

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

Mr. CROW introduced the following bill; which was 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 2025”.

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 the National Security Memo-
15 randum on Critical Infrastructure and Resilience
16 (NSM-22), issued April 30, 2024;

17 (7) the term “Information Sharing and Anal-
18 ysis Organizations” has the meaning given the 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 Risk Management
23 Plan; and

24 (9) the term “Secretary” means the Secretary
25 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 and 2022.

12 (3) According to the “Annual Report to Con-
13 gress on Breaches of Unsecured Protected Health
14 Information for Calendar Year 2022” issued by the
15 Office for Civil Rights of the Department, breaches
16 of unsecured protected health information have in-
17 creased 107 percent since 2018, and, in 2022 alone,
18 the Department received 626 reported breaches af-
19 fecting not fewer than 500 individuals at covered en-
20 tities or business associates (as defined in section
21 160.103 of title 45, Code of Federal Regulations)
22 that occurred or ended in 2022, with nearly
23 42,000,000 individuals affected.

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

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

5 (b) AGENCY LIAISON TO THE DEPARTMENT.—

6 (1) APPOINTMENT.—The Director shall, in co-
7 ordination with the Secretary, appoint an individual,
8 who shall be an employee of the Agency or a detailee
9 assigned to the Administration for Strategic Pre-
10 paredness and Response Office of the Department
11 by the Director, to serve as a liaison of the Agency
12 to the Department, who shall—

13 (A) have appropriate cybersecurity quali-
14 fications and expertise; and

15 (B) report directly to the Director.

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

18 (A) serve as a primary contact of the De-
19 partment to coordinate cybersecurity issues
20 with the Agency;

21 (B) support the implementation and execu-
22 tion of the Plan and assist in the development
23 of updates to the Plan;

24 (C) facilitate the sharing of cyber threat
25 information between the Department and the
26 Agency to improve understanding of cybersecu-

1 rity risks and situational awareness of cyberse-
2 curity incidents;

3 (D) assist in implementing the training de-
4 scribed in section 5;

5 (E) facilitate coordination between the
6 Agency and the Department during cybersecu-
7 rity incidents within the Healthcare and Public
8 Health Sector; and

9 (F) 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.—

14 (A) REQUIREMENT.—Not later than 18
15 months after the date of enactment of this Act,
16 the Secretary, in coordination with the Direc-
17 tor, shall submit a report that describes the ac-
18 tivities undertaken to improve cybersecurity co-
19 ordination between the Agency and the Depart-
20 ment to—

21 (i) the Committee on Health, Edu-
22 cation, Labor, and Pensions, the Com-
23 mittee on Finance, and the Committee on
24 Homeland Security and Governmental Af-
25 fairs of the Senate; and

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

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

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

9 (ii) a description of any challenges to
10 the effectiveness of the liaison appointed
11 under paragraph (1) completing the re-
12 quired duties of the liaison; and

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

16 (c) RESOURCES.—

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

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

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

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

7 **SEC. 5. TRAINING FOR HEALTHCARE OWNERS AND OPERA-**
8 **TORS.**

9 The Agency shall make available training to the own-
10 ers and operators of covered assets on—

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

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

15 **SEC. 6. SECTOR-SPECIFIC RISK MANAGEMENT PLAN.**

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

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

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

1 (A) securing—

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

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

11 (iii) sensitive patient health informa-
12 tion and electronic health records;

13 (B) implementing cybersecurity protocols;
14 and

15 (C) responding to data breaches or cyber-
16 security attacks, including the impact on pa-
17 tient access to care, quality of patient care,
18 timeliness of health care delivery, and health
19 outcomes.

20 (3) An evaluation of the best practices for utili-
21 zation of resources from the Agency to support cov-
22 ered assets before, during, and after data breaches
23 or cybersecurity attacks, such as by Cyber Security
24 Advisors and Cybersecurity State Coordinators of
25 the Agency or other similar resources.

1 (4) An assessment of relevant Healthcare and
2 Public Health Sector cybersecurity workforce short-
3 ages, including—

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

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

9 (5) An evaluation of the most accessible and
10 timely ways for the Agency and the Department to
11 communicate and deploy cybersecurity recommenda-
12 tions and tools to the owners and operators of cov-
13 ered assets.

14 (b) CONGRESSIONAL BRIEFING.—Not later than 120
15 days after the date of enactment of this Act, the Sec-
16 retary, in consultation with the Director, shall provide a
17 briefing on the updating of the Plan under subsection (a)
18 to—

19 (1) the Committee on Health, Education,
20 Labor, and Pensions, the Committee on Finance,
21 and the Committee on Homeland Security and Gov-
22 ernmental Affairs of the Senate; and

23 (2) the Committee on Energy and Commerce,
24 the Committee on Ways and Means, and the Com-

1 mittee on Homeland Security of the House of Rep-
2 resentatives.

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

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

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

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

20 (2) BIENNIAL UPDATING.—The Secretary
21 may—

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

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

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

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

13 **SEC. 8. REPORTS.**

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

23 (b) REPORT ON CRITICAL INFRASTRUCTURE RE-
24 SOURCES.—Not later than 18 months after the date of
25 enactment of this Act, the Comptroller General of the

1 United States shall submit to Congress a report on Fed-
2 eral resources available, as of the date of enactment of
3 this Act, for the Healthcare and Public Health Sector re-
4 lating to critical infrastructure, as defined in section
5 1016(e) of the Critical Infrastructures Protection Act of
6 2001 (42 U.S.C. 5195c(e)), including resources available
7 from recent and ongoing collaboration with the Director
8 and the Secretary.

9 **SEC. 9. RULES OF CONSTRUCTION.**

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

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

20 (c) NO ADDITIONAL FUNDS.—No additional funds
21 are authorized to be appropriated for the purpose of car-
22 rying out this Act.