118TH CONGRESS
2D SESSION

S. 5390

To require the Secretary of Health and Human Services and the Director of the Cybersecurity and Infrastructure Security Agency to coordinate to improve cybersecurity in the health care and public health sectors, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 21, 2024

Mr. CASSIDY (for himself, Ms. HASSAN, Mr. CORNYN, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

---

A BILL

To require the Secretary of Health and Human Services and the Director of the Cybersecurity and Infrastructure Security Agency to coordinate to improve cybersecurity in the health care and public health sectors, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Health Care Cybersecurity and Resiliency Act of 2024''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''Agency'' means the Cybersecurity and Infrastructure Security Agency.

(2) CYBERSECURITY INCIDENT.—The term ''cybersecurity incident'' has the meaning given the term ''incident'' in section 3552 of title 44, United States Code.

(3) CYBERSECURITY STATE COORDINATOR.—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)).

(4) DIRECTOR.—The term ''Director'' means the Director of the Agency.

(5) HEALTHCARE AND PUBLIC HEALTH SECTOR.—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) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''Information Sharing and Analysis Organization'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(7) INFORMATION SYSTEM.—The term ''information system'' has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(8) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

SEC. 3. DEPARTMENT COORDINATION WITH THE AGENCY.

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

(b) ASSISTANCE.—

(1) IN GENERAL.—The Secretary shall coordinate with the Director to make resources available to entities that are receiving information shared through programs managed by the Director or the Secretary, including Information Sharing and Analysis Organizations, information sharing and analysis centers, and non-Federal entities.

(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. 4. CLARIFYING CYBERSECURITY RESPONSIBILITIES AT THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.

Part A of title III of the Public Health Service Act (42 U.S.C. 241 et seq.) is amended by adding at the end the following:

"SEC. 310C. OVERSIGHT OF CYBERSECURITY ACTIVITIES.

''The Secretary, acting through the Assistant Secretary for Preparedness and Response, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency pursuant to section 2218 of the Homeland Security Act of 2002, shall lead oversight and coordination of activities within the Department of Health and Human Services to support cybersecurity resiliency within the Healthcare and Public Health Sector (as defined in section 2 of the Health Care Cybersecurity and Resiliency Act of 2024), including coordination and communication with other public and private entities related to preparedness for, and responses to, cybersecurity incidents, consistent with applicable provisions of this Act, other applicable laws, and Presidential Policy Directive 21 (February

12, 2013; relating to critical infrastructure security and resilience).''.

SEC. 5. CYBERSECURITY INCIDENT RESPONSE PLAN.

Section 405 of the Cybersecurity Act of 2015 (6 U.S.C. 1533) is amended—

(1) in subsection (a)—

(A) in paragraph (4)—

(i) in the paragraph heading, by inserting ''INFORMATION SYSTEM;'' after ''FEDERAL ENTITY;''; and

(ii) by inserting '' 'information system','' after '' 'Federal entity','';

(B) by redesignating paragraphs (4) through (7) as paragraphs (6) through (9), respectively; and

(C) by inserting after paragraph (3) the following:

''(4) CYBERSECURITY INCIDENT.—The term 'cybersecurity incident' has the meaning given the term 'incident' in section 3552 of title 44, United States Code.

''(5) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).''; and

(2) in subsection (d), by adding at the end the following:

"(4) PLAN.—

"(A) IN GENERAL.—Not later than 1 year after the date of enactment of the Health Care Cybersecurity and Resiliency Act of 2024, the Secretary shall develop and implement a cybersecurity incident response plan to inform applicable personnel within the Department of Health and Human Services of processes and protocols to prepare for, and respond to, cybersecurity incidents involving information, including hardware, software, databases, and networks, maintained by, or on behalf of, the Department, including strategies—

"(i) to assess cybersecurity risks;

"(ii) to prevent cybersecurity incidents;

"(iii) to detect and identify cybersecurity incidents;

"(iv) to minimize damage in the event of a cybersecurity incident;

"(v) to protect data; and

"(vi) to recover from any cybersecurity incidents expeditiously.

"(B) CONSULTATION.—In developing the plan under subparagraph (A), the Secretary shall consult with the Director of the Cybersecurity and Infrastructure Security Agency, the Director of the Office of Management and Budget, and the Director of the National Institute of Standards and Technology, and relevant experts, as appropriate.

