernmental Cybersecurity Information Sharing Act, on April 5, 2022. The bill was referred to the Committee on Homeland Security and Governmental Affairs. The Committee considered S. 4000 at a business meeting on May 25, 2022.

During the business meeting, a substitute amendment was offered by Senators Portman and Peters that addressed technical drafting assistance from the Executive Branch. The substitute amendment included clarifying that the purpose of the bill is to enhance collaboration between the Executive Branch and Congress on implementing cybersecurity measures to protect Legislative Branch information technology systems. It also amended the bill to direct the President of the United States, or their designee, to enter into the agreement with Congress, rather than the Secretary of Homeland Security. This was changed to allow for sharing of information from agencies other than the Department of Homeland Security. The substitute was adopted by voice vote *en bloc* with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley present for the vote.

The Committee ordered the bill, as amended, favorably reported by voice vote *en bloc*. Senators present for the vote on the bill were: Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley. Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

---

[6] Senators Gary Peters, Ron Johnson, Ron Wyden, and Tom Cotton: *Peters, Colleagues Press to Strengthen Technology Supply Chain and Protect National Security* (Oct. 10, 2019).

[7] Discussions between HSGAC committee staff and the Sergeant at Arms and Doorkeeper of the United States Senate and the Chief Administrative Officer of the United States House of Representatives.

[8] Director Jen Easterly, Cybersecurity and Infrastructure Security Agency: *Statement from CISA Director Easterly on Passage of Cyber Incident Reporting Legislation* (Mar. 11, 2022) (Information sharing "will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential threats."); *See* Institute for Security and Technology, *Report: Combating Ransomware* (2021) (Recommending a "whole of government" approach to protecting from ransomware attacks.).

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the name of the bill as the "Intragovernmental Cybersecurity Information Sharing Act."

Section 2. Requirement for information sharing agreements

Subsection (a) requires the President, or his designee, to negotiate at least one cybersecurity information sharing agreement with the Sergeant at Arms and Doorkeeper of the Senate and the Chief Administrative Officer of the House of Representatives.

Subsection (b) defines the provisions that may be included in such a cybersecurity information sharing agreement. Sharing agreements may include the identification and exchange of risk factors, the sharing of both classified and unclassified information, the installation of congressional cybersecurity professionals at operations centers, and any other elements the parties find appropriate.

Subsection (c) requires the Secretary of Homeland Security to periodically brief Congressional committees on the status of implementation of the cybersecurity information sharing agreements.

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

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 23, 2022.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 4000, the Intragovernmental Cybersecurity Information Sharing Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 4000, Intragovernmental Cybersecurity Information Sharing Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on May 25, 2022

By Fiscal Year, Millions of Dollars	2022	2022-2027	2022-2032
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	10	not estimated

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 2033?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 4000 would require the Department of Homeland Security (DHS) to provide the Congress with data on cyber threats to the information technology networks of the legislative branch. Under the bill, DHS would share classified and unclassified indicators of malicious cyber activity with the Congress. DHS also would offer workspace to Congressional cybersecurity personnel at the operations centers of the department.

Using information from DHS about the costs of similar information sharing programs, CBO estimates that implementing S. 4000 would cost about $2 million annually, on average, totaling $10 million over the 2022–2027 period. CBO expects that DHS would contract with a cybersecurity services provider to develop a threat-sharing platform and analyze malicious activity. Such 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 Leo Lex, Deputy Director of Budget Analysis.

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

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.

○