[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

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 HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

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 2026''.

SEC. 2. DEFINITIONS.

In this Act:

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

(2) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (or a successor regulation).

(3) COVERED ENTITY.—The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (or a successor regulation).

(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 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)).

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

(7) HEALTHCARE AND PUBLIC HEALTH SECTOR.—The term ''Healthcare and Public Health Sector'' means the Healthcare and Public Health

sector, as identified in National Security Memorandum–22 (April 30, 2024; relating to critical infrastructure security and resilience).

(8) 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).

(9) INFORMATION SYSTEM.—The term ''information system'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(10) RECOGNIZED SECURITY PRACTICES.—The term ''recognized security practices'' has the meaning given such term in section 13412(b)(1) of the HITECH Act (42 U.S.C. 17941(b)(1)).

(11) 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, sector coordinating councils, 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;

(B) sharing information relating to cyber threat indicators and appropriate defensive measures, including automating cyber threat information sharing, in a manner that adequately protects against unauthorized access or disclosure; and

(C) providing technical assistance to covered entities and business associates to improve cybersecurity preparedness.

(c) JOINT CYBERSECURITY PLANNING.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary and the Director shall establish a joint cybersecurity ca-

pability plan to coordinate responses to significant cybersecurity incidents affecting the Healthcare and Public Health Sector.

(2) ELEMENTS.—The joint cybersecurity capability plan established under paragraph (1) shall include—

(A) protocols for rapid information sharing during sector-wide cybersecurity incidents;

(B) coordination mechanisms with the sector coordinating council for the Healthcare and Public Health Sector; and

(C) coordination with Cybersecurity State Coordinators for incidents affecting multiple States.

(3) SUBMISSION TO CONGRESS.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall 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 the final joint cybersecurity capability plan prepared under paragraph (1) and a description of how such plan implements the elements required under paragraph (2).

(B) UPDATES.—If the Secretary and the Director update the joint cybersecurity capability plan required under this subsection, the Secretary shall 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 such updated plan and a description of how such plan implements the elements required under paragraph (2).

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

(a) IN GENERAL.—The Secretary shall delegate a representative to lead oversight and coordination of activities within the Department of Health and Human Services to support internal and external cybersecurity resilience within the Healthcare and Public Health Sector, including coordination and communication with other public and private entities related to preparedness for, and responses to, cybersecurity incidents, consistent with applicable provisions of the Public Health Service Act (42 U.S.C. 201 et seq.), other applicable laws, and National Security Memorandum–22 (April 30, 2024; relating to critical infrastructure security and resilience). Such activities shall

not include implementation or enforcement of part 160 and subparts A and C of part 164 of title 45, Code of Federal Regulations (or successor regulations) (commonly known as the ''HIPAA Security Rule'').

(b) REPORTS.—

(1) REPORT ON DELEGATION.—Not later than 60 days after delegating a representative under subsection (a), and any time a new representative is delegated under such subsection, the Secretary shall 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 how such representative will implement steps to improve internal and external cybersecurity resilience within the Healthcare and Public Health Sector.

(2) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary shall 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 on the state of cybersecurity in the Healthcare and Public Health Sector, including—

(A) an assessment of the most significant cybersecurity threats and vulnerabilities facing the Healthcare and Public Health Sector;

(B) a summary of major cybersecurity incidents affecting the Healthcare and Public Health Sector during the preceding year;

(C) an assessment of the overall cybersecurity posture of the Healthcare and Public Health Sector;

(D) a description of actions taken by the Department of Health and Human Services to improve cybersecurity; and

(E) recommendations to improve Healthcare and Public Health Sector cybersecurity.

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 2026, the Secretary shall expand and implement the Cyber Annex of the All Hazards Plan of the Department of Health and Human Services to inform applicable personnel within the Department of Health and Human Services of proc-

esses and protocols to prepare for, and respond to, cybersecurity incidents.

"(B) SCOPE.—The plan under subparagraph (A) shall address cybersecurity incidents involving information systems, including hardware, software, databases, and networks, used or maintained by, or on behalf of, the Department.

