

Calendar No. 527

117TH CONGRESS
2D SESSION

S. 3904

[Report No. 117-177]

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

IN THE SENATE OF THE UNITED STATES

MARCH 23, 2022

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

OCTOBER 18, 2022

Reported under authority of the order of the Senate of October 14, 2022, by Mr. PETERS, with an amendment and an amendment to the title
[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 2022”.

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 “Cybersecurity State Coordinator”
6 means a Cybersecurity State Coordinator appointed
7 under section 2217(a) of the Homeland Security Act
8 of 2002 (6 U.S.C. 665e(a));

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

11 (4) the term “Director” means the Director of
12 the Agency;

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

18 (6) the term “Information Sharing and Anal-
19 ysis Organizations” has the meaning given that term
20 in section 2222 of the Homeland Security Act of
21 2002 (6 U.S.C. 671); and

22 (7) the term “Secretary” means the Secretary
23 of Health and Human Services.

24 **SEC. 3. FINDINGS.**

25 Congress finds the following:

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

6 (2) Data reported to the Department shows
7 that almost every month in 2020, more than
8 1,000,000 people were affected by data breaches at
9 healthcare organizations. Cyberattacks on healthcare
10 facilities rose 55 percent in 2020, and these attacks
11 also resulted in a 16 percent increase in the average
12 cost of recovering a patient record in 2020, as com-
13 pared to 2019.

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 2020
17 alone, the Department reported 663 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 over 33,000,000 total people affected by
22 health information breaches.

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

24 (a) **IN GENERAL.**—The Agency shall collaborate 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) ASSISTANCE.—

4 (1) IN GENERAL.—The Agency shall coordinate
5 with and make resources available to Information
6 Sharing and Analysis Organizations, information
7 sharing and analysis centers, and non-Federal enti-
8 ties that are receiving information shared through
9 programs managed by the Department.

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

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

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

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

19 The Cyber Security Advisors and Cybersecurity State
20 Coordinators of the Agency shall, in coordination, as ap-
21 propriate, with private sector healthcare experts, provide
22 training to Healthcare and Public Health Sector asset
23 owners and operators on—

1 (1) cybersecurity risks to the Healthcare and
2 Public Health Sector and assets within the sector;
3 and

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

6 **SEC. 6. SECTOR-SPECIFIC STUDY AND REPORT.**

7 (a) IN GENERAL.—Not later than 1 year after the
8 date of enactment of this Act, the Director, in consultation
9 with the Secretary, shall conduct a study and issue a re-
10 port, which shall include the following elements:

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

16 (2) An evaluation of the challenges Healthcare
17 and Public Health Sector assets face in—

18 (A) securing—

19 (i) updated information systems
20 owned, leased, or relied upon by
21 Healthcare and Public Health Sector as-
22 sets;

23 (ii) medical devices or equipment
24 owned, leased, or relied upon by
25 Healthcare and Public Health Sector as-

1 sets, which shall include an analysis of the
2 threat landscape and cybersecurity
3 vulnerabilities of such medical devices or
4 equipment; and

5 (iii) sensitive patient health informa-
6 tion and electronic health records;

7 (B) implementing cybersecurity protocols;

8 and

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

14 (3) An evaluation of best practices for the de-
15 ployment of trained Cyber Security Advisors and Cy-
16 bersecurity State Coordinators of the Agency into
17 Healthcare and Public Health Sector assets before,
18 during, and after data breaches or cybersecurity at-
19 tacks.

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

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

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

5 ~~(5)~~ An identification of cybersecurity challenges
6 related to or brought on by the public health emer-
7 gency declared by the Secretary under section 319
8 of the Public Health Service Act (42 U.S.C. 247d)
9 on January 27, 2020, with respect to COVID-19.

10 ~~(6)~~ An evaluation of the most accessible and
11 timely ways for the Agency and the Department to
12 communicate and deploy cybersecurity recommenda-
13 tions and tools to Healthcare and Public Health Sec-
14 tor assets.

15 ~~(b) REPORT TRANSMITTAL.~~—Not later than 60 days
16 after completing the study and report required under sub-
17 section (a), the Director shall present the completed report
18 to the Secretary, which the Secretary may, in consultation
19 with the Director, consult when updating the Healthcare
20 and Public Health Sector Specific Plan of the Secretary.

21 ~~(c) CONGRESSIONAL BRIEFING.~~—Not later than 120
22 days after the date of enactment of this Act, the Director,
23 in consultation with the Secretary, as appropriate, shall
24 provide a briefing on the status of the study and report
25 required under subsection (a) to—

1 (1) the Committee on Health, Education,
2 Labor, and Pensions and the Committee on Home-
3 land Security and Governmental Affairs of the Sen-
4 ate; and

5 (2) the Committee on Energy and Commerce
6 and the Committee on Homeland Security of the
7 House of Representatives.

