

Calendar No. 365

119TH CONGRESS
2^D SESSION

S. 3315

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

DECEMBER 2, 2025

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

MARCH 23, 2026

Reported by Mr. CASSIDY, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Health Care Cyberse-
3 curity and Resiliency Act of 2025”.

4 **SEC. 2. DEFINITIONS.**

5 In this Act:

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

8 (2) **CYBERSECURITY INCIDENT.**—The term “cy-
9 bersecurity incident” has the meaning given the
10 term “incident” in section 3552 of title 44, United
11 States Code.

12 (3) **CYBERSECURITY STATE COORDINATOR.**—
13 The term “Cybersecurity State Coordinator” means
14 a Cybersecurity State Coordinator appointed under
15 section 2217(a) of the Homeland Security Act of
16 2002 (6 U.S.C. 665e(a)).

17 (4) **DIRECTOR.**—The term “Director” means
18 the Director of the Agency.

19 (5) **HEALTHCARE AND PUBLIC HEALTH SEC-**
20 **TOR.**—The term “Healthcare and Public Health
21 Sector” means the Healthcare and Public Health
22 sector, as identified in Presidential Policy Directive
23 21 (February 12, 2013; relating to critical infra-
24 structure security and resilience).

25 (6) **INFORMATION SHARING AND ANALYSIS OR-**
26 **GANIZATION.**—The term “Information Sharing and

1 Analysis Organization” has the meaning given such
 2 term in section 2200 of the Homeland Security Act
 3 of 2002 (6 U.S.C. 650).

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

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

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

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

15 (b) ASSISTANCE.—

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

23 (2) SCOPE.—The coordination under paragraph
 24 (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 2025), including coordination and communication with other public and private entities related to preparedness for, and responses to, cybersecurity incidents, con-

1 sistent with applicable provisions of this Act, other appli-
 2 cable laws, and Presidential Policy Directive 21 (February
 3 12, 2013; relating to critical infrastructure security and
 4 resilience).”.

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

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

8 (1) in subsection (a)—

9 (A) in paragraph (4)—

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

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

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

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

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

24 “(5) CYBERSECURITY RISK.—The term ‘cyber-
 25 security risk’ has the meaning given such term in

1 section 2200 of the Homeland Security Act of 2002
 2 (6 U.S.C. 650).”;

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

5 “(4) PLAN.—

6 “(A) IN GENERAL.—Not later than 1 year
 7 after the date of enactment of the Health Care
 8 Cybersecurity and Resiliency Act of 2025, the
 9 Secretary shall develop and implement a cyber-
 10 security incident response plan to inform appli-
 11 cable personnel within the Department of
 12 Health and Human Services of processes and
 13 protocols to prepare for, and respond to, cyber-
 14 security incidents involving information, includ-
 15 ing hardware, software, databases, and net-
 16 works, used or maintained by, or on behalf of,
 17 the Department, including strategies—

18 “(i) to assess cybersecurity risks;

19 “(ii) to prevent cybersecurity inci-
 20 dents;

21 “(iii) to detect and identify cybersecu-
 22 rity incidents;

23 “(iv) to minimize damage in the event
 24 of a cybersecurity incident;

25 “(v) to protect data; and

1 “(vi) to recover from any cybersecu-
2 rity incidents expeditiously.

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

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

1 **SEC. 6. BREACH REPORTING PORTAL.**

2 ~~(a) UPDATES TO BREACH REPORTING PORTAL.—~~

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

5 ~~“(k) UPDATES TO REGULATIONS.—Not later than 1~~
6 ~~year after the date of enactment of the Health Care Cy-~~
7 ~~bersecurity and Resiliency Act of 2025, the Secretary shall~~
8 ~~update the regulations promulgated pursuant to sub-~~
9 ~~section (j) to require that information required to be pub-~~
10 ~~licly displayed in the breach reporting portal established~~
11 ~~pursuant to this section includes—~~

12 ~~“(1) information on any corrective action taken~~
13 ~~against a covered entity that provided notification of~~
14 ~~a breach under this section;~~

