

118TH CONGRESS
2D SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

Ms. ROSEN (for herself and Mr. YOUNG) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Healthcare Cybersecu-
5 rity Act of 2024”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act—

8 (1) the term “Agency” means the Cybersecurity
9 and Infrastructure Security Agency;

1 (2) the term “covered asset” means a
2 Healthcare and Public Health Sector asset, includ-
3 ing technologies, services, and utilities;

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

8 (4) the term “Department” means the Depart-
9 ment of Health and Human Services;

10 (5) the term “Director” means the Director of
11 the Agency;

12 (6) the term “Healthcare and Public Health
13 Sector” means the Healthcare and Public Health
14 sector, as identified in Presidential Policy Directive
15 21 (February 12, 2013; relating to critical infra-
16 structure security and resilience);

17 (7) the term “Information Sharing and Anal-
18 ysis Organizations” has the meaning given that term
19 in section 2200 of the Homeland Security Act of
20 2002 (6 U.S.C. 650);

21 (8) the term “Plan” means the Healthcare and
22 Public Health Sector Specific Plan; and

23 (9) the term “Secretary” means the Secretary
24 of Health and Human Services.

1 **SEC. 3. FINDINGS.**

2 Congress finds the following:

3 (1) Covered assets are increasingly the targets
4 of malicious cyberattacks, which result not only in
5 data breaches, but also increased healthcare delivery
6 costs, and can ultimately affect patient health out-
7 comes.

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

12 (3) According to data from the Office for Civil
13 Rights of the Department, health information
14 breaches have increased since 2016, and in 2022
15 alone, the Department reported 626 breaches on
16 covered entities, as defined under the Health Insur-
17 ance Portability and Accountability Act of 1996
18 (Public Law 104–191), affecting more than 500 peo-
19 ple, with nearly 42,000,000 total people affected by
20 health information breaches.

21 **SEC. 4. AGENCY COORDINATION WITH THE DEPARTMENT.**

22 (a) IN GENERAL.—The Agency shall coordinate with
23 the Department, including by entering into an agreement,
24 as appropriate, to improve cybersecurity in the Healthcare
25 and Public Health Sector.

26 (b) AGENCY LIAISON TO THE DEPARTMENT.—

1 (1) APPOINTMENT.—The Director shall, in co-
2 ordination with the Secretary, appoint an individual,
3 who shall be an employee of the Agency or a detailee
4 assigned to the Department by the Director, to serve
5 as the liaison of the Agency to the Department, who
6 shall—

7 (A) have appropriate cybersecurity quali-
8 fications and expertise; and

9 (B) report directly to the Director.

10 (2) RESPONSIBILITIES AND DUTIES.—The liai-
11 son appointed under paragraph (1) shall—

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

16 (B) serve as a primary contact of the De-
17 partment to coordinate cybersecurity issues
18 with the Agency;

19 (C) support the implementation and execu-
20 tion of the Plan and assist in the development
21 of updates to the Plan;

22 (D) facilitate the sharing of cyber threat
23 information to improve understanding of cyber-
24 security risks and situational awareness of cy-
25 bersecurity incidents;

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

3 (F) implement the training described in
4 section 5;

5 (G) coordinate between the Agency and the
6 Department during cybersecurity incidents
7 within the Healthcare and Public Health Sec-
8 tor; and

9 (H) perform such other duties as deter-
10 mined necessary by the Secretary to achieve the
11 goal of improving the cybersecurity of the
12 Healthcare and Public Health Sector.

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

20 (A) the Committee on Health, Education,
21 Labor, and Pensions, the Committee on Fi-
22 nance, and the Committee on Homeland Secu-
23 rity and Governmental Affairs of the Senate;
24 and

1 (B) the Committee on Energy and Com-
2 merce, the Committee on Ways and Means, and
3 the Committee on Homeland Security of the
4 House of Representatives.

5 (c) ASSISTANCE.—

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

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

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

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

21 **SEC. 5. TRAINING FOR HEALTHCARE EXPERTS.**

22 The Cyber Security Advisors and Cybersecurity State
23 Coordinators of the Agency shall, in coordination, as ap-
24 propriate, with the liaison appointed under section 4(b)(1)

1 and private sector healthcare experts, provide training to
2 the owners and operators of covered assets on—

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

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

7 **SEC. 6. SECTOR-SPECIFIC PLAN.**

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

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

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

18 (A) securing—

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

22 (ii) medical devices or equipment
23 owned, leased, or relied upon by covered
24 assets, which shall include an analysis of
25 the threat landscape and cybersecurity

1 vulnerabilities of such medical devices or
2 equipment; and

3 (iii) sensitive patient health informa-
4 tion and electronic health records;

5 (B) implementing cybersecurity protocols;

6 and

7 (C) responding to data breaches or cyber-
8 security attacks, including the impact on pa-
9 tient access to care, quality of patient care,
10 timeliness of health care delivery, and health
11 outcomes.

12 (3) An evaluation of best practices for the de-
13 ployment of trained Cyber Security Advisors and Cy-
14 bersecurity State Coordinators of the Agency into
15 covered assets before, during, and after data
16 breaches or cybersecurity attacks.

17 (4) An assessment of relevant Healthcare and
18 Public Health Sector cybersecurity workforce short-
19 ages, including—

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

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

1 (5) An evaluation of the most accessible and
2 timely ways for the Agency and the Department to
3 communicate and deploy cybersecurity recommenda-
4 tions and tools to the owners and operators of cov-
5 ered assets.

6 (b) CONGRESSIONAL BRIEFING.—Not later than 120
7 days after the date of enactment of this Act, the Sec-
8 retary, in consultation with the Director, shall provide a
9 briefing on the updating of the Plan under subsection (a)
10 to—

11 (1) the Committee on Health, Education,
12 Labor, and Pensions, the Committee on Finance,
13 and the Committee on Homeland Security and Gov-
14 ernmental Affairs of the Senate; and

15 (2) the Committee on Energy and Commerce,
16 the Committee on Ways and Means, and the Com-
17 mittee on Homeland Security of the House of Rep-
18 resentatives.

19 **SEC. 7. IDENTIFYING HIGH-RISK COVERED ASSETS.**

20 (a) IN GENERAL.—Not later than 90 days after the
21 date of enactment of this Act, the Director shall establish
22 objective criteria for determining whether a covered asset
23 should be designated as a high-risk covered asset.

24 (b) METHODOLOGY.—The Director, in consultation
25 with the Secretary, as appropriate, shall establish a meth-

1 odology for determining whether a covered asset meets the
2 criteria established under subsection (a) to be designated
3 as a high-risk covered asset.

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

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

10 (2) BIENNIAL UPDATING.—The Secretary
11 shall—

12 (A) biennially review and update the list
13 of high-risk covered assets developed under
14 paragraph (1); and

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

19 (3) NOTICE TO CONGRESS.—The Secretary
20 shall notify Congress when the initial list of high-
21 risk covered assets is developed under paragraph (1)
22 and each time the list is updated under paragraph
23 (2).

24 (4) USE.—The list developed and updated
25 under this subsection shall be used by the Depart-

1 ment to prioritize resource allocation to high-risk
2 covered assets to bolster cyber resilience.

3 **SEC. 8. REPORT ON ASSISTANCE PROVIDED TO ENTITIES**
4 **OF HEALTHCARE AND PUBLIC HEALTH SEC-**
5 **TOR.**

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