Calendar No. 683

118TH CONGRESS
2D SESSION

S. 4697

[Report No. 118–280]

To enhance the cybersecurity of the Healthcare and Public Health Sector.

IN THE SENATE OF THE UNITED STATES

JULY 11 (legislative day, JULY 10), 2024

Ms. ROSEN (for herself, Mr. YOUNG, Mr. KING, and Mr. OSSOFF) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 9, 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 enhance the cybersecurity of the Healthcare and Public Health Sector.

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 "Healthcare Cybersecurity Act of 2024".~~

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Agency'' means the Cybersecurity and Infrastructure Security Agency;

(2) the term ''covered asset'' means a Healthcare and Public Health Sector asset, including technologies, services, and utilities;

(3) the term ''Cybersecurity State Coordinator'' means a Cybersecurity State Coordinator appointed under section 2217(a) of the Homeland Security Act of 2002 (6 U.S.C. 665c(a));

(4) the term ''Department'' means the Department of Health and Human Services;

(5) the term ''Director'' means the Director of the Agency;

(6) the term ''Healthcare and Public Health Sector'' means the Healthcare and Public Health sector, as identified in Presidential Policy Directive 21 (February 12, 2013, relating to critical infrastructure security and resilience);

(7) the term ''Information Sharing and Analysis Organizations'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650);

(8) the term ''Plan'' means the Healthcare and Public Health Sector Specific Plan; and

(9) the term ''Secretary'' means the Secretary of Health and Human Services.

SEC. 3. FINDINGS.

Congress finds the following:

(1) Covered assets are increasingly the targets of malicious cyberattacks, which result not only in data breaches, but also increased healthcare delivery costs, and can ultimately affect patient health outcomes.

(2) Data reported to the Department shows that large cyber breaches of the information systems of healthcare facilities rose 93 percent between 2018 to 2022 .

(3) According to data from the Office for Civil Rights of the Department, health information breaches have increased since 2016, and in 2022 alone, the Department reported 626 breaches on covered entities, as defined under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191), affecting more than 500 people, with nearly 42,000,000 total people affected by health information breaches.

SEC. 4. AGENCY COORDINATION WITH THE DEPARTMENT.

(a) IN GENERAL.—The Agency shall coordinate with the Department, including by entering into an agreement,

as appropriate, to improve cybersecurity in the Healthcare and Public Health Sector.

(b) AGENCY LIAISON TO THE DEPARTMENT.—

(1) APPOINTMENT.—The Director shall, in coordination with the Secretary, appoint an individual, who shall be an employee of the Agency or a detailee assigned to the Department by the Director, to serve as the liaison of the Agency to the Department, who shall—

(A) have appropriate cybersecurity qualifications and expertise; and

(B) report directly to the Director.

(2) RESPONSIBILITIES AND DUTIES.—The liaison appointed under paragraph (1) shall—

(A) provide to the owners and operators of covered assets technical assistance regarding, information on, and best practices relating to improving cybersecurity;

(B) serve as a primary contact of the Department to coordinate cybersecurity issues with the Agency;

(C) support the implementation and execution of the Plan and assist in the development of updates to the Plan;

~~(D) facilitate the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;~~

~~(E) manage the implementation of the agreement entered into under subsection (a);~~

~~(F) implement the training described in section 5;~~

~~(G) coordinate between the Agency and the Department during cybersecurity incidents within the Healthcare and Public Health Sector; and~~

~~(H) perform such other duties as determined necessary by the Secretary to achieve the goal of improving the cybersecurity of the Healthcare and Public Health Sector.~~

~~(3) REPORT.—Not later than 18 months after the date of enactment of this Act, the liaison appointed under paragraph (1), in consultation with the Secretary and the Director, shall submit a report that describes the activities undertaken to improve cybersecurity coordination between the Agency and the Department to—~~

~~(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Fi-~~

nance, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Ways and Means, and the Committee on Homeland Security of the House of Representatives.

(c) ASSISTANCE.—

(1) IN GENERAL.—The Agency shall coordinate with and make resources available to Information Sharing and Analysis Organizations, information sharing and analysis centers, the sector coordinating councils, and non-Federal entities that are receiving information shared through programs managed by the Department.

(2) SCOPE.—The coordination under paragraph (1) shall include—

(A) developing products specific to the needs of Healthcare and Public Health Sector entities; and

(B) sharing information relating to cyber threat indicators and appropriate defensive measures.