15 ~~“(2) information on whether and to what ex-~~
16 ~~tent, as appropriate, recognized security practices~~
17 ~~(as defined in section 13412(b)(1)) were considered~~
18 ~~in the investigation of such a breach; and~~

19 ~~“(3) such additional information about such a~~
20 ~~breach as the Secretary may require.”.~~

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

22 Section 13402(f) of the HITECH Act (42 U.S.C.
23 17932(f)) is amended by adding at the end the following:

24 ~~“(6) The number of individuals affected by the~~
25 ~~breach.”.~~

1 **SEC. 8. ENHANCING RECOGNITION OF SECURITY PRAC-**
 2 **TICES.**

3 (a) **RECOGNIZED SECURITY PRACTICES.**—Section
 4 13412(b)(1) of the HITECH Act (42 U.S.C. 17941(b)(1))
 5 is amended, in the first sentence, by inserting “, invest-
 6 ments,” after “other programs”.

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

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

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

18 (3) procedural requirements or information that
 19 shall be submitted by a covered entity or business
 20 associate (as such terms are defined in section
 21 13400 of the HITECH Act (42 U.S.C. 17921)) to
 22 the Secretary for consideration.

23 (c) **ANNUAL REPORT.**—Not later than 2 years after
 24 the date of enactment of this Act, and annually thereafter,
 25 the Secretary shall include in the annual report required
 26 under section 13424(a) of the HITECH Act (42 U.S.C.

1 ~~17953(a))~~ information on implementation of section
 2 ~~13412~~ of such Act (~~42 U.S.C. 17941~~), including an ac-
 3 counting of every case in which the Secretary considered
 4 recognized security practices (as defined in subsection
 5 (b)(1) of such section) when effectuating audits and as-
 6 sessing fines under such section.

7 **SEC. 9. REQUIRED CYBERSECURITY STANDARDS.**

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

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

17 (2) Safeguards to encrypt protected health in-
 18 formation.

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

22 (4) Other minimum cybersecurity standards, as
 23 determined by the Secretary, in consultation with
 24 private sector entities, based on landscape analysis

1 of emerging and existing cybersecurity vulnerabilities
 2 and consensus-based best practices.

3 ~~(b) EFFECTIVE DATES.—The Secretary shall specify~~
 4 ~~in the regulations the effective date for each of the new~~
 5 ~~requirements under the regulations updated in accordance~~
 6 ~~with subsection (a). Each such effective date shall provide~~
 7 ~~reasonable time for the entities subject to the requirement~~
 8 ~~to come into compliance.~~

9 **SEC. 10. GUIDANCE ON RURAL CYBERSECURITY READI-**
 10 **NESS.**

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

14 “(5) RURAL CYBERSECURITY GUIDANCE.—

15 “(A) DEFINITION OF RURAL.—In this
 16 paragraph, the term ‘rural’ has the meaning
 17 given such term by the Health Resources and
 18 Services Administration.

19 “(B) GUIDANCE ON RURAL CYBERSECURITY READINESS.—Not later than 1 year after
 20 the date of enactment of the Health Care Cy-
 21 bersecurity and Resiliency Act of 2025, the Sec-
 22 retary shall issue guidance to rural entities on
 23 best practices to improve cyber readiness, in-
 24 cluding strategies—
 25

1 “(i) to improve cyber infrastructure,
2 including any technical safeguards to miti-
3 gate cybersecurity risk;

4 “(ii) to integrate best practices issued
5 by the Secretary to improve cybersecurity
6 preparedness;

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

11 “(iv) to implement policies to facilitate
12 mandatory cybersecurity incident reporting
13 requirements under law.

14 “(C) GAO STUDY AND REPORT.—

15 “(i) IN GENERAL.—Not later than 3
16 years after the date of enactment of the
17 Health Care Cybersecurity and Resiliency
18 Act of 2025, the Comptroller General of
19 the United States shall conduct, and sub-
20 mit to the Committee on Health, Edu-
21 cation, Labor, and Pensions of the Senate
22 and the Committee on Energy and Com-
23 merce of the House of Representatives a
24 report that describes the results of, a study
25 to examine how rural entities have imple-

1 mented the recommendations included in
2 the guidance under subparagraph (B).

