''(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 nonprofit 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.

AUTHORITY FOR COMMITTEES TO MEET

Mrs. BLACKBURN. Mr. President, I have six requests for committees to meet during today's session of the Senate. They have the approval of the Majority and Minority Leaders.

Pursuant to rule XXVI, paragraph 5(a), of the Standing Rules of the Senate, the following committees are authorized to meet during today's session of the Senate:

COMMITTEE ON ARMED SERVICES

The Committee on Armed Services is authorized to meet in closed session during the session of the Senate on Tuesday, June 9, 2026, at 2:30 p.m.

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

The Committee on Commerce, Science, and Transportation is authorized to meet during the session of the Senate on Tuesday, June 9, 2026, at 10 a.m., to conduct a subcommittee hearing.

SUBCOMMITTEE ON AIRLAND

The Subcommittee on Airland of the Committee on Armed Services is authorized to meet in closed session during the session of the Senate on Tuesday, June 9, 2026, at 10 a.m.

SUBCOMMITTEE ON CYBERSECURITY

The Subcommittee on Cybersecurity of the Committee on Armed Services is authorized to meet in closed session during the session of the Senate on Tuesday, June 9, 2026, at 11 a.m.

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

The Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services is authorized to meet in closed session during the session of the Senate on Tuesday, June 9, 2026, at 9:15 a.m.

SUBCOMMITTEE ON PERSONNEL

The Subcommittee on Personnel of the Committee on Armed Services is authorized to meet in open session during the session of the Senate on Tuesday, June 9, 2026, at 9:30 a.m.

PRIVILEGES OF THE FLOOR

Mr. CASSIDY. Mr. President, I ask unanimous consent that Eva Friedlander, an intern in my office, be granted floor privileges until June 10, 2026.

The PRESIDING OFFICER. Without objection, it is so ordered.

RESOLUTIONS SUBMITTED TODAY

Mr. THUNE. Mr. President, I ask unanimous consent that the Senate now proceed to the en bloc consideration of the following Senate resolutions, which are at the desk: S. Res. 764 and S. Res. 765.

There being no objection, the Senate proceeded to consider the resolutions en bloc.

Mr. THUNE. I ask unanimous consent that the resolutions be agreed to, the preambles be agreed to, and that the motions to reconsider be considered made and laid upon the table, all en bloc.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolutions were agreed to.

The preambles were agreed to.