SEC. 5. TRAINING FOR HEALTHCARE EXPERTS.

The Cyber Security Advisors and Cybersecurity State Coordinators of the Agency shall, in coordination, as appropriate, with the liaison appointed under section 4(b)(1) and private sector healthcare experts, provide training to the owners and operators of covered assets on—

(1) cybersecurity risks to the Healthcare and Public Health Sector and covered assets; and

(2) ways to mitigate the risks to information systems in the Healthcare and Public Health Sector.

SEC. 6. SECTOR-SPECIFIC PLAN.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary, in coordination with the Director, shall update the Plan, which shall include the following elements:

(1) An analysis of how identified cybersecurity risks specifically impact covered assets, including the impact on rural and small and medium-sized covered assets.

(2) An evaluation of the challenges the owners and operators of covered assets face in—

(A) securing—

(i) updated information systems owned, leased, or relied upon by covered assets;

(ii) medical devices or equipment owned, leased, or relied upon by covered assets, which shall include an analysis of the threat landscape and cybersecurity vulnerabilities of such medical devices or equipment; and

(iii) sensitive patient health information and electronic health records;

(B) implementing cybersecurity protocols; and

(C) responding to data breaches or cybersecurity attacks, including the impact on patient access to care, quality of patient care, timeliness of health care delivery, and health outcomes.

(3) An evaluation of best practices for the deployment of trained Cyber Security Advisors and Cybersecurity State Coordinators of the Agency into covered assets before, during, and after data breaches or cybersecurity attacks.

(4) An assessment of relevant Healthcare and Public Health Sector cybersecurity workforce shortages, including—

(A) training, recruitment, and retention issues; and

(B) recommendations for how to address these shortages and issues, particularly at rural and small and medium-sized covered assets.

(5) An evaluation of the most accessible and timely ways for the Agency and the Department to communicate and deploy cybersecurity recommendations and tools to the owners and operators of covered assets.

(b) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Secretary, in consultation with the Director, shall provide a briefing on the updating of the Plan under subsection (a) to—

(1) the Committee on Health, Education, Labor, and Pensions, the Committee on Finance, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Energy and Commerce, the Committee on Ways and Means, and the Committee on Homeland Security of the House of Representatives.

SEC. 7. IDENTIFYING HIGH-RISK COVERED ASSETS.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Director shall establish

~~objective criteria for determining whether a covered asset should be designated as a high-risk covered asset.~~

~~(b) METHODOLOGY.—The Director, in consultation with the Secretary, as appropriate, shall establish a methodology for determining whether a covered asset meets the criteria established under subsection (a) to be designated as a high-risk covered asset.~~

~~(c) LIST OF HIGH-RISK COVERED ASSETS.—~~

~~(1) IN GENERAL.—The Secretary shall develop a list of, and notify, the owners and operators of each covered asset determined to be a high-risk covered asset using the methodology established under subsection (b).~~

~~(2) BIANNUAL UPDATING.—The Secretary shall—~~

~~(A) biannually review and update the list of high-risk covered assets developed under paragraph (1); and~~

~~(B) notify the owners and operators of each covered asset added to or removed from the list as part of a review and update of the list under subparagraph (A).~~

~~(3) NOTICE TO CONGRESS.—The Secretary shall notify Congress when the initial list of high-risk covered assets is developed under paragraph (1)~~

~~and each time the list is updated under paragraph (2).~~

~~(4) USE.—The list developed and updated under this subsection shall be used by the Department to prioritize resource allocation to high-risk covered assets to bolster cyber resilience.~~

~~SEC. 8. REPORT ON ASSISTANCE PROVIDED TO ENTITIES OF HEALTHCARE AND PUBLIC HEALTH SECTOR.~~

~~Not later than 120 days after the date of enactment of this Act, the Agency shall submit to Congress a report on the organization-wide level of support and activities that the Agency has provided to the healthcare and public health sector to proactively prepare the sector to face cyber threats and respond to cyber attacks when such threats or attacks occur.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Healthcare Cybersecurity Act of 2024".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Agency" means the Cybersecurity and Infrastructure Security Agency;

(2) the term "covered asset" means a Healthcare and Public Health Sector asset, including technologies, services, and utilities;

(3) the term "Cybersecurity State Coordinator" means a Cybersecurity State Coordinator appointed under section 2217(a) of the Homeland Security Act of 2002 (6 U.S.C. 665c(a));

(4) the term "Department" means the Department of Health and Human Services;

(5) the term "Director" means the Director of the Agency;

(6) the term "Healthcare and Public Health Sector" means the Healthcare and Public Health sector, as identified in the National Security Memorandum on Critical Infrastructure and Resilience (NSM-22), issued April 30, 2024;

(7) the term "Information Sharing and Analysis Organizations" has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650);

(8) the term "Plan" means the Healthcare and Public Health Sector-specific Risk Management Plan; and

(9) the term "Secretary" means the Secretary of Health and Human Services.