3 “(ii) ~~REQUIREMENTS.~~—The study
4 under clause (i) shall assess—

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

10 “(II) steps to further support
11 cyber resilience for rural entities;

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

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

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

21 Part P of title III of the Public Health Service Act
22 (42 U.S.C. 280g et seq.) is amended by adding at the end
23 the following:

1 ~~“SEC. 399V-8. GRANTS.~~

2 ~~“(a) IN GENERAL.—The Secretary may award grants~~
 3 ~~to eligible entities for the adoption and use of cybersecu-~~
 4 ~~rity best practices.~~

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

7 ~~“(1) a public or nonprofit private health center~~
 8 ~~(including a Federally qualified health center (as de-~~
 9 ~~finied in section 1861(aa)(4) of the Social Security~~
 10 ~~Act));~~

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

13 ~~“(3) a hospital;~~

14 ~~“(4) a cancer center;~~

15 ~~“(5) a rural health clinic;~~

16 ~~“(6) an academic health center; or~~

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

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

23 ~~“(1) to hire and train personnel in such cyber-~~
 24 ~~security best practices;~~

25 ~~“(2) to update electronic data systems, such as~~
 26 ~~by migrating to cloud based platforms;~~

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

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

4 “(5) to contract with third parties to assist with
5 the activities described in paragraphs (1) through
6 (5).

7 “(d) GRANT PERIOD.—The Secretary may award a
8 grant under this section for a period of not more than
9 3 years.

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

18 “(f) AUTHORIZATION OF APPROPRIATIONS.—There
19 are authorized to be appropriated to carry out this section
20 such sums as may be necessary for each of fiscal years
21 2025 through 2030.”.

22 **SEC. 12. HEALTHCARE CYBERSECURITY WORKFORCE.**

23 (a) TRAINING FOR HEALTHCARE EXPERTS.—The
24 Secretary, in coordination with the Cybersecurity State
25 Coordinators of the Agency and private sector health care

1 experts, as appropriate, shall provide training to
 2 Healthcare and Public Health Sector asset owners and op-
 3 erators on—

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

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

8 (b) CROSS-AGENCY EDUCATIONAL TOOLS.—

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

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

18 (A) recommendations for existing edu-
 19 cational programs that can be used to support
 20 cybersecurity training;

21 (B) dissemination and development of edu-
 22 cational materials on how to improve cybersecu-
 23 rity resilience;

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

4 (D) opportunities for public-private col-
 5 laboration to strengthen the cybersecurity work-
 6 force.

7 **SECTION 1. SHORT TITLE.**

8 *This Act may be cited as the “Health Care Cybersecu-*
 9 *rity and Resiliency Act of 2026”.*

10 **SEC. 2. DEFINITIONS.**

11 *In this Act:*

12 (1) *AGENCY.*—*The term “Agency” means the Cy-*
 13 *bersecurity and Infrastructure Security Agency.*

14 (2) *BUSINESS ASSOCIATE.*—*The term “business*
 15 *associate” has the meaning given such term in section*
 16 *160.103 of title 45, Code of Federal Regulations (or*
 17 *a successor regulation).*

18 (3) *COVERED ENTITY.*—*The term “covered enti-*
 19 *ty” has the meaning given such term in section*
 20 *160.103 of title 45, Code of Federal Regulations (or*
 21 *a successor regulation).*

22 (4) *CYBERSECURITY INCIDENT.*—*The term “cy-*
 23 *bersecurity incident” has the meaning given the term*
 24 *“incident” in section 3552 of title 44, United States*
 25 *Code.*

1 (5) *CYBERSECURITY STATE COORDINATOR.*—*The*
 2 *term “Cybersecurity State Coordinator” means a Cy-*
 3 *bersecurity State Coordinator appointed under section*
 4 *2217(a) of the Homeland Security Act of 2002 (6*
 5 *U.S.C. 665c(a)).*

6 (6) *DIRECTOR.*—*The term “Director” means the*
 7 *Director of the Agency.*

8 (7) *HEALTHCARE AND PUBLIC HEALTH SEC-*
 9 *TOR.*—*The term “Healthcare and Public Health Sec-*
 10 *tor” means the Healthcare and Public Health sector,*
 11 *as identified in National Security Memorandum–22*
 12 *(April 30, 2024; relating to critical infrastructure se-*
 13 *curity and resilience).*

