118TH CONGRESS
1ST SESSION

S. _____

To direct the Director of the Cybersecurity and Infrastructure Security Agency to establish a K–12 Cybersecurity Technology Improvement Program, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mrs. BLACKBURN (for herself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To direct the Director of the Cybersecurity and Infrastructure Security Agency to establish a K–12 Cybersecurity Technology Improvement Program, 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 cited as the ''Enhancing K–12 Cybersecurity Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED ENTITY.—The term ''covered entity'' means the following:

(A) An elementary school.

(B) A secondary school.

(C) A local educational agency.

(D) A State educational agency.

(E) An educational service agency.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) EDUCATIONAL SERVICE AGENCY.—The term ''educational service agency'' has the meaning given that term in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(4) ELEMENTARY SCHOOL.—The term ''elementary school'' has the meaning given that term in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(5) INFORMATION EXCHANGE.—The term ''Information Exchange'' means the School Cybersecurity Information Exchange established under section 3(a).

(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''Information Sharing and

Analysis Organization'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(7) LOCAL EDUCATIONAL AGENCY.—The term ''local educational agency'' has the meaning given that term in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(8) SECONDARY SCHOOL.—The term ''secondary school'' has the meaning given that term in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(9) STATE EDUCATIONAL AGENCY.—The term ''State educational agency'' has the meaning given that term in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

SEC. 3. SCHOOL CYBERSECURITY INFORMATION EXCHANGE.

(a) ESTABLISHMENT.—The Director shall enhance existing information exchange efforts implemented through partnerships with 1 or more Information Sharing and Analysis Organizations to focus specific attention on the needs of covered entities with regard to cybersecurity, including a new publicly accessible website (to be known as the ''School Cybersecurity Information Exchange'') to disseminate information, cybersecurity best practices,

training, and lessons learned tailored to the specific needs of, technical expertise of, and resources available to covered entities, in accordance with subsection (b).

(b) DUTIES.—In establishing the Information Exchange, the Director shall—

(1) engage appropriate Federal, State, local, and nongovernmental organizations to identify, promote, and disseminate information and best practices for State educational agencies, local educational agencies, and educational service agencies with respect to cybersecurity, data protection, remote learning security, and student online privacy;

(2) maintain a database through which an elementary school, secondary school, local educational agency, State educational agency, or educational service agency may identify cybersecurity tools and services funded by the Federal Government and tools and services recommended for purchase with State and local government funding; and

(3) provide a searchable database through which covered entities may find and apply for funding opportunities to improve cybersecurity.

(c) CONSULTATION.—In carrying out the duties under subsection (b), the Director shall consult with the following:

(1) The Secretary of Education.

(2) The Director of the National Institute of Standards and Technology.

(3) The Federal Communications Commission.

(4) The Director of the National Science Foundation.

(5) The Federal Bureau of Investigation.

(6) State and local leaders, including, when appropriate, Governors, employees of State departments and agencies, members of State legislatures and State boards of education, local educational agencies, State educational agencies, representatives of Indian Tribes, teachers, principals, other school leaders, charter school leaders, specialized instructional support personnel, paraprofessionals, school administrators, other school staff, and parents.

(7) When determined appropriate by the Director, subject matter experts and expert organizations, including nongovernmental organizations, vendors of school information technology products and services, cybersecurity insurance companies, and cybersecurity threat companies.

SEC. 4. CYBERSECURITY INCIDENT REGISTRY.

(a) IN GENERAL.—The Director shall—

(1) establish, through partnerships with 1 or more Information Sharing and Analysis Organizations, a voluntary registry of information relating to cyber incidents affecting information technology systems owned or managed by a covered entity; and

(2) determine the scope of cyber incidents to be included in the registry and processes by which incidents can be reported for collection in the registry.

(b) USE.—Information in the registry established pursuant under subsection (a) may be used to—

(1) improve data collection and coordination activities related to the nationwide monitoring of the incidence and impact of cyber incidents affecting a covered entity;

(2) conduct analyses regarding trends in cyber incidents affecting a covered entity;

(3) develop systematic approaches to assist a covered entity in preventing and responding to cyber incidents;

(4) increase the awareness and preparedness of a covered entity regarding the cybersecurity of the covered entity; and

(5) identify, prevent, or investigate cyber incidents targeting a covered entity.

(c) INFORMATION COLLECTION.—

(1) IN GENERAL.—The Director may collect information relating to cyber incidents to store in the registry established pursuant to subsection (a).

(2) SUBMISSION OF INFORMATION.—Information relating to a cyber incident may be submitted by a covered entity and may include the following:

(A) The date of the cyber incident, including the date on which the incident was initially detected and the date on which the incident was first publicly reported or disclosed to another entity.

(B) A description of the cyber incident, which shall include whether the incident was as a result of a breach, malware, distributed denial of service attack, or other method designed to cause a vulnerability.

(C) The effects of the cyber incident, including descriptions of the type and size of each such incident.

(D) Other information determined relevant by the Director.

(d) REPORT.—The Director shall make available on the Information Exchange an annual report relating to cyber incidents affecting elementary schools and secondary

schools which includes data, and the analysis of such data, in a manner that—

(1) is—

(A) de-identified; and

(B) presented in the aggregate; and

(2) at a minimum, protects personal privacy to the extent required by applicable Federal and State privacy laws.

SEC. 5. K–12 CYBERSECURITY TECHNOLOGY IMPROVEMENT PROGRAM.

(a) ESTABLISHMENT.—The Director shall establish, through partnerships with 1 or more Information Sharing and Analysis Organizations, a program (to be known as the ''K–12 Cybersecurity Technology Improvement Program'') to deploy cybersecurity capabilities to address cybersecurity risks and threats to information systems of elementary schools and secondary schools through—

(1) the development of cybersecurity strategies and installation of effective cybersecurity tools tailored for covered entities;

(2) making available cybersecurity services that enhance the ability of elementary schools and secondary schools to protect themselves from ransomware and other cybersecurity threats; and

(3) providing training opportunities on cybersecurity threats, best practices, and relevant technologies for elementary schools and secondary schools.

(b) REPORT.—The Director shall make available on the Information Exchange an annual report relating to the impact of the K–12 Cybersecurity Technology Improvement Program, including information on the cybersecurity capabilities made available to information technology systems owned or managed by covered entities, the number of students served, and cybersecurity incidents identified or prevented.

SEC. 6. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this Act $10,000,000 for each of fiscal years 2023 and 2024.