"(C) ELEMENTS.—The plan under subparagraph (A) shall include 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;

"(vi) to recover from any cybersecurity incidents expeditiously; and

"(vii) to communicate and share non-sensitive information about cybersecurity incidents with entities in the Healthcare and Public Health Sector (as defined in

section 2 of the Health Care Cybersecurity and Resiliency Act of 2026).

''(D) 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, the Director of the National Institute of Standards and Technology, and relevant experts, as appropriate.

''(E) UPDATES.—The Secretary shall review and update the plan under subparagraph (A)—

''(i) not less frequently than once every 2 years; and

''(ii) after any significant cybersecurity incident affecting the Department of Health and Human Services or a Federal health program.

''(F) 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 Gov-

ernmental Affairs of the Senate and the Committee on Energy and Commerce, the Committee on Oversight and Government Reform, and the Committee on Homeland Security of the House of Representatives a report that describes such plan.''.

SEC. 6. 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. 7. 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) REGULATION.—Not later than 1 year after the date of enactment of this Act, the Secretary shall promulgate regulations implementing section 13412 of the HITECH Act (42 U.S.C. 17941), which shall include—

(1) recognized security practices 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;

(3) procedural requirements or information that shall be submitted by a covered entity or business associate to the Secretary for consideration; and

(4) how the Secretary will take into account such recognized security practices when determining fines, earlier favorable termination of audits, or mitigating remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of part 160 and subparts A and C of part 164 of title 45, Code of Federal Regulations (or successor regulations) (commonly known as the ''HIPAA Security rule'') between the covered entity or business associate and the Department of Health and Human Services.

(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 when effectuating audits and assessing fines under such section.

SEC. 8. REQUIRED CYBERSECURITY STANDARDS.

(a) IN GENERAL.—The Secretary shall update the security regulations under part 160, and subparts A and C of part 164, of title 45, Code of Federal Regulations (or any successor regulation), to require non-governmental entities in the Healthcare and Public Health Sector and covered entities and business associates to adopt minimum risk-based cybersecurity practices, including—

(1) multifactor authentication, or a successor technology;

(2) encryption of protected health information, or a successor technology;

(3) requirements to conduct monitoring, including penetration testing, to maintain the protections of information systems; and

(4) other minimum cybersecurity standards, as reflected in national cybersecurity frameworks.

(b) REQUIREMENTS.—The minimum risk-based cybersecurity practices adopted pursuant to subsection (a) shall be based on—

(1) national cybersecurity frameworks, as appropriate, such as—

(A) the National Institute of Standards and Technology Risk Management Framework (or a successor framework);

(B) the National Institute of Standards and Technology Cybersecurity Framework (or a successor framework);

(C) the National Institute of Standards and Technology SP 800–53 r5 Security and Privacy Controls for Information Systems and Organizations (or a successor special publication), with relevant components of the National Institute of Standards and Technology Privacy Framework; or

(D) the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework;

(2) the Health Sector Coordinating Council Cybersecurity Healthcare and Public Health Cybersecurity Performance Goals; and

(3) the health care-specific cybersecurity performance goals of the Cybersecurity and Infrastructure Security Agency.

(c) EFFECTIVE DATES.—The regulations updated in accordance with subsection (a), including each new re-

quirement established, shall take effect on the date that is 36 months after the date of enactment of this Act.

(d) ENFORCEMENT.—The Secretary may exercise enforcement discretion for entities experiencing extraordinary circumstances in complying with the requirements of subsection (a).

(e) MEDICAL DEVICE EXCLUSION.—Notwithstanding subsection (a), the security regulations referred to in such subsection shall not apply to a device (as defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321)) with respect to any activity that is subject to any medical device regulation or guidance issued by the Secretary of Health and Human Services, acting through the Commissioner of Food and Drugs, pursuant to the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301 et seq.).

SEC. 9. 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 further 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 Federal Office of Rural Health Policy.