14 (8) *INFORMATION SHARING AND ANALYSIS ORGA-*
 15 *NIZATION.*—*The term “Information Sharing and*
 16 *Analysis Organization” has the meaning given such*
 17 *term in section 2200 of the Homeland Security Act*
 18 *of 2002 (6 U.S.C. 650).*

19 (9) *INFORMATION SYSTEM.*—*The term “informa-*
 20 *tion system” has the meaning given such term in sec-*
 21 *tion 2200 of the Homeland Security Act of 2002 (6*
 22 *U.S.C. 650).*

23 (10) *RECOGNIZED SECURITY PRACTICES.*—*The*
 24 *term “recognized security practices” has the meaning*

1 *given such term in section 13412(b)(1) of the*
 2 *HITECH Act (42 U.S.C. 17941(b)(1)).*

3 (11) *SECRETARY.*—*The term “Secretary” means*
 4 *the Secretary of Health and Human Services.*

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

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

10 (b) *ASSISTANCE.*—

11 (1) *IN GENERAL.*—*The Secretary shall coordi-*
 12 *nate with the Director to make resources available to*
 13 *entities that are receiving information shared through*
 14 *programs managed by the Director or the Secretary,*
 15 *including Information Sharing and Analysis Organi-*
 16 *zations, sector coordinating councils, and non-Federal*
 17 *entities.*

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

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

22 (B) *sharing information relating to cyber*
 23 *threat indicators and appropriate defensive*
 24 *measures, including automating cyber threat in-*
 25 *formation sharing, in a manner that adequately*

1 *protects against unauthorized access or disclo-*
 2 *sure; and*

3 (C) *providing technical assistance to cov-*
 4 *ered entities and business associates to improve*
 5 *cybersecurity preparedness.*

6 (c) *JOINT CYBERSECURITY PLANNING.—*

7 (1) *IN GENERAL.—Not later than 1 year after*
 8 *the date of enactment of this Act, the Secretary and*
 9 *the Director shall establish a joint cybersecurity capa-*
 10 *bility plan to coordinate responses to significant cy-*
 11 *bersecurity incidents affecting the Healthcare and*
 12 *Public Health Sector.*

13 (2) *ELEMENTS.—The joint cybersecurity capa-*
 14 *bility plan established under paragraph (1) shall in-*
 15 *clude—*

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

18 (B) *coordination mechanisms with the sec-*
 19 *tor coordinating council for the Healthcare and*
 20 *Public Health Sector; and*

21 (C) *coordination with Cybersecurity State*
 22 *Coordinators for incidents affecting multiple*
 23 *States.*

24 (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

1 *within the Department of Health and Human Services to*
 2 *support internal and external cybersecurity resilience with-*
 3 *in the Healthcare and Public Health Sector, including co-*
 4 *ordination and communication with other public and pri-*
 5 *vate entities related to preparedness for, and responses to,*
 6 *cybersecurity incidents, consistent with applicable provi-*
 7 *sions of the Public Health Service Act (42 U.S.C. 201 et*
 8 *seq.), other applicable laws, and National Security Memo-*
 9 *randum–22 (April 30, 2024; relating to critical infrastruc-*
 10 *ture security and resilience). Such activities shall not in-*
 11 *clude implementation or enforcement of part 160 and sub-*
 12 *parts A and C of part 164 of title 45, Code of Federal Regu-*
 13 *lations (or successor regulations) (commonly known as the*
 14 *“HIPAA Security Rule”).*

15 (b) *REPORTS.—*

16 (1) *REPORT ON DELEGATION.—Not later than 60*
 17 *days after delegating a representative under sub-*
 18 *section (a), and any time a new representative is del-*
 19 *egated under such subsection, the Secretary shall sub-*
 20 *mit to the Committee on Health, Education, Labor,*
 21 *and Pensions of the Senate and the Committee on*
 22 *Energy and Commerce of the House of Representa-*
 23 *tives a report that describes how such representative*
 24 *will implement steps to improve internal and external*

