AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—117th Cong., 2d Sess.

S. 3904

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Ms. ROSEN

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Healthcare Cybersecurity Act of 2022''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Agency'' means the Cybersecurity and Infrastructure Security Agency;

(2) the term ''Cybersecurity State Coordinator'' means a Cybersecurity State Coordinator appointed

under section 2217(a) of the Homeland Security Act of 2002 (6 U.S.C. 665c(a));

(3) the term ''Department'' means the Department of Health and Human Services;

(4) the term ''Director'' means the Director of the Agency;

(5) the term ''Healthcare and Public Health Sector'' means the Healthcare and Public Health sector, as identified in Presidential Policy Directive 21 (February 12, 2013; relating to critical infrastructure security and resilience);

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

(7) the term ''Secretary'' means the Secretary of Health and Human Services.

SEC. 3. FINDINGS.

Congress finds the following:

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

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

(3) According to data from the Office for Civil Rights of the Department, health information breaches have increased since 2016, and in 2020 alone, the Department reported 663 breaches on covered entities, as defined under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191), affecting more than 500 people, with over 33,000,000 total people affected by health information breaches.

SEC. 4. AGENCY COORDINATION WITH THE DEPARTMENT.

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

(b) ASSISTANCE.—

(1) IN GENERAL.—The Agency shall coordinate with and make resources available to Information

Sharing and Analysis Organizations, information sharing and analysis centers, and non-Federal entities that are receiving information shared through programs managed by the Department.

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

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

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

SEC. 5. TRAINING FOR HEALTHCARE EXPERTS.

The Secretary, in coordination with the Cyber Security Advisors and Cybersecurity State Coordinators of the Agency and private sector healthcare experts, as appropriate, shall provide training to Healthcare and Public Health Sector asset owners and operators on—

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

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

SEC. 6. SECTOR-SPECIFIC PLAN.

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

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

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

(A) securing—

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

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

(iii) sensitive patient health information and electronic health records;

(B) implementing cybersecurity protocols; and

(C) responding to data breaches or cybersecurity attacks, including the impact on patient access to care, quality of patient care, timeliness of health care delivery, and health outcomes.

(3) An evaluation of best practices for the deployment of trained Cyber Security Advisors and Cybersecurity State Coordinators of the Agency into Healthcare and Public Health Sector assets before, during, and after data breaches or cybersecurity attacks.

(4) An assessment of relevant Healthcare and Public Health Sector cybersecurity workforce shortages, including—

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

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

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

(6) An evaluation of the most accessible and timely ways for the Agency and the Department to communicate and deploy cybersecurity recommendations and tools to Healthcare and Public Health Sector assets.

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

(1) the Committee on Health, Education, Labor, and Pensions and the Committee on Homeland Security and Governmental Affairs of the Senate; and

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