Calendar No. 381

118TH CONGRESS *2d Session*	SENATE	REPORT 118–170

RURAL HOSPITAL CYBERSECURITY ENHANCEMENT ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1560

TO REQUIRE THE DEVELOPMENT OF A COMPREHENSIVE RURAL HOSPITAL CYBERSECURITY WORKFORCE DEVELOPMENT STRATEGY, AND FOR OTHER PURPOSES

MAY 9, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
49–010 WASHINGTON : 2024

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*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 381

118TH CONGRESS *2d Session* | SENATE | REPORT 118–170

RURAL HOSPITAL CYBERSECURITY ENHANCEMENT ACT

MAY 9, 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. 1560]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1560) to require the development of a comprehensive rural hospital cybersecurity workforce development strategy, 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. 1560, the *Rural Hospital Cybersecurity Enhancement Act*, aims to address the need for skilled cybersecurity professionals in rural healthcare settings. The legislation directs the Cybersecurity and Infrastructure Security Agency (CISA) to develop a comprehensive strategy to improve cybersecurity preparedness and create a technical workforce to protect rural healthcare systems from cyber threats.

The legislation requires the CISA Director to ensure that the strategy include topics, like opportunities for public-private partnerships to strengthen cybersecurity, development of curricula and

training resources to build technical skills of the healthcare workforce, and policy recommendations. The strategy will also identify workforce challenges and common mitigation practices for rural and non-rural hospitals. Moreover, the bill requires the CISA Director to make cybersecurity instructional materials available for rural hospitals and to annually report to the Homeland Security and Governmental Affairs Committee of the Senate and Committee on Homeland Security in the House of Representatives with updates regarding the strategy and any programs that have been implemented pursuant to the strategy.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Cyberattacks on critical infrastructure continue to increase in sophistication as cyber adversaries and criminals compromise vital assets integral to the delivery of critical services to the public.[1] The health care and public health sectors face cyberattacks that threaten the confidentiality, availability, integrity, and reliability of systems, data, and personnel that provide lifesaving, diagnostic, and comprehensive care to patients across the country.[2] The expansion of interconnected medical devices and systems used for patient care, medical research, health care, and public health operations has increased potential points of entry to networks for adversaries or criminals.[3] Cyber-attackers continue to target the paths of least resistance to compromise systems, often through under-resourced rural health care delivery ecosystems.[4]

Rural health care ecosystems are vulnerable to cyber-attacks due to a combination of factors, such as staffing shortages, lack of expertise in cybersecurity, and inadequate resources.[5] According to two health care executives, the leadership of rural medical facilities are often forced to decide whether to invest in personnel and resources to enhance cybersecurity defenses, or in personnel and resources capable of maintaining the delivery of patient care. St. Margaret's Health in Spring Valley, Illinois, for example, had its systems crippled by ransomware, preventing the organization from submitting claims to insurers, Medicare, and Medicaid, for months, and ultimately leading to the organization closing its facility.[6] A 2021 analysis of ransomware attack impacts on hospitals found short term critical care disruptions, including the diversion of

---

[1] Government Accountability Office, *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure* (GAO–23–106441) (Feb. 7, 2023).

[2] Greg Garcia, Executive Director, Healthcare Sector Coordinating Council, Interview with Senate Committee on Homeland Security and Governmental Affairs (Mar. 1, 2023).

[3] Kate Pierce, Senior Virtual Information Security Officer, Fortified Health Security, Interview with Senate Committee on Homeland Security and Governmental Affairs (Feb. 27, 2023); Greg Garcia, Executive Director, Healthcare Sector Coordinating Council, Interview with Senate Committee on Homeland Security and Governmental Affairs (Mar. 1, 2023); Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, *Health Industry Cybersecurity-Managing Legacy Technology Security,* (Mar. 3, 2023) (www.healthsectorcouncil.org/legacy-tech-security/); Armis: *Armis Data Highlights Increased Risk for Healthcare Organizations as Attack Surface Expands* (Nov. 10, 2021); Government Accountability Office, *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure* (GAO–23–106441) (Feb. 7, 2023).

[4] *Id.*

[5] Minnesota Department of Health, Office of Rural Health and Primary Care, Critical Access Hospitals (www.health.state.mn.us/facilities/ruralhealth/flex/cah/index.html) (accessed Dec. 12, 2023); Centers for Medicare and Medicaid Services, Critical Access Hospitals (www.cms.gov/Medicare/Provider-Enrollment-and-Certification/CertificationandComplianc/CAHs) (accessed Dec. 11, 2023).

[6] *An Illinois Hospital is the First Health Care Facility to Link its Closing to a Ransomware Attack*, NBC News (June 12, 2023) (www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983).

emergency patients to other hospitals which can drastically reduce patient survival rates, and long-term complications of care for patients.[7] The study found that victim hospitals were more likely to experience hospital strain for weeks or even months after the attack, leading to worsening health outcomes for patients, including excess deaths.[8]

Additionally, rural hospitals struggle to recover the costs associated with being victims of cyberattacks. The second-hand impacts of attacks are often handed down to patients, medical insurance providers, electronic health record companies, and cybersecurity insurance providers.[9] The "hack one, breach many" strategy of cybercriminals is prevalent in the rural health care delivery ecosystem. Here, rural hospitals frequently do not have basic or robust security practices. They often further lack technology teams to defend their infrastructure, conduct and plan for continuity and recovery if an attack occurs, and conduct risk-based analysis on the evolving threat landscape.[10]

S. 1560, the *Rural Hospital Cybersecurity Enhancement Act* follows a hearing before this Committee in March 2023, in which rural health care facilities were identified as soft targets for cybercriminals.[11] Vulnerabilities in the cybersecurity of rural hospitals can also be used to disrupt larger healthcare systems, potentially jeopardizing the sensitive medical and personal data of hundreds of thousands of American patients simultaneously. This bill will increase the cyber-resilience of the rural health care delivery ecosystem and establish the steering of these collaborative efforts through CISA.

III. LEGISLATIVE HISTORY

Senator Josh Hawley (R–MO) introduced S. 1560, the *Rural Hospital Cybersecurity Enhancement Act*, on May 11, 2023, with original cosponsor Senator Gary Peters (D–MI). The bill was referred to the Committee on Homeland Security and Governmental Affairs. Senator Jon Ossoff (D–GA) and Senator Raphael Warnock (D–GA) joined the bill as cosponsors on May 16, 2023 and July 19, 2023, respectively.

The Committee considered S. 1560 at a business meeting on June 14, 2023. At the business meeting, Senator Hawley, for himself and Senator Peters, offered a substitute amendment to the bill, as well as modification to the substitute amendment. The Hawley-Peters substitute amendment as modified made technical edits and clarified that relationships between, or common issues facing, rural and non-rural health care systems may be helpful in addressing rural healthcare challenges. The substitute amendment as modified also removed a Federal Advisory Council Act exemption in the bill. The Committee adopted the modification to the Hawley-Peters sub-

---

[7] Cybersecurity and Infrastructure Security Agency, *Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm* (September, 2021) (www.cisa.gov/sites/default/files/publications/Insights_MedicalCare_FINAL-v2_0.pdf).

[8] *Id.*

[9] Kate Pierce, Senior Virtual Information Security Officer, Fortified Health Security, Interview with Senate Committee on Homeland Security and Governmental Affairs (Feb. 27, 2023).

[10] CORL Technologies, *Mitigating Fourth-Party Cyber Risks in Healthcare*, CORL Technologies (blog) (Apr. 21, 2022) (www.corltech.com/blog/mitigating-fourth-party-cyber-risks-in-healthcare/).

[11] Senate Committee on Homeland Security and Governmental Affairs, Hearing Memorandum, *In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector*, 118th Cong. (Mar. 16, 2023) (S. Hrg. 118–55).

stitute amendment by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present. The Hawley-Peters substitute amendment, as modified, was adopted by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

Senator Paul offered an amendment adding a provision stating that no additional funds are authorized for the implementation of the bill. The Paul amendment was adopted by voice vote with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

The bill, as amended the Hawley-Peters substitute amendment as modified and the Paul amendment, was ordered reported favorably by roll call vote of 10 yeas to 0 nays, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Lankford, Romney, Scott, and Hawley voting in the affirmative and Senator Paul recorded "present." Senators Carper, Blumenthal, Johnson, 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 name of the bill as the "Rural Hospital Cybersecurity Enhancement Act."

Section 2. Definitions

This section defines the terms "agency," "appropriate committees of Congress," "Director," "geographic division," "rural hospital," and "Secretary."

Section 3. Rural hospital cybersecurity workforce development strategy

Subsection (a) requires the Secretary of Homeland Security, acting through the Director of CISA, to develop and transmit a comprehensive rural hospital cybersecurity workforce development strategy to the Senate Homeland Security and Governmental Affairs Committee (HSGAC) and the House Committee on Homeland Security (CHS).

Subsection (b) allows the Secretary of Homeland Security and CISA Director to consult with the Secretaries of Health and Human Services, Education, Labor, and any other appropriate agency in carrying out subsection (a). It also requires the Secretary of Homeland Security to consult with at least two representatives of rural healthcare providers from each of the nine U.S. geographic divisions determined by the Census Bureau.

Subsection (c) requires that the strategy under subsection (a) consider partnerships with non-governmental entities, cybersecurity curricula and teaching resources for use in rural educational institutions, identification of and best practices to mitigate cybersecurity workforce challenges in rural hospitals, and policy recommendations.

Subsection (d) requires the Secretary of Homeland Security to provide an annual briefing to HSGAC and CHS that includes updates to the strategy, any programs or initiatives established pursuant to the strategy and the number of individuals served, addi-

tional policy recommendations, and the effectiveness of the strategy in addressing the need for skilled cybersecurity professionals in rural hospitals.

Section 4. Instructional materials for rural hospitals

Subsection (a) requires the CISA Director to make available instructional materials for rural hospitals that can be used to train staff on fundamental cybersecurity efforts.

Subsection (b) requires the CISA Director to, in carrying out subsection (a), consult with appropriate federal agencies and non-governmental experts, identify existing materials that can be adapted for use and create new materials as needed, and conduct an awareness campaign to promote the materials.

Section 5. No additional funds

This section states that no additional funds are authorized to be appropriated for the purpose of carrying out this bill.

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. 1560, Rural Hospital Cybersecurity Enhancement Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 14, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
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 2034?	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 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 1560 would require the Cybersecurity and Infrastructure Security Agency (CISA) to study cybersecurity threats facing rural hospitals. Under the bill, CISA would provide the Congress with recommendations to improve the recruitment and training of cyber professionals at rural hospitals. The bill also would require CISA

to develop and disseminate information on cyber safety measures to employees of rural hospitals.

Using information from CISA about similar information sharing efforts, CBO anticipates that the agency would need two full-time employees to prepare the reports and to develop online training resources for rural hospital employees. CBO estimates that staff salaries and technology costs to publish instructional materials would total $5 million over the 2023–2028 period. 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 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

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.

○