1 *cybersecurity resilience within the Healthcare and*
2 *Public Health Sector.*

3 (2) *ANNUAL REPORT.*—*Not later than 1 year*
4 *after the date of enactment of this Act, and annually*
5 *thereafter, the Secretary shall submit to the Com-*
6 *mittee on Health, Education, Labor, and Pensions of*
7 *the Senate and the Committee on Energy and Com-*
8 *merce of the House of Representatives a report on the*
9 *state of cybersecurity in the Healthcare and Public*
10 *Health Sector, including—*

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

14 (B) *a summary of major cybersecurity inci-*
15 *dents affecting the Healthcare and Public Health*
16 *Sector during the preceding year;*

17 (C) *an assessment of the overall cybersecu-*
18 *rity posture of the Healthcare and Public Health*
19 *Sector;*

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

23 (E) *recommendations to improve*
24 *Healthcare and Public Health Sector cybersecu-*
25 *rity.*

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

2 *Section 405 of the Cybersecurity Act of 2015 (6 U.S.C.*
 3 *1533) is amended—*

4 *(1) in subsection (a)—*

5 *(A) in paragraph (4)—*

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

9 *(ii) by inserting “‘information sys-*
 10 *tem’,” after “‘Federal entity’,”;*

11 *(B) by redesignating paragraphs (4)*
 12 *through (7) as paragraphs (6) through (9), re-*
 13 *spectively; and*

14 *(C) by inserting after paragraph (3) the fol-*
 15 *lowing:*

16 *“(4) CYBERSECURITY INCIDENT.—The term ‘cy-*
 17 *bersecurity incident’ has the meaning given the term*
 18 *‘incident’ in section 3552 of title 44, United States*
 19 *Code.*

20 *“(5) CYBERSECURITY RISK.—The term ‘cyberse-*
 21 *curity risk’ has the meaning given such term in sec-*
 22 *tion 2200 of the Homeland Security Act of 2002 (6*
 23 *U.S.C. 650).”; and*

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

26 *“(4) PLAN.—*

1 “(A) *IN GENERAL.*—Not later than 1 year
2 after the date of enactment of the Health Care
3 Cybersecurity and Resiliency Act of 2026, the
4 Secretary shall expand and implement the Cyber
5 Annex of the All Hazards Plan of the Depart-
6 ment of Health and Human Services to inform
7 applicable personnel within the Department of
8 Health and Human Services of processes and
9 protocols to prepare for, and respond to, cyberse-
10 curity incidents.

11 “(B) *SCOPE.*—The plan under subpara-
12 graph (A) shall address cybersecurity incidents
13 involving information systems, including hard-
14 ware, software, databases, and networks, used or
15 maintained by, or on behalf of, the Department.

16 “(C) *ELEMENTS.*—The plan under subpara-
17 graph (A) shall include strategies—

18 “(i) to assess cybersecurity risks;

19 “(ii) to prevent cybersecurity incidents;

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

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

24 “(v) to protect data;

1 “(vi) to recover from any cybersecurity
2 incidents expeditiously; and

3 “(vii) to communicate and share non-
4 sensitive information about cybersecurity
5 incidents with entities in the Healthcare
6 and Public Health Sector (as defined in sec-
7 tion 2 of the Health Care Cybersecurity and
8 Resiliency Act of 2026).

9 “(D) CONSULTATION.—In developing the
10 plan under subparagraph (A), the Secretary
11 shall consult with the Director of the Cybersecu-
12 rity and Infrastructure Security Agency, the Di-
13 rector of the Office of Management and Budget,
14 the Director of the National Institute of Stand-
15 ards and Technology, and relevant experts, as
16 appropriate.

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

19 “(i) not less frequently than once every
20 2 years; and

21 “(ii) after any significant cybersecu-
22 rity incident affecting the Department of
23 Health and Human Services or a Federal
24 health program.