''(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 2026, the Secretary shall issue guidance to rural entities on best practices to improve cybersecurity readiness, including strategies—

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

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

''(v) to explore and recommend best practices, including—

''(I) outsourcing information technology and chief information secu-

rity officer functions to third parties on a part-time basis;

"(II) participating in regional rural health care information technology management sharing programs; and

"(III) migrating data to secure cloud-based platforms.

"(C) TECHNICAL ASSISTANCE.—The Secretary shall provide technical assistance to rural entities to implement the recommendations included in the guidance under subparagraph (B).

"(D) 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 2026, the Comptroller General of the United States shall conduct a study, 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, on how rural entities have implemented the recommendations included in the guidance under subparagraph (B).

''(ii) CONTENTS.—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 cybersecurity 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 cybersecurity readiness.''.

SEC. 10. GRANTS TO ENHANCE CYBERSECURITY IN THE HEALTH AND PUBLIC HEALTH SECTORS.

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

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

(1) a Federally qualified health center (as defined in section 1861(aa)(4) of the Social Security Act (42 U.S.C. 1395x(aa)(4));

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

(3) a non-profit hospital;

(4) a rural health clinic (as defined in section 1861(aa)(2) of the Social Security Act (42 U.S.C. 1395x(aa)(2)); or

(5) a nonprofit entity that enters into a partnership or coordinates referrals with an entity described in any of paragraphs (1) through (4).

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

(1) to hire individuals with demonstrated cybersecurity expertise 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 contract with third parties to assist the eligible entity in carrying out the activities described in this subsection;

(5) to conduct cybersecurity risk assessments and vulnerability assessments; and

(6) to develop or improve cybersecurity incident response plans.

(d) GRANT PERIOD.—A grant awarded under this section shall be for a period of not more than 3 years.

(e) PRIORITY.—In awarding grants under this section, the Secretary may give consideration to the demonstrated need of eligible entities.

(f) 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—

(1) a description of how the eligible entity will establish baseline measures and benchmarks that meet the Secretary's requirements to evaluate performance outcomes; and

(2) a strategic plan for how, after the end of the grant period, the eligible entity will sustain the activities funded under the grant and continue to adopt cybersecurity best practices.

SEC. 11. HEALTHCARE CYBERSECURITY WORKFORCE.

(a) TRAINING FOR HEALTHCARE EXPERTS.—The Secretary, in coordination with the Cybersecurity State

Coordinators of the Agency, the Office of the National Cyber Director, and private sector health care experts, as appropriate, shall provide training to Healthcare and Public Health Sector entities 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) STRATEGIC PLAN.—

(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) CONTENTS.—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;

(D) development of recommendations specific to rural facilities;

(E) development of best practices to leverage artificial intelligence to support cybersecurity preparedness;

(F) opportunities for public-private collaboration to strengthen the cybersecurity workforce; and

(G) alignment with the National Initiative for Cybersecurity Education Workforce Framework.

SEC. 12. CYBERSECURITY INCIDENT REPORTING COORDINATION WORKING GROUP.

(a) WORKING GROUP.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall convene a working group to examine how to streamline and reduce duplicative reporting for cybersecurity incidents.

(2) MEMBERSHIP.—The working group described in paragraph (1) shall include representatives of—

(A) the Cybersecurity and Infrastructure Security Agency;

(B) the Securities and Exchange Commission;

(C) the Office of the National Cyber Director;

(D) the Federal Bureau of Investigation;

(E) the Federal Trade Commission;

(F) State attorneys general;

(G) State health departments; and

(H) private sector health care entities.

(3) CONCLUSION.—The working group shall conclude not later than 18 months after the date of the first meeting of the working group.

(b) REPORT.—Not later than 1 year after the conclusion of the working group under subsection (a)(3), the Secretary shall 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—

(1) identifies areas the working group has identified to streamline and reduce duplicative reporting;

(2) includes recommendations to Congress on further streamlining such reporting; and

(3) addresses coordination with State breach notification laws.