K-12 Cybersecurity Act of 2021

[Public Law 117–47]

[This law has not been amended]

[Currency: This publication is a compilation of the text of Public Law 117–47. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at https://www.govinfo.gov/app/collection/comps/]

[Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).]

AN ACT To establish a K-12 education cybersecurity initiative, 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. [6 U.S.C. 652 note] SHORT TITLE.

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.—

(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—

(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).

(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.

(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

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

(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).