

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.

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”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act—

3 (1) the term “Agency” means the Cybersecurity
4 and Infrastructure Security Agency;

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

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

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

14 (5) the term “Director” means the Director of
15 the Agency;

16 (6) the term “Healthcare and Public Health
17 Sector” means the Healthcare and Public Health
18 sector, as identified in Presidential Policy Directive
19 21 (February 12, 2013; relating to critical infra-
20 structure security and resilience);

21 (7) the term “Information Sharing and Anal-
22 ysis Organizations” has the meaning given that term
23 in section 2200 of the Homeland Security Act of
24 2002 (6 U.S.C. 650);

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

1 (9) the term “Secretary” means the Secretary
2 of Health and Human Services.

3 **SEC. 3. FINDINGS.**

4 Congress finds the following:

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

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

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

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

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

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

3 (b) AGENCY LIAISON TO THE DEPARTMENT.—

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

10 (A) have appropriate cybersecurity quali-
11 fications and expertise; and

12 (B) report directly to the Director.

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

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

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

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

1 (D) facilitate the sharing of cyber threat
2 information to improve understanding of cyber-
3 security risks and situational awareness of cy-
4 bersecurity incidents;

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

7 (F) implement the training described in
8 section 5;

9 (G) coordinate between the Agency and the
10 Department during cybersecurity incidents
11 within the Healthcare and Public Health Sec-
12 tor; and

13 (H) perform such other duties as deter-
14 mined necessary by the Secretary to achieve the
15 goal of improving the cybersecurity of the
16 Healthcare and Public Health Sector.

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

24 (A) the Committee on Health, Education,
25 Labor, and Pensions; the Committee on Fi-

1 nance, and the Committee on Homeland Secu-
2 rity and Governmental Affairs of the Senate;
3 and

4 ~~(B)~~ the Committee on Energy and Com-
5 merce, the Committee on Ways and Means, and
6 the Committee on Homeland Security of the
7 House of Representatives.

8 ~~(c)~~ ASSISTANCE.—

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

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

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

21 ~~(B)~~ sharing information relating to cyber
22 threat indicators and appropriate defensive
23 measures.

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

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

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

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

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

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

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

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

22 (A) securing—

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

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

7 (iii) sensitive patient health informa-
8 tion and electronic health records;

9 (B) implementing cybersecurity protocols;
10 and

11 (C) responding to data breaches or cyber-
12 security attacks, including the impact on pa-
13 tient access to care, quality of patient care,
14 timeliness of health care delivery, and health
15 outcomes.

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

21 (4) An assessment of relevant Healthcare and
22 Public Health Sector cybersecurity workforce short-
23 ages, including—

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

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

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

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

14 ~~(1)~~ the Committee on Health, Education,
15 Labor, and Pensions, the Committee on Finance,
16 and the Committee on Homeland Security and Gov-
17 ernmental Affairs of the Senate; and

18 ~~(2)~~ the Committee on Energy and Commerce,
19 the Committee on Ways and Means, and the Com-
20 mittee on Homeland Security of the House of Rep-
21 resentatives.

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

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

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

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

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

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

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

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

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

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

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

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

7 **SEC. 8. REPORT ON ASSISTANCE PROVIDED TO ENTITIES**
8 **OF HEALTHCARE AND PUBLIC HEALTH SEC-**
9 **TOR.**

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

17 **SECTION 1. SHORT TITLE.**

18 *This Act may be cited as the “Healthcare Cybersecu-*
19 *rity Act of 2024”.*

20 **SEC. 2. DEFINITIONS.**

21 *In this Act—*

22 (1) *the term “Agency” means the Cybersecurity*
23 *and Infrastructure Security Agency;*

1 (2) *the term “covered asset” means a Healthcare*
2 *and Public Health Sector asset, including tech-*
3 *nologies, 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 the*
11 *Agency;*

12 (6) *the term “Healthcare and Public Health Sec-*
13 *tor” means the Healthcare and Public Health sector,*
14 *as identified in the National Security Memorandum*
15 *on Critical Infrastructure and Resilience (NSM-22),*
16 *issued April 30, 2024;*

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

21 (8) *the term “Plan” means the Healthcare and*
22 *Public Health Sector-specific Risk Management Plan;*
23 *and*

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

1 **SEC. 3. FINDINGS.**

2 *Congress finds the following:*

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

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

11 (3) *According to the “Annual Report to Congress*
12 *on Breaches of Unsecured Protected Health Informa-*
13 *tion for Calendar Year 2022” issued by the Office for*
14 *Civil Rights of the Department, breaches of unsecured*
15 *protected health information have increased 107 per-*
16 *cent since 2018, and, in 2022 alone, the Department*
17 *received 626 reported breaches affecting not less than*
18 *500 individuals at covered entities or business associ-*
19 *ates (as defined in section 160.103 of title 45, Code*
20 *of Federal Regulations) that occurred or ended in*
21 *2022, with nearly 42,000,000 individuals affected.*