SEC. 3. FINDINGS.

Congress finds the following:

(1) Covered assets are increasingly the targets of malicious cyberattacks, which result not only in data breaches, but also increased healthcare delivery costs, and can ultimately affect patient health outcomes.

(2) Data reported to the Department shows that large cyber breaches of the information systems of healthcare facilities rose 93 percent between 2018 to 2022.

(3) According to the "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022" issued by the Office for Civil Rights of the Department, breaches of unsecured protected health information have increased 107 percent since 2018, and, in 2022 alone, the Department received 626 reported breaches affecting not less than 500 individuals at covered entities or business associates (as defined in section 160.103 of title 45, Code of Federal Regulations) that occurred or ended in 2022, with nearly 42,000,000 individuals affected.

SEC. 4. AGENCY COORDINATION WITH THE DEPARTMENT.

(a) IN GENERAL.—The Agency shall coordinate with the Department to improve cybersecurity in the Healthcare and Public Health Sector.

(b) AGENCY LIAISON TO THE DEPARTMENT.—

(1) APPOINTMENT.—The Director shall, in coordination with the Secretary, appoint an individual, who shall be an employee of the Agency or a detailee assigned to the Administration for Strategic Preparedness and Response Office of the Department by the Director, to serve as a liaison of the Agency to the Department, who shall—

(A) have appropriate cybersecurity qualifications and expertise; and

(B) report directly to the Director.

(2) RESPONSIBILITIES AND DUTIES.—The liaison appointed under paragraph (1) shall—

(A) serve as a primary contact of the Department to coordinate cybersecurity issues with the Agency;

(B) support the implementation and execution of the Plan and assist in the development of updates to the Plan;

(C) facilitate the sharing of cyber threat information between the Department and the Agency to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(D) assist in implementing the training described in section 5;

(E) facilitate coordination between the Agency and the Department during cybersecurity incidents within the Healthcare and Public Health Sector; and

(F) perform such other duties as determined necessary by the Secretary to achieve the goal of improving the cybersecurity of the Healthcare and Public Health Sector.

(3) REPORT.—

(A) REQUIREMENT.—Not later than 18 months after the date of enactment of this Act, the Secretary, in coordination with the Director, shall submit a report that describes the activities undertaken to improve cybersecurity coordination between the Agency and the Department to—

(i) the Committee on Health, Education, Labor, and Pensions, the Committee on Finance, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(ii) the Committee on Energy and Commerce, the Committee on Ways and Means, and the Committee on Homeland Security of the House of Representatives.

(B) CONTENTS.—The report submitted under subparagraph (A) shall include—

(i) a summary of the activities of the liaison appointed under paragraph (1);

(ii) a description of any challenges to the effectiveness of the liaison appointed under paragraph (1) completing the required duties of the liaison; and

(iii) a study of the feasibility of an agreement to improve cybersecurity in the public sector of healthcare.

(c) RESOURCES.—

(1) IN GENERAL.—The Agency shall coordinate with and make resources available to Information Sharing and Analysis Organizations, information sharing and analysis centers, the sector coordinating councils, and non-Federal entities that are receiving information shared through programs managed by the Department.

(2) SCOPE.—The coordination under paragraph (1) shall include—

(A) developing products specific to the needs of Healthcare and Public Health Sector entities; and

(B) sharing information relating to cyber threat indicators and appropriate defensive measures.

SEC. 5. TRAINING FOR HEALTHCARE OWNERS AND OPERATORS.

The Agency shall make available training to the owners and operators of covered assets on—

(1) cybersecurity risks to the Healthcare and Public Health Sector and covered assets; and

(2) ways to mitigate the risks to information systems in the Healthcare and Public Health Sector.

SEC. 6. SECTOR-SPECIFIC RISK MANAGEMENT PLAN.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary, in coordination with the Director, shall update the Plan, which shall include the following elements:

(1) An analysis of how identified cybersecurity risks specifically impact covered assets, including the impact on rural and small- and medium-sized covered assets.

