

117TH CONGRESS
2D SESSION

S. 3904

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 and Mr. CASSIDY) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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”.

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

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

7 (4) the term “Director” means the Director of
8 the Agency;

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

14 (6) the term “Information Sharing and Anal-
15 ysis Organizations” has the meaning given that term
16 in section 2222 of the Homeland Security Act of
17 2002 (6 U.S.C. 671); and

18 (7) the term “Secretary” means the Secretary
19 of Health and Human Services.

20 **SEC. 3. FINDINGS.**

21 Congress finds the following:

22 (1) Healthcare and Public Health Sector assets
23 are increasingly the targets of malicious
24 cyberattacks, which result not only in data breaches,

1 but also increased healthcare delivery costs, and can
2 ultimately affect patient health outcomes.

3 (2) Data reported to the Department shows
4 that almost every month in 2020, more than
5 1,000,000 people were affected by data breaches at
6 healthcare organizations. Cyberattacks on healthcare
7 facilities rose 55 percent in 2020, and these attacks
8 also resulted in a 16 percent increase in the average
9 cost of recovering a patient record in 2020, as com-
10 pared to 2019.

11 (3) According to data from the Office for Civil
12 Rights of the Department, health information
13 breaches have increased since 2016, and in 2020
14 alone, the Department reported 663 breaches on
15 covered entities, as defined under the Health Insur-
16 ance Portability and Accountability Act of 1996
17 (Public Law 104–191), affecting more than 500 peo-
18 ple, with over 33,000,000 total people affected by
19 health information breaches.

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

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

25 (b) ASSISTANCE.—

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

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

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

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

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

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

21 (1) cybersecurity risks to the Healthcare and
22 Public Health Sector and assets within the sector;
23 and

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

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

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

6 (1) An analysis of how identified cybersecurity
7 risks specifically impact Healthcare and Public
8 Health Sector assets, including the impact on rural
9 and small and medium-sized Healthcare and Public
10 Health Sector assets.

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

13 (A) securing—

14 (i) updated information systems
15 owned, leased, or relied upon by
16 Healthcare and Public Health Sector as-
17 sets;

18 (ii) medical devices or equipment
19 owned, leased, or relied upon by
20 Healthcare and Public Health Sector as-
21 sets, which shall include an analysis of the
22 threat landscape and cybersecurity
23 vulnerabilities of such medical devices or
24 equipment; and

25 (iii) sensitive patient health informa-
26 tion and electronic health records;

1 (B) implementing cybersecurity protocols;
2 and

3 (C) responding to data breaches or cyber-
4 security attacks, including the impact on pa-
5 tient access to care, quality of patient care,
6 timeliness of health care delivery, and health
7 outcomes.

8 (3) An evaluation of best practices for the de-
9 ployment of trained Cyber Security Advisors and Cy-
10 bersecurity State Coordinators of the Agency into
11 Healthcare and Public Health Sector assets before,
12 during, and after data breaches or cybersecurity at-
13 tacks.

14 (4) An assessment of relevant Healthcare and
15 Public Health Sector cybersecurity workforce short-
16 ages, including—

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

19 (B) recommendations for how to address
20 these shortages and issues, particularly at rural
21 and small and medium-sized Healthcare and
22 Public Health Sector assets.

23 (5) An identification of cybersecurity challenges
24 related to or brought on by the public health emer-
25 gency declared by the Secretary under section 319

1 of the Public Health Service Act (42 U.S.C. 247d)
2 on January 27, 2020, with respect to COVID–19.

3 (6) An evaluation of the most accessible and
4 timely ways for the Agency and the Department to
5 communicate and deploy cybersecurity recommenda-
6 tions and tools to Healthcare and Public Health Sec-
7 tor assets.

8 (b) REPORT TRANSMITTAL.—Not later than 60 days
9 after completing the study and report required under sub-
10 section (a), the Director shall present the completed report
11 to the Secretary, which the Secretary may, in consultation
12 with the Director, consult when updating the Healthcare
13 and Public Health Sector Specific Plan of the Secretary.

14 (c) CONGRESSIONAL BRIEFING.—Not later than 120
15 days after the date of enactment of this Act, the Director,
16 in consultation with the Secretary, as appropriate, shall
17 provide a briefing on the status of the study and report
18 required under subsection (a) to—

19 (1) the Committee on Health, Education,
20 Labor, and Pensions and the Committee on Home-
21 land Security and Governmental Affairs of the Sen-
22 ate; and

1 (2) the Committee on Energy and Commerce
2 and the Committee on Homeland Security of the
3 House of Representatives.

○