□ 1600

K–12 CYBERSECURITY ACT OF 2021

Mr. THOMPSON of Mississippi. Madam Speaker, I move to suspend the rules and pass the bill (S. 1917) to establish a K–12 education cybersecurity initiative, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 1917

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 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).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Mississippi (Mr. THOMPSON) and the gentleman from Mississippi (Mr. GUEST) each will control 20 minutes.

The Chair recognizes the gentleman from Mississippi (Mr. THOMPSON).

GENERAL LEAVE

Mr. THOMPSON of Mississippi. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Mississippi?

There was no objection.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, in the past few weeks, millions of students have returned to school across the country. The range of public health, safety, and security risks that schools face today is truly astounding.

In recent years, schools have increasingly been subjected to ransomware attacks where cybercriminals lock networks and demand ransom payments, sometimes while threatening to release sensitive information, including students' personal data.

According to the K–12 Cybersecurity Resource Center, in 2020 alone, there were over 480 publicly disclosed cyber incidents at schools in the United States, an 18 percent increase over the previous year.

Notably, the rate of such incidents increased in the second half of last year as COVID–19 forced schools to shift to virtual learning, creating new risks, such as the disruption of online classes and online school meetings.

The impacts of ransomware attacks on schools have included the cancellation of classes, the release of sensitive information, like the name of a 9-year-old student being evaluated for a disability, and costs as high as $7.7 million for Baltimore County schools to respond to and recover from a November 2020 attack.

With many schools still operating under virtual or hybrid conditions because of the ongoing COVID–19 pandemic, the vulnerabilities to such cyberattacks are even greater.

In December, the FBI Cybersecurity and Infrastructure Security Agency, or CISA, and the Multi-State Information Sharing and Analysis Center released a joint cybersecurity advisory to alert schools to the increase in cyber threats and provide best practices on how to reduce the risk of such incidents.

To further assist K–12 schools, we must do more to help schools guard against cyber threats.

S. 1917, the K–12 Cybersecurity Act, introduced by Senator GARY PETERS from Michigan, requires CISA to conduct a study of the cybersecurity risks facing K–12 educational institutions and develop recommendations based on that study.

By developing an online training tool kit for schools, and making the study and recommendations publicly available, CISA will be able to provide schools with targeted information to better protect their networks and reduce their cybersecurity risk.

An identical version of this legislation was introduced in the House by the gentleman from Rhode Island (Mr. LANGEVIN) and cosponsored by Representatives MATSUI, SLOTKIN, GARBARINO, and CLYDE. The House measure was reported favorably by the Homeland Security Committee by voice vote in July.

Passing S. 1917 today would send this bill to the President for signature, allowing CISA to begin this important work to better secure our schools.

Mr. Speaker, I urge my colleagues to support this legislation, and I reserve the balance of my time.

Mr. GUEST. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of S. 1917, the K–12 Cybersecurity Act of 2021.

Schools around our country are increasingly the target of malicious cyber actors and have recently been targeted with a deluge of ransomware attacks.

This legislation introduced by Chairman PETERS and passed by the Senate mirrors the House version spearheaded by Representatives LANGEVIN, GARBARINO, and MATSUI.

This bill requires CISA to conduct a study to develop recommendations and provide resources regarding specific cybersecurity risks facing K–12 educational institutions. Importantly, it requires CISA to do so in consultation with teachers, schools, administrators, Federal agencies, nine Federal cybersecurity entities, and other private-sector organizations.

In doing so, the study required by this bill would help the Federal Government better support schools in defending against cyber threats.

I urge Members to join me in supporting S. 1917, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, while we are in the process of getting the sponsor of this legislation prepared to give his comments, let me say that we all have been involved in making sure that our schools are as safe as possible. Clearly, this legislation, as offered by Senator PETERS and Representative LANGEVIN and others, is integral to making sure that our schools are kept as safe as possible from cyberattacks.

Mr. Speaker, I yield 3 minutes to the gentleman from Rhode Island (Mr. LANGEVIN), the sponsor of the House version of this bill.

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding, and I commend the chairman for his strong leadership on cybersecurity issues and in support of this act before us today.

This bill, the House companion of which I sponsored with Representatives MATSUI, KATKO, and GARBARINO, would help address a serious issue that has not received the attention it deserves: the cyber threats targeting our Nation's schools.

