Calendar No. 527

117TH CONGRESS *2d Session*	SENATE	REPORT 117–177

HEALTHCARE CYBERSECURITY ACT OF 2022

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3904

TO ENHANCE THE CYBERSECURITY OF THE HEALTHCARE AND PUBLIC HEALTH SECTOR

OCTOBER 18, 2022.—Ordered to be printed
Filed, under authority of the order of the Senate of October 14, 2022

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. 527

117TH CONGRESS
2d Session

SENATE

REPORT
117–177

HEALTHCARE CYBERSECURITY ACT OF 2022

OCTOBER 18, 2022.—Ordered to be printed

Filed, under authority of the order of the Senate of October 14, 2022

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

R E P O R T

[To accompany S. 3904]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3904), to enhance the cybersecurity of the Healthcare and Public Health Sector, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and an amendment to the title, and recommends the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3904, the *Healthcare Cybersecurity Act of 2022*, aims to improve the cybersecurity of the Healthcare and Public Health Sector. The bill directs the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate with the Department of Health and Human Services (HHS) on improving cybersecurity in the Healthcare and Public Health Sector. As part of this, the bill requires CISA, in collaboration with HHS, to coordinate with and provide resources to non-Federal Healthcare and Public Health Sector entities, including products specific to those entities and sharing cyber threat indicators. Additionally, the HHS Secretary,

in coordination with CISA Cyber Security Advisors, CISA Cybersecurity State Coordinators, and private sector healthcare experts, must provide training to Healthcare and Public Health Sector asset owners and operators on cybersecurity risks and mitigations. Lastly, the bill requires the HHS Secretary to update the Healthcare and Public Health Sector Specific Plan, including an evaluation of challenges Healthcare and Public Health Sector entities face and an assessment of cybersecurity workforce shortages in the Healthcare and Public Health Sector.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Cyberattacks against entities in the Healthcare and Public Health Sector pose grave, and increasing, threats to the security of healthcare infrastructure, the safety of patients, and the security of individuals' personally identifiable information. According to an analysis of data from HHS, there were 599 healthcare data breaches in 2020, a 55 percent increase from 2019.[1] In 2020 alone, at least 24,000,000 individuals were affected by healthcare data breaches.[2] This included a ransomware attack on the fundraising software company Blackbaud, which exposed the data of millions of individuals, including 1.05 million donors to the Virginia-based Inova Health System.[3]

Cyberattacks with the potential to disrupt the functioning of Healthcare and Public Health Sector entities are also increasing. Amidst the COVID–19 pandemic, CISA, the Federal Bureau of Investigation (FBI), and HHS released an alert about ransomware threat actors targeting Healthcare and Public Health Sector entities.[4] According to CISA, past ransomware attacks against hospitals have "resulted in inaccessible patient schedules and records" and downstream effects included "cancelled or delayed surgeries and cancer treatments".[5]

The attack surface of the Healthcare and Public Health Sector includes medical devices, which are increasingly Internet-connected and can pose cybersecurity risks to hospital networks.[6] The Food and Drug Administration (FDA), a component agency of HHS, regulates medical devices and works to reduce cybersecurity risks.[7] When a vulnerability that can pose a risk is identified, the FDA issues a "safety communication" to inform patients, providers, and manufacturers.[8]

Cybersecurity risks in the Healthcare and Public Health Sector can only be addressed with a robust cybersecurity workforce. Glob-

---

[1] BitGlass, *Healthcare Breach Report 2021* (Feb. 17, 2021) (https://pages.bitglass.com/rs/418-ZAL–815/images/CDFY21Q1HealthcareBreachReport2021.pdf).

[2] *Id*.

[3] Hipaa Journal, *Inova Health System Says 1.05 Million Individuals Impacted by Blackbaud Ransomware Attack* (Sep. 11, 2020) (https://www.hipaajournal.com/inova-health-system-says-1-05-million-individuals-impacted-by-blackbaud-ransomware-attack/).

[4] U.S. Cybersecurity and Infrastructure Security Agency, *Ransomware Activity Targeting the Healthcare and Public Health Sector* (Oct. 28, 2020) (https://www.cisa.gov/uscert/ncas/alerts/aa20-302a).

[5] U.S. Cybersecurity and Infrastructure Security Agency, *Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm* (Sept. 2021) (https://www.cisa.gov/sites/default/files/publications/Insights__MedicalCare__FINAL-v2__0.pdf).

[6] U.S. Food and Drug Administration, *Cybersecurity* (Apr. 8, 2022) (https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity).

[7] U.S. Food and Drug Administration, *Medical Device Cybersecurity: What You Need to Know* (Feb. 4, 2022) (https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know).

[8] *Id*.

ally, there is an estimated shortage of 2.72 million cybersecurity workers.[9] This is especially true in the healthcare sector, where a 2018 study found that 79% of surveyed executives in healthcare organizations reported difficulty recruiting cybersecurity personnel.[10]

CISA and HHS share responsibility to help protect Healthcare and Public Health Sector entities. As defined in law, Sector Risk Management Agencies, designated by the President, provide institutional knowledge and lead risk management activities in their sector, in coordination with the Department of Homeland Security (DHS).[11] As the Sector Risk Management Agency for the Healthcare and Public Health Sector, HHS's responsibilities include collaborating with healthcare asset owners and operators, coordinating sector-specific activities at the federal level, and carrying out incident management responsibilities.[12] As part of this, HHS operates the Health Sector Cybersecurity Coordination Center (HC3) to foster cybersecurity information sharing across the Healthcare and Public Health Sector.[13]

S. 3904 ensures that CISA and HHS coordinate to provide appropriate resources to Healthcare and Public Health Sector entities to prevent, detect, and respond to cyber incidents. This includes developing products for sector entities, information sharing, and providing cybersecurity training to sector asset owners and operators. Additionally, the bill requires that HHS update the Healthcare and Public Health Sector-Specific Plan, last updated in 2015, within one year of enactment.[14]

III. LEGISLATIVE HISTORY

Senator Jacky Rosen (D–NV) introduced S. 3904, the *Healthcare Cybersecurity Act of 2022*, on March 23, 2022, with Senator Bill Cassidy (R–LA). The bill was referred to the Committee on Homeland Security and Governmental Affairs. Senators Margaret Hassan (D–NH), Jon Ossoff (D–GA), Thom Tillis (R–NC), and Dianne Feinstein (D–CA) later joined as cosponsors on March 28, 2022, April 4, 2022, April 6, 2022, and May 16, 2022, respectively.

The Committee considered S. 3904 at a business meeting on March 30, 2022. During the business meeting, Senator Rosen offered a substitute amendment, as modified. The Rosen substitute amendment, as modified, updated the bill to require the HHS Secretary to update the Healthcare and Public Health Sector Specific Plan, rather than the CISA Director conducting a study and issuing a report. The Rosen substitute amendment, as modified, also included changes to require the HHS Secretary, in coordination with CISA and private sector healthcare experts, to provide training to Healthcare and Public Health Sector asset owners and

---

[9] International Information System Security Certification Consortium, *A Resilient Cybersecurity Profession Charts the Path Forward* (2021) (https://www.isc2.org/Research/Workforce-Study).

[10] Merlin International, *Merlin International & Ponemon Institute Cybersecurity Study Signals Dangerous Diagnosis for Healthcare Industry* (Mar. 12 2018) (https://www.businesswire.com/news/home/20180312005302/en/Merlin-International-Ponemon-Institute-Cybersecurity-Study-Signals).

[11] 6 U.S. Code § 651.

[12] U.S. Government Accountability Office, *HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration* (June 2021) (https://www.gao.gov/assets/gao-21-403.pdf).

[13] U.S. Department of Health and Human Services, *Health Sector Cybersecurity Coordination Center (HC3)* (Mar. 31, 2022) (https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html).

[14] U.S. Cybersecurity and Infrastructure Security Agency, *Healthcare and Public Health Sector-Specific Plan* (May 2016) (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf).

operators, rather than CISA. The Rosen substitute amendment, as modified, was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

Senator Rosen offered another amendment to change the long title of the bill. The Rosen amendment was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

The bill, as amended, was ordered reported favorably by voice vote *en bloc*. Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley were present for the vote.

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

Section 1. Short title

This section designates the name of the bill as the "Healthcare Cybersecurity Act of 2022."

Section 2. Definitions

This section defines the terms "Agency," "Cybersecurity State Coordinator," "Department," "Director," "Healthcare and Public Health Sector," "Information Sharing and Analysis Organizations," and "Secretary".

Section 3. Findings

This section includes the findings of Congress.

Section 4. Agency coordination with the Department

Subsection (a) requires CISA and HHS to coordinate, including by entering into an agreement, as appropriate, to improve cybersecurity in the Healthcare and Public Health Sector.

Subsection (b) requires CISA to coordinate with and make resources available to Information Sharing and Analysis Organizations, information sharing and analysis centers, and certain other non-federal entities. This coordination includes information sharing of cyber threat indicators and developing products specific to the Healthcare and Public Health Sector's needs.

Section 5. Training for healthcare experts

This section requires the HHS Secretary, in coordination with private sector healthcare experts and CISA's regional advisors and state coordinators, to provide training to Healthcare and Public Health Sector asset owners and operators. This training covers cybersecurity risks to the sector and ways to mitigate these risks.

Section 6. Sector-specific plan

Subsection (a) requires the HHS Secretary, in coordination with the CISA Director, to update the Healthcare and Public Health Sector Specific Plan within a year of enactment of this bill. The updated plan must include an analysis of cybersecurity risks affecting the sector. The updated plan must also include an evaluation of challenges the sector faces in securing information systems and medical devices, as well as implementing cybersecurity protocols

and responding to data breaches or cybersecurity attacks. Additionally, the updated plan must include: an evaluation of best practices for the deployment of CISA advisors over the course of data breaches or cybersecurity attacks, an assessment of Healthcare and Public Health Sector cybersecurity workforce shortages, an identification of cybersecurity challenges related to COVID–19, and an evaluation of ways for CISA and HHS to communicate and deploy cybersecurity recommendations and tools to sector assets.

Subsection (b) requires the HHS Secretary, in consultation with the CISA Director, to provide a briefing to Congress on required updates to the Healthcare and Public Health Sector Specific Plan set forth in subsection (a) no later than 120 days after the date of enactment of 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

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 6, 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. 3904, the Healthcare Cybersecurity Act of 2022.

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. 3904, Healthcare Cybersecurity Act of 2022

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 30, 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. 3904 would require the Cybersecurity and Infrastructure Security Agency (CISA) to provide cybersecurity threat information and training to health care providers in coordination with the Department of Health and Human Services. The bill also would require CISA to report to the Congress on the effectiveness of its efforts.

Under current law, CISA currently employs 32 analysts to provide training to and share information with eight critical infrastructure sectors. Using information from CISA, CBO expects that the agency would need four additional analysts to expand its support to the health care sector. CBO estimates that staff salaries and technology costs to deliver the training would total $2 million annually. Accounting for the time needed to hire new employees and develop the training, CBO estimates that implementing the bill would cost $10 million over the 2022–2027 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 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.

○