

118TH CONGRESS
1ST SESSION

S. 1191

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

APRIL 19, 2023

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

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.

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 cited as the “Enhancing K–12 Cyberse-

5 curity Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) COVERED ENTITY.—The term “covered en-
2 tity” means the following:

3 (A) An elementary school.

4 (B) A secondary school.

5 (C) A local educational agency.

6 (D) A State educational agency.

7 (E) An educational service agency.

8 (2) DIRECTOR.—The term “Director” means
9 the Director of the Cybersecurity and Infrastructure
10 Security Agency.

11 (3) EDUCATIONAL SERVICE AGENCY.—The
12 term “educational service agency” has the meaning
13 given that term in section 8101 of the Elementary
14 and Secondary Education Act of 1965 (20 U.S.C.
15 7801).

16 (4) ELEMENTARY SCHOOL.—The term “elemen-
17 tary school” has the meaning given that term in sec-
18 tion 8101 of the Elementary and Secondary Edu-
19 cation Act of 1965 (20 U.S.C. 7801).

20 (5) INFORMATION EXCHANGE.—The term “In-
21 formation Exchange” means the School Cybersecu-
22 rity Information Exchange established under section
23 3(a).

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

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

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

8 (8) SECONDARY SCHOOL.—The term “sec-
 9 ondary school” has the meaning given that term in
 10 section 8101 of the Elementary and Secondary Edu-
 11 cation Act of 1965 (20 U.S.C. 7801).

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

16 **SEC. 3. SCHOOL CYBERSECURITY INFORMATION EX-**
 17 **CHANGE.**

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

1 training, and lessons learned tailored to the specific needs
2 of, technical expertise of, and resources available to cov-
3 ered entities, in accordance with subsection (b).

4 (b) DUTIES.—In establishing the Information Ex-
5 change, the Director shall—

6 (1) engage appropriate Federal, State, local,
7 and nongovernmental organizations to identify, pro-
8 mote, and disseminate information and best prac-
9 tices for State educational agencies, local educational
10 agencies, and educational service agencies with re-
11 spect to cybersecurity, data protection, remote learn-
12 ing security, and student online privacy;

13 (2) maintain a database through which an ele-
14 mentary school, secondary school, local educational
15 agency, State educational agency, or educational
16 service agency may identify cybersecurity tools and
17 services funded by the Federal Government and
18 tools and services recommended for purchase with
19 State and local government funding; and

20 (3) provide a searchable database through
21 which covered entities may find and apply for fund-
22 ing opportunities to improve cybersecurity.

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

1 (1) The Secretary of Education.

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

4 (3) The Federal Communications Commission.

5 (4) The Director of the National Science Foun-
6 dation.

7 (5) The Federal Bureau of Investigation.

8 (6) State and local leaders, including, when ap-
9 propriate, Governors, employees of State depart-
10 ments and agencies, members of State legislatures
11 and State boards of education, local educational
12 agencies, State educational agencies, representatives
13 of Indian Tribes, teachers, principals, other school
14 leaders, charter school leaders, specialized instruc-
15 tional support personnel, paraprofessionals, school
16 administrators, other school staff, and parents.

17 (7) When determined appropriate by the Direc-
18 tor, subject matter experts and expert organizations,
19 including nongovernmental organizations, vendors of
20 school information technology products and services,
21 cybersecurity insurance companies, and cybersecu-
22 rity threat companies.

23 **SEC. 4. CYBERSECURITY INCIDENT REGISTRY.**

24 (a) IN GENERAL.—The Director shall—

1 (1) establish, through partnerships with 1 or
2 more Information Sharing and Analysis Organiza-
3 tions, a voluntary registry of information relating to
4 cyber incidents affecting information technology sys-
5 tems owned or managed by a covered entity; and

6 (2) determine the scope of cyber incidents to be
7 included in the registry and processes by which inci-
8 dents can be reported for collection in the registry.

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

11 (1) improve data collection and coordination ac-
12 tivities related to the nationwide monitoring of the
13 incidence and impact of cyber incidents affecting a
14 covered entity;

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

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

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

23 (5) identify, prevent, or investigate cyber inci-
24 dents targeting a covered entity.

25 (c) INFORMATION COLLECTION.—

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

4 (2) SUBMISSION OF INFORMATION.—Informa-
5 tion relating to a cyber incident may be submitted
6 by a covered entity and may include the following:

7 (A) The date of the cyber incident, includ-
8 ing the date on which the incident was initially
9 detected and the date on which the incident was
10 first publicly reported or disclosed to another
11 entity.

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

17 (C) The effects of the cyber incident, in-
18 cluding descriptions of the type and size of each
19 such incident.

20 (D) Other information determined relevant
21 by the Director.

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

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

3 (1) is—

4 (A) de-identified; and

5 (B) presented in the aggregate; and

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

9 **SEC. 5. K-12 CYBERSECURITY TECHNOLOGY IMPROVEMENT**
10 **PROGRAM.**

11 (a) ESTABLISHMENT.—The Director shall establish,
12 through partnerships with 1 or more Information Sharing
13 and Analysis Organizations, a program (to be known as
14 the “K–12 Cybersecurity Technology Improvement Pro-
15 gram”) to deploy cybersecurity capabilities to address cy-
16 bersecurity risks and threats to information systems of el-
17 ementary schools and secondary schools through—

18 (1) the development of cybersecurity strategies
19 and installation of effective cybersecurity tools tai-
20 lored for covered entities;

21 (2) making available cybersecurity services that
22 enhance the ability of elementary schools and sec-
23 ondary schools to protect themselves from
24 ransomware and other cybersecurity threats; and

1 (3) providing training opportunities on cyberse-
2 curity threats, best practices, and relevant tech-
3 nologies for elementary schools and secondary
4 schools.

5 (b) REPORT.—The Director shall make available on
6 the Information Exchange an annual report relating to the
7 impact of the K–12 Cybersecurity Technology Improve-
8 ment Program, including information on the cybersecurity
9 capabilities made available to information technology sys-
10 tems owned or managed by covered entities, the number
11 of students served, and cybersecurity incidents identified
12 or prevented.

13 **SEC. 6. AUTHORIZATION OF APPROPRIATIONS.**

14 There are authorized to be appropriated to carry out
15 this Act \$10,000,000 for each of fiscal years 2023 and
16 2024.

○