I

117TH CONGRESS
1ST SESSION

H. R. 4005

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 17, 2021

Ms. MATSUI (for herself, Mr. KATKO, Mr. LANGEVIN, and Mr. GARBARINO) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Education and Labor, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To direct the Director of the Cybersecurity and Infrastructure Security Agency to establish a School Cybersecurity 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. SCHOOL CYBERSECURITY INFORMATION EXCHANGE.

(a) ESTABLISHMENT.—The Director of the Cybersecurity and Infrastructure Security Agency shall enhance existing information exchange efforts implemented through partnerships with one or more information sharing and analysis organizations to focus specific attention on the needs of K–12 organizations 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, technical expertise, and resources available to K–12 organizations in accordance with subsection (b).

(b) DUTIES.—In establishing the School Cybersecurity Information Exchange under subsection (a), the Director shall—

(1) engage appropriate Federal, State, local, and nongovernmental organizations to identify, promote, and disseminate information and best practices for local educational agencies, state educational agencies, and educational service agencies (as such terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801)) with respect to cybersecurity, data protec-

tion, remote learning security, and student online privacy;

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

(3) provide a searchable database for an elementary school, secondary school, local educational agency, State educational agency, and educational service agency to 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 Communication 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 government 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, administrators, other staff, and parents.

(7) When determined appropriate by the Secretary, subject-matter experts and expert organizations, including but not limited to, nongovernmental organizations, vendors of school information technology products and services, cybersecurity insurance companies, and cybersecurity threat companies.

SEC. 3. CYBERSECURITY INCIDENT REGISTRY.

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall establish, through partnerships with one 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 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 to 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 against such entity;

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

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

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

(c) INFORMATION COLLECTION.—The Director of the Cybersecurity and Infrastructure Security Agency may collect information relating to cyber incidents to store in the registry established pursuant to subsection (a). Such information may be submitted by a covered entity and may include the following:

(1) The dates of each cyber incident, including the dates on which each such incident was initially detected and the dates on which each such incident

was first publicly reported or disclosed to another entity.

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

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

(4) Other information determined relevant by the Director.

(d) REPORT.—The Director of the Cybersecurity and Infrastructure Security Agency shall make available on the School Cybersecurity Information Exchange established under section 1, 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.

(e) COVERED ENTITY DEFINED.—In this section, the term ''covered entity'' means the following:

(1) An elementary school.

(2) A secondary school.

(3) A local educational agency.

(4) A State educational agency.

(5) An educational service agency.

SEC. 4. K–12 CYBERSECURITY TECHNOLOGY IMPROVEMENT PROGRAM.

(a) ESTABLISHMENT.—The Director of the Cybersecurity and Infrastructure Security Agency, shall establish, through partnerships with one 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 K–12 organizations;

(2) making available cybersecurity services that enhance the ability of K–12 schools to protect themselves from ransomware and other cybersecurity threats; and

(3) continuing training opportunities on cybersecurity threats, best practices, and relevant technologies for K–12 schools.

(b) REPORT.—The Director of the Cybersecurity and Infrastructure Security Agency shall make available on the School Cybersecurity Information Exchange established under section 1, an annual report relating to the impact of the K–12 Cybersecurity Technology Improvement Program including but not limited to information on the cybersecurity capabilities made available to information technology systems owned or managed by elementary schools, secondary schools, local educational agencies, state educational agencies, and educational service agencies, number of students served, and cybersecurity incidents identified or prevented.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this Act under this section $10,000,000 for each of fiscal years 2022 and 2023.

SEC. 6. DEFINITIONS.

In this Act:

(1) 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).

(2) 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).

(3) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given that term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(4) 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).

(5) 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).

(6) 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).

○