1 “(F) *REPORT*.—Not later than 60 days be-
 2 fore the date on which the Secretary begins im-
 3 plementing the plan under subparagraph (A),
 4 the Secretary shall submit to the Committee on
 5 Health, Education, Labor, and Pensions and the
 6 Committee on Homeland Security and Govern-
 7 mental Affairs of the Senate and the Committee
 8 on Energy and Commerce, the Committee on
 9 Oversight and Reform, and the Committee on
 10 Homeland Security of the House of Representa-
 11 tives a report that describes such plan.”.

12 **SEC. 6. CLARIFYING BREACH REPORTING OBLIGATIONS.**

13 Section 13402(f) of the HITECH Act (42 U.S.C.
 14 17932(f)) is amended by adding at the end the following:

15 “(6) The number of individuals affected by the
 16 breach.”.

17 **SEC. 7. ENHANCING RECOGNITION OF SECURITY PRACTICES.**

18 **TICES.**
 19 (a) *RECOGNIZED SECURITY PRACTICES*.—Section
 20 13412(b)(1) of the HITECH Act (42 U.S.C. 17941(b)(1))
 21 is amended, in the first sentence, by inserting “, invest-
 22 ments,” after “other programs”.

23 (b) *REGULATION*.—Not later than 1 year after the date
 24 of enactment of this Act, the Secretary shall promulgate reg-

1 *ulations implementing section 13412 of the HITECH Act*
2 *(42 U.S.C. 17941), which shall include—*

3 *(1) recognized security practices that the Sec-*
4 *retary may consider when determining fines under*
5 *such section;*

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

9 *(3) procedural requirements or information that*
10 *shall be submitted by a covered entity or business as-*
11 *sociate to the Secretary for consideration; and*

12 *(4) how the Secretary will take into account such*
13 *recognized security practices when determining fines,*
14 *earlier favorable termination of audits, or mitigating*
15 *remedies that would otherwise be agreed to in any*
16 *agreement with respect to resolving potential viola-*
17 *tions of part 160 and subparts A and C of part 164*
18 *of title 45, Code of Federal Regulations (or successor*
19 *regulations) (commonly known as the “HIPAA Secu-*
20 *urity Rule”)* *between the covered entity or business as-*
21 *sociate and the Department of Health and Human*
22 *Services.*

23 *(c) ANNUAL REPORT.—Not later than 2 years after the*
24 *date of enactment of this Act, and annually thereafter, the*
25 *Secretary shall include in the annual report required under*

1 *section 13424(a) of the HITECH Act (42 U.S.C. 17953(a))*
 2 *information on implementation of section 13412 of such Act*
 3 *(42 U.S.C. 17941), including an accounting of every case*
 4 *in which the Secretary considered recognized security prac-*
 5 *tices when effectuating audits and assessing fines under*
 6 *such section.*

7 **SEC. 8. REQUIRED CYBERSECURITY STANDARDS.**

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

15 *(1) multifactor authentication, or a successor*
 16 *technology;*

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

19 *(3) requirements to conduct monitoring, includ-*
 20 *ing penetration testing, to maintain the protections of*
 21 *information systems; and*

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

1 (b) *REQUIREMENTS.*—*The minimum risk-based cyber-*
 2 *security practices adopted pursuant to subsection (a) shall*
 3 *be based on—*

4 (1) *national cybersecurity frameworks, as appro-*
 5 *priate, such as—*

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

9 (B) *the National Institute of Standards and*
 10 *Technology Cybersecurity Framework (or a suc-*
 11 *cessor framework);*

12 (C) *the National Institute of Standards and*
 13 *Technology SP 800–53 r5 Security and Privacy*
 14 *Controls for Information Systems and Organiza-*
 15 *tions (or a successor special publication), with*
 16 *relevant components of the National Institute of*
 17 *Standards and Technology Privacy Framework;*
 18 *or*

19 (D) *the National Institute of Standards and*
 20 *Technology Artificial Intelligence Risk Manage-*
 21 *ment Framework;*

22 (2) *the Health Sector Coordinating Council Cy-*
 23 *bersecurity Healthcare and Public Health Cybersecu-*
 24 *rity Performance Goals; and*

1 (3) *the health care-specific cybersecurity per-*
 2 *formance goals of the Cybersecurity and Infrastruc-*
 3 *ture Security Agency.*