The education of our children is clearly a critical function, yet the increasing frequency and severity of cyber threats targeting K–12 schools have jeopardized the education of students across America.

In the past 4 years, more than 1,000 educational organizations across the country have fallen victim to cybercriminals. More than 400 incidents have occurred in the past year alone. What is more, an increasing proportion of these incidents are ransomware attacks that are particularly debilitating to the operation of our schools.

Our students and educators have experienced more than enough disruption in the past year and a half. We cannot afford to let this issue continue to go unaddressed.

Many of our schools do not have the resources to counter the cyber threats that we face. Without assistance, this problem will continue to get worse, jeopardizing our students' privacy and ability to learn.

Fortunately, this Congress has already demonstrated a recognition of the government's need to provide cybersecurity assistance to entities that perform essential functions yet live below the cybersecurity poverty line, unable to defend themselves against the myriad threats they face.

It is why we took steps to invest $50 million in support for State and local government entities as part of the forthcoming reconciliation bill.

It is also why I fought to increase the budget of the Cybersecurity and Infrastructure Security Agency by more than $400 million earlier this year. I thank Chairwoman ROYBAL-ALLARD for her leadership, and I thank her team and the members of the Appropriations Committee, along with Chairman THOMPSON and his team and the members of the Homeland Security Committee.

It should also be the reason that we pass the K–12 Cybersecurity Act into law without delay.

This bill would direct the Cybersecurity and Infrastructure Security Agency to study the cybersecurity risks facing our elementary schools and secondary schools.

With a detailed understanding of the specific cybersecurity challenges facing our schools, including challenges raised by remote learning, CISA would then be required to develop cybersecurity recommendations and online training tools for educational officials at K–12 institutions. Our educators and administrators would be equipped with the knowledge they need to better defend themselves against cyber threats and keep our schools safe for our students.

Mr. Speaker, I thank Representative MATSUI for her tireless attention to this issue and Representatives GARBARINO, SLOTKIN, and CLYDE for joining us in advancing this legislation. I recognize the efforts of my colleagues in the Senate, Senator PETERS and Senator SCOTT, who deftly shepherded this bill through their Chamber. Finally, I recognize my good friend, Chairman BENNIE THOMPSON, for ensuring this bill received the consideration it deserves.

Mr. Speaker, I urge my colleagues to support this important legislation.

Mr. GUEST. Mr. Speaker, I urge all Members to support this bill, and I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself the balance of my time.

With sophisticated cybercriminals operating overseas launching ransomware attacks on our schools, it is essential that the Federal Government step up efforts to support the cybersecurity of our schools.

Without more assistance, many of our Nation's school districts will continue to be vulnerable, as many lack the cyber expertise to defend against these incidents.

Enactment of the K–12 Cybersecurity Act would enhance the technical support provided by CISA to schools to help better protect school IT networks.

Mr. Speaker, I urge my colleagues to support S. 1917, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. CUELLAR). The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, S. 1917.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

HOMELAND SECURITY FOR CHILDREN ACT

Mr. THOMPSON of Mississippi. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4426) to amend the Homeland Security Act of 2002 to ensure that the needs of children are considered in homeland security planning, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4426

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 ''Homeland Security for Children Act''.

SEC. 2. RESPONSIBILITIES OF SECRETARY OF HOMELAND SECURITY.

Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended by adding at the end of the following new subsection:

''(h) PLANNING REQUIREMENTS.—The Secretary shall ensure the head of each office and component of the Department takes into account the needs of children, including children within under-served communities, in mission planning and mission execution. In furtherance of this subsection, the Secretary shall require each such head to seek, to the extent practicable, advice and feedback from organizations representing the needs of children. The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply whenever such advice or feedback is sought in accordance with this subsection.''.

SEC. 3. TECHNICAL EXPERT AUTHORIZED.

Paragraph (2) of section 503(b) of the Homeland Security Act (6 U.S.C. 313(b)) is amended—

(1) in subparagraph (G), by striking ''and'' at the end;

(2) in subparagraph (H), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new subparagraph:

''(I) identify, integrate, and implement the needs of children, including children within under-served communities, into activities to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other disasters, including catastrophic incidents, including by appointing a technical expert, who may consult with relevant outside organizations and experts, as necessary, to coordinate such integration, as necessary.''.

SEC. 4. REPORT.

Not later than one year after the date of the enactment of this Act and annually thereafter for five years, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure