

118TH CONGRESS
2D SESSION

S. _____

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

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 _____

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.

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 “Health Care Cyberse-
5 curity and Resiliency Act of 2024”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) AGENCY.—The term “Agency” means the
2 Cybersecurity and Infrastructure Security Agency.

3 (2) CYBERSECURITY INCIDENT.—The term “cy-
4 bersecurity incident” has the meaning given the
5 term “incident” in section 3552 of title 44, United
6 States Code.

7 (3) CYBERSECURITY STATE COORDINATOR.—
8 The term “Cybersecurity State Coordinator” means
9 a Cybersecurity State Coordinator appointed under
10 section 2217(a) of the Homeland Security Act of
11 2002 (6 U.S.C. 665c(a)).

12 (4) DIRECTOR.—The term “Director” means
13 the Director of the Agency.

14 (5) HEALTHCARE AND PUBLIC HEALTH SEC-
15 TOR.—The term “Healthcare and Public Health
16 Sector” means the Healthcare and Public Health
17 sector, as identified in Presidential Policy Directive
18 21 (February 12, 2013; relating to critical infra-
19 structure security and resilience).

20 (6) INFORMATION SHARING AND ANALYSIS OR-
21 GANIZATION.—The term “Information Sharing and
22 Analysis Organization” has the meaning given such
23 term in section 2200 of the Homeland Security Act
24 of 2002 (6 U.S.C. 650).

1 (7) INFORMATION SYSTEM.—The term “infor-
2 mation system” has the meaning given such term in
3 section 102 of the Cybersecurity Information Shar-
4 ing Act of 2015 (6 U.S.C. 1501).

5 (8) SECRETARY.—The term “Secretary” means
6 the Secretary of Health and Human Services.

7 **SEC. 3. DEPARTMENT COORDINATION WITH THE AGENCY.**

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

12 (b) ASSISTANCE.—

13 (1) IN GENERAL.—The Secretary shall coordi-
14 nate with the Director to make resources available
15 to entities that are receiving information shared
16 through programs managed by the Director or the
17 Secretary, including Information Sharing and Anal-
18 ysis Organizations, information sharing and analysis
19 centers, and non-Federal entities.

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

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

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

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

7 Part A of title III of the Public Health Service Act
8 (42 U.S.C. 241 et seq.) is amended by adding at the end
9 the following:

10 **“SEC. 310C. OVERSIGHT OF CYBERSECURITY ACTIVITIES.**

11 “The Secretary, acting through the Assistant Sec-
12 retary for Preparedness and Response, in coordination
13 with the Director of the Cybersecurity and Infrastructure
14 Security Agency pursuant to section 2218 of the Home-
15 land Security Act of 2002, shall lead oversight and coordi-
16 nation of activities within the Department of Health and
17 Human Services to support cybersecurity resiliency within
18 the Healthcare and Public Health Sector (as defined in
19 section 2 of the Health Care Cybersecurity and Resiliency
20 Act of 2024), including coordination and communication
21 with other public and private entities related to prepared-
22 ness for, and responses to, cybersecurity incidents, con-
23 sistent with applicable provisions of this Act, other appli-
24 cable laws, and Presidential Policy Directive 21 (February

1 12, 2013; relating to critical infrastructure security and
2 resilience).”.

3 **SEC. 5. CYBERSECURITY INCIDENT RESPONSE PLAN.**

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

6 (1) in subsection (a)—

7 (A) in paragraph (4)—

8 (i) in the paragraph heading, by in-
9 serting “INFORMATION SYSTEM;” after
10 “FEDERAL ENTITY;”; and

11 (ii) by inserting “‘information sys-
12 tem’,” after “‘Federal entity’,”;

13 (B) by redesignating paragraphs (4)
14 through (7) as paragraphs (6) through (9), re-
15 spectively; and

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

18 “(4) CYBERSECURITY INCIDENT.—The term
19 ‘cybersecurity incident’ has the meaning given the
20 term ‘incident’ in section 3552 of title 44, United
21 States Code.