4 (c) *EFFECTIVE DATES.*—*The regulations updated in*
 5 *accordance with subsection (a), including each new require-*
 6 *ment established, shall take effect on the date that is 36*
 7 *months after the date of enactment of this Act.*

8 (d) *ENFORCEMENT.*—*The Secretary may exercise en-*
 9 *forcement discretion for entities experiencing extraordinary*
 10 *circumstances in complying with the requirements of sub-*
 11 *section (a).*

12 **SEC. 9. GUIDANCE ON RURAL CYBERSECURITY READINESS.**

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

16 “(5) *RURAL CYBERSECURITY GUIDANCE.*—

17 “(A) *DEFINITION OF RURAL.*—*In this para-*
 18 *graph, the term ‘rural’ has the meaning given*
 19 *such term by the Federal Office of Rural Health*
 20 *Policy.*

21 “(B) *GUIDANCE ON RURAL CYBERSECURITY*
 22 *READINESS.*—*Not later than 1 year after the*
 23 *date of enactment of the Health Care Cybersecu-*
 24 *rity and Resiliency Act of 2026, the Secretary*
 25 *shall issue guidance to rural entities on best*

1 *practices to improve cybersecurity readiness, in-*
2 *cluding strategies—*

3 *“(i) to improve cybersecurity infra-*
4 *structure, including any technical safe-*
5 *guards to mitigate cybersecurity risk;*

6 *“(ii) to integrate best practices issued*
7 *by the Secretary to improve cybersecurity*
8 *preparedness;*

9 *“(iii) to improve workforce prepara-*
10 *tion to mitigate any cybersecurity risks, in-*
11 *cluding existing public-private programs to*
12 *support educational initiatives;*

13 *“(iv) to implement policies to facilitate*
14 *mandatory cybersecurity incident reporting*
15 *requirements under law; and*

16 *“(v) to explore and recommend best*
17 *practices, including—*

18 *“(I) outsourcing information tech-*
19 *nology and chief information security*
20 *officer functions to third parties on a*
21 *part-time basis;*

22 *“(II) participating in regional*
23 *rural health care information tech-*
24 *nology management sharing programs;*
25 *and*

1 “(III) *migrating data to secure*
2 *cloud-based platforms.*

3 “(C) *TECHNICAL ASSISTANCE.—The Sec-*
4 *retary shall provide technical assistance to rural*
5 *entities to implement the recommendations in-*
6 *cluded in the guidance under subparagraph (B).*

7 “(D) *GAO STUDY AND REPORT.—*

8 “(i) *IN GENERAL.—Not later than 3*
9 *years after the date of enactment of the*
10 *Health Care Cybersecurity and Resiliency*
11 *Act of 2026, the Comptroller General of the*
12 *United States shall conduct a study, and*
13 *submit to the Committee on Health, Edu-*
14 *cation, Labor, and Pensions of the Senate*
15 *and the Committee on Energy and Com-*
16 *merce of the House of Representatives a re-*
17 *port, on how rural entities have imple-*
18 *mented the recommendations included in*
19 *the guidance under subparagraph (B).*

20 “(ii) *CONTENTS.—The study under*
21 *clause (i) shall assess—*

22 “(I) *how rural entities have im-*
23 *plemented any technical safeguards*
24 *and any challenges faced by such rural*

1 *entities in areas for which safeguards*
 2 *were not implemented;*

3 *“(II) steps to further support cy-*
 4 *bersecurity resilience for rural entities;*

5 *“(III) areas to improve coordina-*
 6 *tion between Federal agencies, includ-*
 7 *ing for the purposes of required cyber*
 8 *reporting; and*

9 *“(IV) any opportunities to sup-*
 10 *port public-private collaboration in the*
 11 *area of cybersecurity readiness.”.*

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

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

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

19 *(1) a Federally qualified health center (as de-*
 20 *finied in section 1861(aa)(4) of the Social Security*
 21 *Act (42 U.S.C. 1395x(aa)(4)));*

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

24 *(3) a nonprofit hospital;*

1 (4) a rural health clinic (as defined in section
2 1861(aa)(2) of the Social Security Act (42 U.S.C.
3 1395x(aa)(2))); or

