

116TH CONGRESS
1ST SESSION

S. 3033

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

IN THE SENATE OF THE UNITED STATES

DECEMBER 12, 2019

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 2019”.

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 that 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 that 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 defined in
4 section 8101 of the Elementary and Secondary Edu-
5 cation Act of 1965 (20 U.S.C. 7801).

6 (b) STUDY.—

7 (1) IN GENERAL.—Not later than 1 year after
8 the date of enactment of this Act, the Director, in
9 accordance with subsection (f), shall conduct a study
10 on the cybersecurity risks facing K-12 educational
11 institutions, including the challenges K-12 edu-
12 cational institutions face in securing—

13 (A) information systems owned, leased, or
14 relied upon by K-12 educational institutions;
15 and

16 (B) sensitive student and employee re-
17 cords.

18 (2) CONGRESSIONAL BRIEFING.—Not later than
19 1 year after the enactment of this Act, the Director
20 shall provide a Congressional briefing on the study
21 required under paragraph (1).

22 (c) CYBERSECURITY RECOMMENDATIONS.—

23 (1) IN GENERAL.—Not later than 270 days
24 after the completion of the study required under
25 subsection (b)(1), the Director, in accordance with

1 subsection (f), shall develop recommendations that
2 include cybersecurity guidelines designed to assist
3 K–12 educational institutions in facing the cyberse-
4 curity risks described in subsection (b)(1), using the
5 findings of the study.

6 (2) VOLUNTARY USE.—The use of the cyberse-
7 curity recommendations developed under paragraph
8 (1) by K–12 educational institutions shall be vol-
9 untary.

10 (d) ONLINE TRAINING TOOLKIT.—Not later than 90
11 days after the completion of the development of the rec-
12 ommendations required under subsection (c)(1), the Di-
13 rector shall develop an online training toolkit designed for
14 officials at K–12 educational institutions to—

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

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

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

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

3 (2) The cybersecurity guidelines developed
4 under subsection (c)(1).

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

7 (f) CONSULTATION.—In the course of the conduction
8 of the study required under subsection (b)(1) and the de-
9 velopment of the guidelines required under subsection
10 (c)(1), the Director shall consult with entities focused on
11 cybersecurity and education, including appropriate—

12 (1) Federal agencies; and

13 (2) private sector organizations.

○