22 “(5) CYBERSECURITY RISK.—The term ‘cyber-
23 security risk’ has the meaning given such term in
24 section 2200 of the Homeland Security Act of 2002
25 (6 U.S.C. 650).”; and

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

3 “(4) PLAN.—

4 “(A) IN GENERAL.—Not later than 1 year
5 after the date of enactment of the Health Care
6 Cybersecurity and Resiliency Act of 2024, the
7 Secretary shall develop and implement a cyber-
8 security incident response plan to inform appli-
9 cable personnel within the Department of
10 Health and Human Services of processes and
11 protocols to prepare for, and respond to, cyber-
12 security incidents involving information, includ-
13 ing hardware, software, databases, and net-
14 works, maintained by, or on behalf of, the De-
15 partment, including strategies—

16 “(i) to assess cybersecurity risks;

17 “(ii) to prevent cybersecurity inci-
18 dents;

19 “(iii) to detect and identify cybersecu-
20 rity incidents;

21 “(iv) to minimize damage in the event
22 of a cybersecurity incident;

23 “(v) to protect data; and

24 “(vi) to recover from any cybersecu-
25 rity incidents expeditiously.

1 “(B) CONSULTATION.—In developing the
2 plan under subparagraph (A), the Secretary
3 shall consult with the Director of the Cyberse-
4 curity and Infrastructure Security Agency, the
5 Director of the Office of Management and
6 Budget, and the Director of the National Insti-
7 tute of Standards and Technology, and relevant
8 experts, as appropriate.

9 “(C) REPORT.—Not later than 60 days be-
10 fore the date on which the Secretary begins im-
11 plementing the plan under subparagraph (A),
12 the Secretary shall submit to the Committee on
13 Health, Education, Labor, and Pensions and
14 the Committee on Homeland Security and Gov-
15 ernmental Affairs of the Senate and the Com-
16 mittee on Energy and Commerce, the Com-
17 mittee on Oversight and Reform, and the Com-
18 mittee on Homeland Security of the House of
19 Representatives a report that describes such
20 plan.”.

21 **SEC. 6. BREACH REPORTING PORTAL.**

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

1 “(k) UPDATES TO REGULATIONS.—Not later than 1
2 year after the date of enactment of the Health Care Cy-
3 bersecurity and Resiliency Act of 2024, the Secretary shall
4 update the regulations promulgated pursuant to sub-
5 section (j) to require that information required to be pub-
6 licly displayed in the breach reporting portal established
7 pursuant to this section includes—

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

11 “(2) information on whether and to what ex-
12 tent, as appropriate, recognized security practices
13 (as defined in section 13412(b)(1)) were considered
14 in the investigation of such a breach; and

15 “(3) such additional information about such a
16 breach as the Secretary may require.”.

17 **SEC. 7. CLARIFYING BREACH REPORTING OBLIGATIONS.**

18 Section 13402(f) of the HITECH Act (42 U.S.C.
19 17932(f)) is amended by adding at the end the following:

20 “(6) The number of individuals affected by the
21 breach.”.

22 **SEC. 8. ENHANCING RECOGNITION OF SECURITY PRACTICES.**
23 **TICES.**

24 (a) **RECOGNIZED SECURITY PRACTICES.**—Section
25 13412(b)(1) of the HITECH Act (42 U.S.C. 17941(b)(1))

1 is amended, in the first sentence, by inserting “, invest-
2 ments,” after “other programs”.

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

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

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

14 (3) procedural requirements or information that
15 shall be submitted by a covered entity or business
16 associate (as such terms are defined in section
17 13400 of the HITECH Act (42 U.S.C. 17921)) to
18 the Secretary for consideration.

19 (c) ANNUAL REPORT.—Not later than 2 years after
20 the date of enactment of this Act, and annually thereafter,
21 the Secretary shall include in the annual report required
22 under section 13424(a) of the HITECH Act (42 U.S.C.
23 17953(a)) information on implementation of section
24 13412 of such Act (42 U.S.C. 17941), including an ac-
25 counting of every case in which the Secretary considered

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

4 **SEC. 9. REQUIRED CYBERSECURITY STANDARDS.**

5 (a) IN GENERAL.—The Secretary shall update the
6 privacy, security, and breach notification regulations
7 under parts 160 and 164 of title 45, Code of Federal Reg-
8 ulations (or any successor regulation) to require covered
9 entities and business associates to adopt the following cy-
10 bersecurity practices:

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

14 (2) Safeguards to encrypt protected health in-
15 formation.

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

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

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

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

5 **SEC. 10. GUIDANCE ON RURAL CYBERSECURITY READI-**
6 **NESS.**

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

10 “(5) RURAL CYBERSECURITY GUIDANCE.—

11 “(A) DEFINITION OF RURAL.—In this
12 paragraph, the term ‘rural’ has the meaning
13 given such term by the Health Resources and
14 Services Administration.

