

Union Calendar No. 87

117TH CONGRESS
1ST SESSION

H. R. 4691

[Report No. 117-122]

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

IN THE HOUSE OF REPRESENTATIVES

JULY 26, 2021

Mr. LANGEVIN (for himself, Ms. MATSUI, Ms. SLOTKIN, Mr. GARBARINO, and Mr. CLYDE) introduced the following bill; which was referred to the Committee on Homeland Security

SEPTEMBER 14, 2021

Reported from the Committee on Homeland Security; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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.

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

14 (A) grades and information on scholastic
15 development;

16 (B) medical records;

17 (C) family records; and

18 (D) personally identifiable information.

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

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

24 (a) DEFINITIONS.—In this section:

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

5 (2) DIRECTOR.—The term “Director” means
6 the Director of Cybersecurity and Infrastructure Se-
7 curity.

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

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

16 (b) STUDY.—

17 (1) IN GENERAL.—Not later than 120 days
18 after the date of enactment of this Act, the Director,
19 in accordance with subsection (g)(1), shall conduct
20 a study on the specific cybersecurity risks facing K–
21 12 educational institutions that—

22 (A) analyzes how identified cybersecurity
23 risks specifically impact K–12 educational insti-
24 tutions;

1 (B) includes an evaluation of the chal-
2 lenges K–12 educational institutions face in—

3 (i) securing—

4 (I) information systems owned,
5 leased, or relied upon by K–12 edu-
6 cational institutions; and

7 (II) sensitive student and em-
8 ployee records; and

9 (ii) implementing cybersecurity proto-
10 cols;

11 (C) identifies cybersecurity challenges re-
12 lating to remote learning; and

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

16 (2) CONGRESSIONAL BRIEFING.—Not later than
17 120 days after the date of enactment of this Act, the
18 Director shall provide a congressional briefing on the
19 study conducted under paragraph (1).

20 (c) CYBERSECURITY RECOMMENDATIONS.—Not later
21 than 60 days after the completion of the study required
22 under subsection (b)(1), the Director, in accordance with
23 subsection (g)(1), shall develop recommendations that in-
24 clude cybersecurity guidelines designed to assist K–12
25 educational institutions in facing the cybersecurity risks

1 described in subsection (b)(1), using the findings of the
2 study.

3 (d) ONLINE TRAINING TOOLKIT.—Not later than
4 120 days after the completion of the development of the
5 recommendations required under subsection (c), the Direc-
6 tor shall develop an online training toolkit designed for
7 officials at K–12 educational institutions to—

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

11 (2) provide strategies for the officials to imple-
12 ment the recommendations developed under sub-
13 section (c).

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

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

20 (2) The cybersecurity recommendations devel-
21 oped under subsection (c).

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

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

4 (g) CONSULTATION.—

5 (1) IN GENERAL.—In the course of the conduc-
6 tion of the study required under subsection (b)(1)
7 and the development of the recommendations re-
8 quired under subsection (c), the Director shall con-
9 sult with individuals and entities focused on cyberse-
10 curity and education, as appropriate, including—

11 (A) teachers;

12 (B) school administrators;

13 (C) Federal agencies;

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

16 (E) private sector organizations.

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

Union Calendar No. 87

117TH CONGRESS
1ST Session

H. R. 4691

[Report No. 117-122]

A BILL

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

SEPTEMBER 14, 2021

Committed to the Committee of the Whole House on the
State of the Union and ordered to be printed