"(C) REPORT.—Not later than 60 days before the date on which the Secretary begins implementing the plan under subparagraph (A), the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Energy and Commerce, the Committee on Oversight and Reform, and the Committee on Homeland Security of the House of Representatives a report that describes such plan.".

SEC. 6. BREACH REPORTING PORTAL.

(a) UPDATES TO BREACH REPORTING PORTAL.—Section 13402 of the HITECH Act (42 U.S.C. 17932) is amended by adding at the end the following:

''(k) UPDATES TO REGULATIONS.—Not later than 1 year after the date of enactment of the Health Care Cybersecurity and Resiliency Act of 2024, the Secretary shall update the regulations promulgated pursuant to subsection (j) to require that information required to be publicly displayed in the breach reporting portal established pursuant to this section includes—

''(1) information on any corrective action taken against a covered entity that provided notification of a breach under this section;

''(2) information on whether and to what extent, as appropriate, recognized security practices (as defined in section 13412(b)(1)) were considered in the investigation of such a breach; and

''(3) such additional information about such a breach as the Secretary may require.''.

SEC. 7. CLARIFYING BREACH REPORTING OBLIGATIONS.

Section 13402(f) of the HITECH Act (42 U.S.C. 17932(f)) is amended by adding at the end the following:

''(6) The number of individuals affected by the breach.''.

SEC. 8. ENHANCING RECOGNITION OF SECURITY PRACTICES.

(a) RECOGNIZED SECURITY PRACTICES.—Section 13412(b)(1) of the HITECH Act (42 U.S.C. 17941(b)(1))

is amended, in the first sentence, by inserting ‘‘, investments,’’ after ‘‘other programs’’.

(b) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Secretary shall issue guidance on the implementation of section 13412 of the HITECH Act (42 U.S.C. 17941), which shall include—

(1) recognized security practices (as defined in subsection (b)(1) of such section) that the Secretary may consider when determining fines under such section;

(2) the extent to which such recognized security practices should be in place for consideration by the Secretary; and

(3) procedural requirements or information that shall be submitted by a covered entity or business associate (as such terms are defined in section 13400 of the HITECH Act (42 U.S.C. 17921)) to the Secretary for consideration.

(c) ANNUAL REPORT.—Not later than 2 years after the date of enactment of this Act, and annually thereafter, the Secretary shall include in the annual report required under section 13424(a) of the HITECH Act (42 U.S.C. 17953(a)) information on implementation of section 13412 of such Act (42 U.S.C. 17941), including an accounting of every case in which the Secretary considered

recognized security practices (as defined in subsection (b)(1) of such section) when effectuating audits and assessing fines under such section.

SEC. 9. REQUIRED CYBERSECURITY STANDARDS.

(a) IN GENERAL.—The Secretary shall update the privacy, security, and breach notification regulations under parts 160 and 164 of title 45, Code of Federal Regulations (or any successor regulation) to require covered entities and business associates to adopt the following cybersecurity practices:

(1) Multifactor authentication, or a successor technology, for access to any information systems that may include protected health information.

(2) Safeguards to encrypt protected health information.

(3) Requirements to conduct audits, including penetration testing, to maintain the protections of information systems.

(4) Other minimum cybersecurity standards, as determined by the Secretary, in consultation with private sector entities, based on landscape analysis of emerging and existing cybersecurity vulnerabilities and consensus-based best practices.

(b) EFFECTIVE DATES.—The Secretary shall specify in the regulations the effective date for each of the new

requirements under the regulations updated in accordance with subsection (a). Each such effective date shall provide reasonable time for the entities subject to the requirement to come into compliance.

SEC. 10. GUIDANCE ON RURAL CYBERSECURITY READINESS.

Section 405(d) of the Cybersecurity Act of 2015 (6 U.S.C. 1533(d)) (as amended by section 5(2)) is amended by adding at the end the following:

''(5) RURAL CYBERSECURITY GUIDANCE.—

''(A) DEFINITION OF RURAL.—In this paragraph, the term 'rural' has the meaning given such term by the Health Resources and Services Administration.