15 “(B) GUIDANCE ON RURAL CYBERSECURITY READINESS.—Not later than 1 year after
16 the date of enactment of the Health Care Cy-
17 bersecurity and Resiliency Act of 2024, the Sec-
18 retary shall issue guidance to rural entities on
19 best practices to improve cyber readiness, in-
20 cluding strategies—

22 “(i) to improve cyber infrastructure,
23 including any technical safeguards to miti-
24 gate cybersecurity risk;

1 “(ii) to integrate best practices issued
2 by the Secretary to improve cybersecurity
3 preparedness;

4 “(iii) to improve employee preparation
5 to mitigate any cybersecurity risks, includ-
6 ing existing public-private programs to
7 support educational initiatives; and

8 “(iv) to implement policies to facilitate
9 mandatory cybersecurity incident reporting
10 requirements under law.

11 “(C) GAO STUDY AND REPORT.—

12 “(i) IN GENERAL.—Not later than 3
13 years after the date of enactment of the
14 Health Care Cybersecurity and Resiliency
15 Act of 2024, the Comptroller General of
16 the United States shall conduct, and sub-
17 mit to the Committee on Health, Edu-
18 cation, Labor, and Pensions of the Senate
19 and the Committee on Energy and Com-
20 merce of the House of Representatives a
21 report that describes the results of, a study
22 to examine how rural entities have imple-
23 mented the recommendations included in
24 the guidance under subparagraph (B).

1 “(ii) REQUIREMENTS.—The study
2 under clause (i) shall assess—

3 “(I) how rural entities have im-
4 plemented any technical safeguards
5 and any challenges faced by such
6 rural entities in areas for which safe-
7 guards were not implemented;

8 “(II) steps to further support
9 cyber resilience for rural entities;

10 “(III) areas to improve coordina-
11 tion between Federal agencies, includ-
12 ing for the purposes of required cyber
13 reporting; and

14 “(IV) any opportunities to sup-
15 port public-private collaboration in the
16 area of cyber readiness.”.

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

19 Part P of title III of the Public Health Service Act
20 (42 U.S.C. 280g et seq.) is amended by adding at the end
21 the following:

22 **“SEC. 399V-8. GRANTS.**

23 “(a) IN GENERAL.—The Secretary may award grants
24 to eligible entities for the adoption and use of cybersecu-
25 rity best practices.

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

3 “(1) a public or nonprofit private health center
4 (including a Federally qualified health center (as de-
5 fined in section 1861(aa)(4) of the Social Security
6 Act));

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

9 “(3) a hospital;

10 “(4) a cancer center;

11 “(5) a rural health clinic;

12 “(6) an academic health center; or

13 “(7) a nonprofit entity that enters into a part-
14 nership or coordinates referrals with an entity de-
15 scribed in any of paragraphs (1) through (6).

16 “(c) USE OF FUNDS.—In adopting and using cyber-
17 security best practices pursuant to a grant under sub-
18 section (a), an eligible entity may use grant funds—

19 “(1) to hire and train personnel in such cyber-
20 security best practices;

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

23 “(3) to join and participate in health cybersecu-
24 rity threat information sharing organizations;

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

1 “(5) to contract with third parties to assist with
2 the activities described in paragraphs (1) through
3 (5).

4 “(d) GRANT PERIOD.—The Secretary may award a
5 grant under this section for a period of not more than
6 3 years.

7 “(e) APPLICATION.—An eligible entity seeking a
8 grant under subsection (a) shall submit to the Secretary
9 an application at such time, in such manner, and con-
10 taining such information as the Secretary may require in-
11 cluding, at a minimum a description of how the eligible
12 entity will establish baseline measures and benchmarks
13 that meet the Secretary’s requirements to evaluate pro-
14 gram outcomes.

15 “(f) AUTHORIZATION OF APPROPRIATIONS.—There
16 are authorized to be appropriated to carry out this section
17 such sums as may be necessary for each of fiscal years
18 2025 through 2030.”.

19 **SEC. 12. HEALTHCARE CYBERSECURITY WORKFORCE.**

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

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

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

5 (b) CROSS-AGENCY EDUCATIONAL TOOLS.—

6 (1) IN GENERAL.—Not later than 1 year after
7 the date of enactment of this Act, the Secretary, act-
8 ing through the Administrator of the Health Re-
9 sources and Services Administration, in coordination
10 with the Agency, shall develop a strategic plan to
11 support growing the cybersecurity workforce for
12 health care entities.

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

15 (A) recommendations for existing edu-
16 cational programs that can be used to support
17 cybersecurity training;

18 (B) dissemination and development of edu-
19 cational materials on how to improve cybersecu-
20 rity resilience;

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

1 (D) opportunities for public-private col-
2 laboration to strengthen the cybersecurity work-
3 force.