

117TH CONGRESS
1ST SESSION

S. 1917

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

IN THE SENATE OF THE UNITED STATES

MAY 27, 2021

Mr. PETERS (for himself and Mr. SCOTT of Florida) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To establish a K–12 education cybersecurity initiative, 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 be cited as the “K–12 Cybersecurity
5 Act of 2021”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

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

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

5 (A) grades and information on scholastic
 6 development;

7 (B) medical records;

8 (C) family records; and

9 (D) personally identifiable information.

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

14 **SEC. 3. K–12 EDUCATION CYBERSECURITY INITIATIVE.**

15 (a) DEFINITIONS.—In this section:

16 (1) CYBERSECURITY RISK.—The term “cyberse-
 17 curity risk” has the meaning given the term in sec-
 18 tion 2209 of the Homeland Security Act of 2002 (6
 19 U.S.C. 659).

20 (2) DIRECTOR.—The term “Director” means
 21 the Director of Cybersecurity and Infrastructure Se-
 22 curity.

23 (3) INFORMATION SYSTEM.—The term “infor-
 24 mation system” has the meaning given the term in
 25 section 3502 of title 44, United States Code.

1 (4) K-12 EDUCATIONAL INSTITUTION.—The
 2 term “K-12 educational institution” means an ele-
 3 mentary school or a secondary school, as those terms
 4 are defined in section 8101 of the Elementary and
 5 Secondary Education Act of 1965 (20 U.S.C. 7801).

6 (b) STUDY.—

7 (1) IN GENERAL.—Not later than 120 days
 8 after the date of enactment of this Act, the Director,
 9 in accordance with subsection (g)(1), shall conduct
 10 a study on the specific cybersecurity risks facing K-
 11 12 educational institutions that—

12 (A) analyzes how identified cybersecurity
 13 risks specifically impact K-12 educational insti-
 14 tutions;

15 (B) includes an evaluation of the chal-
 16 lenges K-12 educational institutions face in—

17 (i) securing—

18 (I) information systems owned,
 19 leased, or relied upon by K-12 edu-
 20 cational institutions; and

21 (II) sensitive student and em-
 22 ployee records; and

23 (ii) implementing cybersecurity proto-
 24 cols;

1 (C) identifies cybersecurity challenges re-
2 lating to remote learning; and

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

6 (2) CONGRESSIONAL BRIEFING.—Not later than
7 120 days after the date of enactment of this Act, the
8 Director shall provide a Congressional briefing on
9 the study conducted under paragraph (1).

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

18 (d) ONLINE TRAINING TOOLKIT.—Not later than
19 120 days after the completion of the development of the
20 recommendations required under subsection (c), the Direc-
21 tor shall develop an online training toolkit designed for
22 officials at K–12 educational institutions to—

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

1 (2) provide strategies for the officials to imple-
2 ment the recommendations developed under sub-
3 section (c).

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

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

10 (2) The cybersecurity recommendations devel-
11 oped under subsection (c).

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

14 (f) VOLUNTARY USE.—The use of the cybersecurity
15 recommendations developed under (c) by K–12 edu-
16 cational institutions shall be voluntary.

17 (g) CONSULTATION.—

18 (1) IN GENERAL.—In the course of the conduc-
19 tion of the study required under subsection (b)(1)
20 and the development of the recommendations re-
21 quired under subsection (c), the Director shall con-
22 sult with individuals and entities focused on cyberse-
23 curity and education, as appropriate, including—

24 (A) teachers;

25 (B) school administrators;

1 (C) Federal agencies;

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

4 (E) private sector organizations.

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

○