116TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

A BILL

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. SHORT TITLE.

This Act may be cited as the ''K-12 Cybersecurity Act of 2019''.

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 that 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 that 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 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 1 year after the date of enactment of this Act, the Director, in accordance with subsection (f), shall conduct a study on the cybersecurity risks facing K-12 educational institutions, including the challenges K-12 educational institutions face in securing—

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

(B) sensitive student and employee records.

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

(c) CYBERSECURITY RECOMMENDATIONS.—

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

subsection (f), 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.

(2) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under paragraph (1) by K-12 educational institutions shall be voluntary.

(d) ONLINE TRAINING TOOLKIT.—Not later than 90 days after the completion of the development of the recommendations required under subsection (c)(1), 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)(1); and

(2) provide strategies for the officials to implement the recommendations developed under subsection (c)(1).

(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 guidelines developed under subsection (c)(1).

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

(f) CONSULTATION.—In the course of the conduction of the study required under subsection (b)(1) and the development of the guidelines required under subsection (c)(1), the Director shall consult with entities focused on cybersecurity and education, including appropriate—

(1) Federal agencies; and

(2) private sector organizations.