(2) An evaluation of the challenges the owners and operators of covered assets face in—

(A) securing—

(i) updated information systems owned, leased, or relied upon by covered assets;

(ii) medical devices or equipment owned, leased, or relied upon by covered assets, which shall include an analysis of the threat landscape and cybersecurity vulnerabilities of such medical devices or equipment; and

(iii) sensitive patient health information and electronic health records;

(B) implementing cybersecurity protocols; and

(C) responding to data breaches or cybersecurity attacks, including the impact on patient access to care, quality of patient care, timeliness of health care delivery, and health outcomes.

(3) An evaluation of the best practices for utilization of resources from the Agency to support covered assets before, during, and after data breaches or cybersecurity attacks, such as by Cyber Security Advisors and Cybersecurity State Coordinators of the Agency or other similar resources.

(4) An assessment of relevant Healthcare and Public Health Sector cybersecurity workforce shortages, including—

(A) training, recruitment, and retention issues; and

(B) recommendations for how to address these shortages and issues, particularly at rural and small- and medium-sized covered assets.

(5) An evaluation of the most accessible and timely ways for the Agency and the Department to communicate and deploy cybersecurity recommendations and tools to the owners and operators of covered assets.

(b) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Secretary, in consultation with the Director, shall provide a briefing on the updating of the Plan under subsection (a) to—

(1) the Committee on Health, Education, Labor, and Pensions, the Committee on Finance, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Energy and Commerce, the Committee on Ways and Means, and the Committee on Homeland Security of the House of Representatives.

SEC. 7. IDENTIFYING HIGH-RISK COVERED ASSETS.

(a) IN GENERAL.—The Secretary, in consultation with the Director and health sector owners and operators, as appropriate, may establish objective criteria for determining whether a covered asset may be designated as a high-risk covered asset, provided that such criteria shall align with the methodology promulgated by the Director for identifying functions relating to critical infrastructure, as defined in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)), and associated risk assessments.

(b) LIST OF HIGH-RISK COVERED ASSETS.—

(1) IN GENERAL.—The Secretary may develop a list of, and notify, the owners and operators of each covered asset determined to be a high-risk covered asset using the methodology promulgated by the Director pursuant to subsection (a).

(2) BIANNUAL UPDATING.—The Secretary may—

(A) biannually review and update the list of high-risk covered assets developed under paragraph (1); and

(B) notify the owners and operators of each covered asset added to or removed from the list as part of a review and update of the list under subparagraph (A).

(3) NOTICE TO CONGRESS.—The Secretary shall notify Congress when an initial list of high-risk covered assets is developed under paragraph (1) and each time the list is updated under paragraph (2).

(4) USE.—The list developed and updated under this subsection may be used by the Department to prioritize resource allocation to high-risk covered assets to bolster cyber resilience.

SEC. 8. REPORTS.

(a) REPORT ON ASSISTANCE PROVIDED TO ENTITIES OF HEALTHCARE AND PUBLIC HEALTH SECTOR.—Not later than 120 days after the date of enactment of this Act, the Agency shall submit to Congress a report on the organization-wide level of support and activities that the Agency has provided to the healthcare and public health sector to proactively prepare the sector to face cyber threats and respond to cyber attacks when such threats or attacks occur.

(b) REPORT ON CRITICAL INFRASTRUCTURE RESOURCES.—Not later than 18 months after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on Federal resources available, as of the date of enactment of this Act, for the Healthcare and Public Health Sector relating to critical infrastructure, as defined in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C.

5195c(e)), including resources available from recent and ongoing collaboration with the Director and the Secretary.

SEC. 9. RULES OF CONSTRUCTION.

(a) AGENCY ACTIONS.—Nothing in this Act shall be construed to authorize the Secretary or Director to take an action that is not authorized by this Act or existing law.

(b) PROTECTION OF RIGHTS.—Nothing in this Act shall be construed to permit the violation of the rights of any individual protected by the Constitution of the United States, including through censorship of speech protected by the Constitution of the United States or unauthorized surveillance.

(c) NO ADDITIONAL FUNDS.—No additional funds are authorized to be appropriated for the purpose of carrying out this Act.

Calendar No. 683

118TH CONGRESS
2D SESSION

S. 4697

[Report No. 118–280]

A BILL

To enhance the cybersecurity of the Healthcare and Public Health Sector.

DECEMBER 9, 2024

Reported with an amendment