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

7 (c) *USE OF FUNDS.*—In adopting and implementing
8 cybersecurity best practices pursuant to a grant under sub-
9 section (a), an eligible entity may use grant funds—

10 (1) to hire individuals with demonstrated cyber-
11 security expertise and train personnel in such cyber-
12 security best practices;

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

15 (3) to join and participate in health cybersecu-
16 rity threat information sharing organizations;

17 (4) to contract with third parties to assist the el-
18 igible entity in carrying out the activities described
19 in this subsection;

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

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

24 (d) *GRANT PERIOD.*—A grant awarded under this sec-
25 tion shall be for a period of not more than 3 years.

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

4 (f) *APPLICATION.*—*An eligible entity seeking a grant*
 5 *under subsection (a) shall submit to the Secretary an appli-*
 6 *cation at such time, in such manner, and containing such*
 7 *information as the Secretary may require, including—*

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

12 (2) *a strategic plan for how, after the end of the*
 13 *grant period, the eligible entity will sustain the ac-*
 14 *tivities funded under the grant and continue to adopt*
 15 *cybersecurity best practices.*

16 (g) *AUTHORIZATION OF APPROPRIATIONS.*—*There are*
 17 *authorized to be appropriated to carry out this section such*
 18 *sums as may be necessary for each of fiscal years 2026*
 19 *through 2030.*

20 **SEC. 11. HEALTHCARE CYBERSECURITY WORKFORCE.**

21 (a) *TRAINING FOR HEALTHCARE EXPERTS.*—*The Sec-*
 22 *retary, in coordination with the Cybersecurity State Coor-*
 23 *dinators of the Agency, the Office of the National Cyber Di-*
 24 *rector, and private sector health care experts, as appro-*

1 *priate, shall provide training to Healthcare and Public*
 2 *Health Sector entities on—*

3 *(1) cybersecurity risks to information systems*
 4 *within the Healthcare and Public Health Sector; and*
 5 *(2) ways to mitigate the risks to information*
 6 *systems in the Healthcare and Public Health Sector.*

7 *(b) STRATEGIC PLAN.—*

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

15 *(2) CONTENTS.—The strategic plan under para-*
 16 *graph (1) shall include—*

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

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

23 *(C) development of best practices to train*
 24 *the health care workforce on cybersecurity best*
 25 *practices;*

1 (D) development of recommendations spe-
2 cific to rural facilities;

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

6 (F) opportunities for public-private collabo-
7 ration to strengthen the cybersecurity workforce;
8 and

9 (G) alignment with the National Initiative
10 for Cybersecurity Education Workforce Frame-
11 work.

12 **SEC. 12. CYBERSECURITY INCIDENT REPORTING COORDI-**
13 **NATION WORKING GROUP.**

14 (a) *WORKING GROUP.*—

15 (1) *IN GENERAL.*—Not later than 1 year after
16 the date of enactment of this Act, the Secretary shall
17 convene a working group to examine how to stream-
18 line and reduce duplicative reporting for cybersecu-
19 rity incidents.

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

22 (A) the Cybersecurity and Infrastructure
23 Security Agency;

24 (B) the Securities and Exchange Commis-
25 sion;

1 (C) the Office of the National Cyber Direc-
2 tor;

3 (D) the Federal Bureau of Investigation;

4 (E) the Federal Trade Commission;

5 (F) State attorneys general;

6 (G) State health departments; and

7 (H) private sector health care entities.

8 (3) CONCLUSION.—The working group shall con-
9 clude not later than 18 months after the date of the
10 first meeting of the working group.

11 (b) REPORT.—Not later than 1 year after the conclu-
12 sion of the working group under subsection (a)(3), the Sec-
13 retary shall submit to the Committee on Health, Education,
14 Labor, and Pensions of the Senate and the Committee on
15 Energy and Commerce of the House of Representatives a
16 report that—

17 (1) identifies areas the working group has identi-
18 fied to streamline and reduce duplicative reporting;

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

21 (3) addresses coordination with State breach no-
22 tification laws.

Calendar No. 365

119TH CONGRESS
2^D Session
S. 3315

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.

MARCH 23, 2026
Reported with an amendment