Public Law 117–47
117th Congress

An Act

To establish a K–12 education cybersecurity initiative, and for other purposes.

Oct. 8, 2021
[S. 1917]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

K–12 Cybersecurity Act of 2021.
6 USC 652 note.

This Act may be cited as the "K–12 Cybersecurity Act of 2021".

SEC. 2. FINDINGS.

Congress finds the following:

(1) K–12 educational institutions across the United States are facing cyber attacks.

(2) Cyber attacks place the information systems of K–12 educational institutions at risk of possible disclosure of sensitive student and employee information, including—

(A) grades and information on scholastic development;

(B) medical records;

(C) family records; and

(D) personally identifiable information.

(3) Providing K–12 educational institutions with resources to aid cybersecurity efforts will help K–12 educational institutions prevent, detect, and respond to cyber events.

SEC. 3. K–12 EDUCATION CYBERSECURITY INITIATIVE.

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

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

(3) INFORMATION SYSTEM.—The term "information system" has the meaning given the term in section 3502 of title 44, United States Code.

(4) K–12 EDUCATIONAL INSTITUTION.—The term "K–12 educational institution" means an elementary school or a secondary school, as those terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(b) STUDY.—

Deadlines.
Evaluations.

(1) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director, in accordance with subsection (g)(1), shall conduct a study on the specific cybersecurity risks facing K–12 educational institutions that—

Analysis.

(A) analyzes how identified cybersecurity risks specifically impact K–12 educational institutions;

(B) includes an evaluation of the challenges K–12 educational institutions face in—

(i) securing—

(I) information systems owned, leased, or relied upon by K–12 educational institutions; and

(II) sensitive student and employee records; and

(ii) implementing cybersecurity protocols;

(C) identifies cybersecurity challenges relating to remote learning; and

(D) evaluates the most accessible ways to communicate cybersecurity recommendations and tools.

(2) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Director shall provide a Congressional briefing on the study conducted under paragraph (1).

Deadline. Guidelines.

(c) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after the completion of the study required under subsection (b)(1), the Director, in accordance with subsection (g)(1), shall develop recommendations that include cybersecurity guidelines designed to assist K–12 educational institutions in facing the cybersecurity risks described in subsection (b)(1), using the findings of the study.

Deadline.

(d) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the completion of the development of the recommendations required under subsection (c), the Director shall develop an online training toolkit designed for officials at K–12 educational institutions to—

(1) educate the officials about the cybersecurity recommendations developed under subsection (c); and

Strategy.

(2) provide strategies for the officials to implement the recommendations developed under subsection (c).

Web posting.

(e) PUBLIC AVAILABILITY.—The Director shall make available on the website of the Department of Homeland Security with other information relating to school safety the following:

(1) The findings of the study conducted under subsection (b)(1).

(2) The cybersecurity recommendations developed under subsection (c).

(3) The online training toolkit developed under subsection (d).

(f) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under (c) by K–12 educational institutions shall be voluntary.

(g) CONSULTATION.—

(1) IN GENERAL.—In the course of the conduction of the study required under subsection (b)(1) and the development of the recommendations required under subsection (c), the Director shall consult with individuals and entities focused on cybersecurity and education, as appropriate, including—

(A) teachers;

(B) school administrators;

(C) Federal agencies;

(D) non-Federal cybersecurity entities with experience in education issues; and

(E) private sector organizations.

(2) INAPPLICABILITY OF FACA.—The Federal Advisory Committee Act (5 U.S.C App.) shall not apply to any consultation under paragraph (1).

Approved October 8, 2021.

LEGISLATIVE HISTORY—S. 1917 (H.R. 4691):
HOUSE REPORTS: No. 117–122 (Comm. on Homeland Security) accompanying H.R. 4691.
SENATE REPORTS: No. 117–32 (Comm. on Homeland Security and Governmental Affairs).
CONGRESSIONAL RECORD, Vol. 167 (2021):
Aug. 9, considered and passed Senate.
Sept. 29, considered and passed House.

○

EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.