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

23 (a) *IN GENERAL.—The Agency shall coordinate with*
24 *the Department 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 Administration for Strategic Pre-*
5 *paredness and Response Office of the Department by*
6 *the Director, to serve as a liaison of the Agency to the*
7 *Department, who shall—*

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

10 (B) *report directly to the Director.*

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

13 (A) *serve as a primary contact of the De-*
14 *partment to coordinate cybersecurity issues with*
15 *the Agency;*

16 (B) *support the implementation and execu-*
17 *tion of the Plan and assist in the development of*
18 *updates to the Plan;*

19 (C) *facilitate the sharing of cyber threat in-*
20 *formation between the Department and the Agen-*
21 *cy to improve understanding of cybersecurity*
22 *risks and situational awareness of cybersecurity*
23 *incidents;*

24 (D) *assist in implementing the training de-*
25 *scribed in section 5;*

1 (E) *facilitate coordination between the*
2 *Agency and the Department during cybersecurity*
3 *incidents within the Healthcare and Public*
4 *Health Sector; and*

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

9 (3) *REPORT.—*

10 (A) *REQUIREMENT.—Not later than 18*
11 *months after the date of enactment of this Act,*
12 *the Secretary, in coordination with the Director,*
13 *shall submit a report that describes the activities*
14 *undertaken to improve cybersecurity coordina-*
15 *tion between the Agency and the Department*
16 *to—*

17 (i) *the Committee on Health, Edu-*
18 *cation, Labor, and Pensions, the Committee*
19 *on Finance, and the Committee on Home-*
20 *land Security and Governmental Affairs of*
21 *the Senate; and*

22 (ii) *the Committee on Energy and*
23 *Commerce, the Committee on Ways and*
24 *Means, and the Committee on Homeland*
25 *Security of the House of Representatives.*

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

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

5 (ii) *a description of any challenges to*
6 *the effectiveness of the liaison appointed*
7 *under paragraph (1) completing the re-*
8 *quired duties of the liaison; and*

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

12 (c) *RESOURCES.*—

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

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

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

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

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

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

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

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

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

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

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

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

23 (A) securing—

1 (i) updated information systems
2 owned, leased, or relied upon by covered as-
3 sets;

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

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

12 (B) implementing cybersecurity protocols;

13 and

14 (C) responding to data breaches or cyberse-
15 curity attacks, including the impact on patient
16 access to care, quality of patient care, timeliness
17 of health care delivery, and health outcomes.

18 (3) An evaluation of the best practices for utili-
19 zation of resources from the Agency to support covered
20 assets before, during, and after data breaches or cy-
21 bersecurity attacks, such as by Cyber Security Advi-
22 sors and Cybersecurity State Coordinators of the
23 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 covered*
13 *assets.*

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

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

22 (2) *the Committee on Energy and Commerce, the*
23 *Committee on Ways and Means, and the Committee*
24 *on Homeland Security of the House of Representa-*
25 *tives.*

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

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

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

13 (1) *IN GENERAL.*—*The Secretary may develop a*
14 *list of, and notify, the owners and operators of each*
15 *covered asset determined to be a high-risk covered*
16 *asset using the methodology promulgated by the Di-*
17 *rector pursuant to subsection (a).*

18 (2) *BIANNUAL UPDATING.*—*The Secretary may—*

19 (A) *biannually review and update the list of*
20 *high-risk covered assets developed under para-*
21 *graph (1); and*

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

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

5 (4) *USE.*—*The list developed and updated under*
6 *this subsection may be used by the Department to*
7 *prioritize resource allocation to high-risk covered as-*
8 *sets to bolster cyber resilience.*

9 **SEC. 8. REPORTS.**

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

18 (b) *REPORT ON CRITICAL INFRASTRUCTURE RE-*
19 *SOURCES.*—*Not later than 18 months after the date of en-*
20 *actment of this Act, the Comptroller General of the United*
21 *States shall submit to Congress a report on Federal re-*
22 *sources available, as of the date of enactment of this Act,*
23 *for the Healthcare and Public Health Sector relating to*
24 *critical infrastructure, as defined in section 1016(e) of the*
25 *Critical Infrastructures Protection Act of 2001 (42 U.S.C.*

1 5195c(e)), including resources available from recent and on-
2 going collaboration with the Director and the Secretary.

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

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

7 (b) *PROTECTION OF RIGHTS.*—Nothing in this Act
8 shall be construed to permit the violation of the rights of
9 any individual protected by the Constitution of the United
10 States, including through censorship of speech protected by
11 the Constitution of the United States or unauthorized sur-
12 veillance.

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

Calendar No. 683

118TH CONGRESS
2^D 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