''(B) GUIDANCE ON RURAL CYBERSECURITY READINESS.—Not later than 1 year after the date of enactment of the Health Care Cybersecurity and Resiliency Act of 2024, the Secretary shall issue guidance to rural entities on best practices to improve cyber readiness, including strategies—

''(i) to improve cyber infrastructure, including any technical safeguards to mitigate cybersecurity risk;

''(ii) to integrate best practices issued by the Secretary to improve cybersecurity preparedness;

''(iii) to improve employee preparation to mitigate any cybersecurity risks, including existing public-private programs to support educational initiatives; and

''(iv) to implement policies to facilitate mandatory cybersecurity incident reporting requirements under law.

''(C) GAO STUDY AND REPORT.—

''(i) IN GENERAL.—Not later than 3 years after the date of enactment of the Health Care Cybersecurity and Resiliency Act of 2024, the Comptroller General of the United States shall conduct, and submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that describes the results of, a study to examine how rural entities have implemented the recommendations included in the guidance under subparagraph (B).

''(ii) REQUIREMENTS.—The study under clause (i) shall assess—

''(I) how rural entities have implemented any technical safeguards and any challenges faced by such rural entities in areas for which safeguards were not implemented;

''(II) steps to further support cyber resilience for rural entities;

''(III) areas to improve coordination between Federal agencies, including for the purposes of required cyber reporting; and

''(IV) any opportunities to support public-private collaboration in the area of cyber readiness.''.

SEC. 11. GRANTS TO ENHANCE CYBERSECURITY IN THE HEALTH AND PUBLIC HEALTH SECTORS.

Part P of title III of the Public Health Service Act (42 U.S.C. 280g et seq.) is amended by adding at the end the following:

''SEC. 399V–8. GRANTS.

''(a) IN GENERAL.—The Secretary may award grants to eligible entities for the adoption and use of cybersecurity best practices.

''(b) ELIGIBLE ENTITY.—To be eligible to receive a grant under subsection (a) an entity shall be—

''(1) a public or nonprofit private health center (including a Federally qualified health center (as defined in section 1861(aa)(4) of the Social Security Act));

''(2) a health facility operated by or pursuant to a contract with the Indian Health Service;

''(3) a hospital;

''(4) a cancer center;

''(5) a rural health clinic;

''(6) an academic health center; or

''(7) a nonprofit entity that enters into a partnership or coordinates referrals with an entity described in any of paragraphs (1) through (6).

''(c) USE OF FUNDS.—In adopting and using cybersecurity best practices pursuant to a grant under subsection (a), an eligible entity may use grant funds—

''(1) to hire and train personnel in such cybersecurity best practices;

''(2) to update electronic data systems, such as by migrating to cloud based platforms;

''(3) to join and participate in health cybersecurity threat information sharing organizations;

''(4) to reduce the use of legacy systems; and

''(5) to contract with third parties to assist with the activities described in paragraphs (1) through (5).

''(d) GRANT PERIOD.—The Secretary may award a grant under this section for a period of not more than 3 years.

''(e) APPLICATION.—An eligible entity seeking a grant under subsection (a) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require including, at a minimum a description of how the eligible entity will establish baseline measures and benchmarks that meet the Secretary's requirements to evaluate program outcomes.

''(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section such sums as may be necessary for each of fiscal years 2025 through 2030.''.

SEC. 12. HEALTHCARE CYBERSECURITY WORKFORCE.

(a) TRAINING FOR HEALTHCARE EXPERTS.—The Secretary, in coordination with the Cybersecurity State Coordinators of the Agency and private sector health care experts, as appropriate, shall provide training to Healthcare and Public Health Sector asset owners and operators on—

(1) cybersecurity risks to information systems within the Healthcare and Public Health Sector; and

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

(b) CROSS-AGENCY EDUCATIONAL TOOLS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary, acting through the Administrator of the Health Resources and Services Administration, in coordination with the Agency, shall develop a strategic plan to support growing the cybersecurity workforce for health care entities.

(2) INCLUSIONS.—The strategic plan under paragraph (1) shall include—

(A) recommendations for existing educational programs that can be used to support cybersecurity training;

(B) dissemination and development of educational materials on how to improve cybersecurity resilience;

(C) development of best practices to train the health care workforce on cybersecurity best practices; and

(D) opportunities for public-private collaboration to strengthen the cybersecurity workforce.

○