8 **SECTION 1. SHORT TITLE.**

9 *This Act may be cited as the “Healthcare Cybersecu-*
10 *riety Act of 2022”.*

11 **SEC. 2. DEFINITIONS.**

12 *In this Act—*

13 (1) the term “Agency” means the Cybersecurity
14 and Infrastructure Security Agency;

15 (2) the term “Cybersecurity State Coordinator”
16 means a Cybersecurity State Coordinator appointed
17 under section 2217(a) of the Homeland Security Act
18 of 2002 (6 U.S.C. 665c(a));

19 (3) the term “Department” means the Depart-
20 ment of Health and Human Services;

21 (4) the term “Director” means the Director of the
22 Agency;

23 (5) the term “Healthcare and Public Health Sec-
24 tor” means the Healthcare and Public Health sector,
25 as identified in Presidential Policy Directive 21 (Feb-

1 *ruary 12, 2013; relating to critical infrastructure se-*
2 *curity and resilience);*

3 *(6) the term “Information Sharing and Analysis*
4 *Organizations” has the meaning given that term in*
5 *section 2222 of the Homeland Security Act of 2002 (6*
6 *U.S.C. 671); and*

7 *(7) the term “Secretary” means the Secretary of*
8 *Health and Human Services.*

9 **SEC. 3. FINDINGS.**

10 *Congress finds the following:*

11 *(1) Healthcare and Public Health Sector assets*
12 *are increasingly the targets of malicious cyberattacks,*
13 *which result not only in data breaches, but also in-*
14 *creased healthcare delivery costs, and can ultimately*
15 *affect patient health outcomes.*

16 *(2) Data reported to the Department shows that*
17 *almost every month in 2020, more than 1,000,000*
18 *people were affected by data breaches at healthcare or-*
19 *ganizations. Cyberattacks on healthcare facilities rose*
20 *55 percent in 2020, and these attacks also resulted in*
21 *a 16 percent increase in the average cost of recovering*
22 *a patient record in 2020, as compared to 2019.*

23 *(3) According to data from the Office for Civil*
24 *Rights of the Department, health information*
25 *breaches have increased since 2016, and in 2020*

1 *alone, the Department reported 663 breaches on cov-*
2 *ered entities, as defined under the Health Insurance*
3 *Portability and Accountability Act of 1996 (Public*
4 *Law 104–191), affecting more than 500 people, with*
5 *over 33,000,000 total people affected by health infor-*
6 *mation breaches.*

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

8 *(a) IN GENERAL.—The Agency and the Department*
9 *shall coordinate, including by entering into an agreement,*
10 *as appropriate, to improve cybersecurity in the Healthcare*
11 *and Public Health Sector.*

12 *(b) ASSISTANCE.—*

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, and non-Federal enti-*
17 *ties that are receiving information shared through*
18 *programs managed by the Department.*

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

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

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

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

5 The Secretary, in coordination with the Cyber Secu-
6 rity Advisors and Cybersecurity State Coordinators of the
7 Agency and private sector healthcare experts, as appro-
8 priate, shall provide training to Healthcare and Public
9 Health Sector asset owners and operators on—

10 (1) cybersecurity risks to the Healthcare and
11 Public Health Sector and assets within the sector; and

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

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

15 (a) *IN GENERAL.*—Not later than 1 year after the date
16 of enactment of this Act, the Secretary, in coordination with
17 the Director, shall update the Healthcare and Public Health
18 Sector Specific Plan (referred to in this section as the
19 “Plan”), which shall include the following elements:

20 (1) An analysis of how identified cybersecurity
21 risks specifically impact Healthcare and Public
22 Health Sector assets, including the impact on rural
23 and small and medium-sized Healthcare and Public
24 Health Sector assets.

1 (2) *An evaluation of the challenges Healthcare*
2 *and Public Health Sector assets face in—*

3 (A) *securing—*

4 (i) *updated information systems*
5 *owned, leased, or relied upon by Healthcare*
6 *and Public Health Sector assets;*

7 (ii) *medical devices or equipment*
8 *owned, leased, or relied upon by Healthcare*
9 *and Public Health Sector assets, which shall*
10 *include an analysis of the threat landscape*
11 *and cybersecurity vulnerabilities of such*
12 *medical devices or equipment; and*

13 (iii) *sensitive patient health informa-*
14 *tion and electronic health records;*

15 (B) *implementing cybersecurity protocols;*

16 *and*

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

21 (3) *An evaluation of best practices for the de-*
22 *ployment of trained Cyber Security Advisors and Cy-*
23 *bersecurity State Coordinators of the Agency into*
24 *Healthcare and Public Health Sector assets before,*

1 *during, and after data breaches or cybersecurity at-*
2 *tacks.*

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

6 (A) *training, recruitment, and retention*
7 *issues; and*

8 (B) *recommendations for how to address*
9 *these shortages and issues, particularly at rural*
10 *and small and medium-sized Healthcare and*
11 *Public Health Sector assets.*

12 (5) *An identification of cybersecurity challenges*
13 *related to or brought on by the public health emer-*
14 *gency declared by the Secretary under section 319 of*
15 *the Public Health Service Act (42 U.S.C. 247d) on*
16 *January 27, 2020, with respect to COVID–19.*

17 (6) *An evaluation of the most accessible and*
18 *timely ways for the Agency and the Department to*
19 *communicate and deploy cybersecurity recommenda-*
20 *tions and tools to Healthcare and Public Health Sec-*
21 *tor assets.*

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

1 (1) *the Committee on Health, Education, Labor,*
2 *and Pensions and the Committee on Homeland Secu-*
3 *urity and Governmental Affairs of the Senate; and*

4 (2) *the Committee on Energy and Commerce and*
5 *the Committee on Homeland Security of the House of*
6 *Representatives.*

Amend the title so as to read: “A bill to enhance the cybersecurity of the Healthcare and Public Health Sector and update the Healthcare and Public Health Sector Specific Plan.”.

Calendar No. 527

117TH CONGRESS
2^D SESSION

S. 3904

[Report No. 117-177]

A BILL

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

OCTOBER 18, 2022

Reported under authority of the order of the Senate of
October 14, 2022, with an amendment and an amend-
ment to the title