117TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
117–122

K–12 CYBERSECURITY ACT OF 2021

SEPTEMBER 14, 2021.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 4691]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4691) to establish a K–12 education cybersecurity initiative, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 4691, the "K–12 Cybersecurity Act" requires the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a study of the cybersecurity risks facing K–12 educational institutions, in consultation with teachers, school administrators, other Federal

agencies, and private sector organizations. The bill further directs CISA to develop recommendations based on this study, including cybersecurity guidelines for K–12 educational institutions and an online training toolkit with information on the guidelines and how to implement them. Additionally, the bill requires CISA to make the study, recommendations, and online toolkit publicly available on the Department of Homeland Security's (DHS) website.

BACKGROUND AND NEED FOR LEGISLATION

K–12 educational institutions have experienced an increasing number of cyber incidents in recent years. According to one report, in 2020, there were 408 publicly disclosed cyber incidents at schools in the United States, an 18 percent increase over the prior year and the highest level since the tracking of incidents began in 2016.[1] Additionally, the number of incidents was higher in the second half of 2020, as many schools were operating remotely due to the COVID–19 pandemic, creating new cyber risks, including disruptions to online classes and online school meetings.[2] The Multi-State Information Sharing and Analysis Center (MS-ISAC) projects the number of K–12 cyber incidents could increase by 86 percent in 2021.[3] The Federal Government has recognized this growing threat, and in December 2020, CISA, the MS-ISAC, and the Federal Bureau of Investigation (FBI) released a Joint Cybersecurity Advisory detailing the cyber threats to K–12 educational institutions and providing best practices to protect against cyber incidents.[4]

Cyber incidents at K–12 educational institutions can have a major impact on schools' ability to operate, can cause significant financial losses, and can put at risk student and employee privacy. For example, after the Broward County School District in Florida refused to pay a $40 million ransom demand, the ransomware group Conti posted 26,000 files online, including the name of a 9-year-old student being evaluated for a disability.[5] In another incident, Haverhill Public Schools in Massachusetts were forced to close for a day, canceling remote classes and delaying the return of in-person instruction for some grades due a ransomware attack that disrupted the districts' networks.[6] Furthermore, in November 2020, a ransomware incident shut down Baltimore County schools for two days for 111,000 students and cost the district at least $7.7 million to respond and recover from the attack.[7]

---

[1] Douglas A. Levin, *The State of K–12 Cybersecurity: 2020 Year in Review*, EdTech Strategies/K–12 Cybersecurity Resource Center and the K12 Security Information Exchange, (March 10, 2021), p. 3, Available at https://k12cybersecure.com/year-in-review/.

[2] *Id.*

[3] Joseph Marks, "The Cybersecurity 202: Schools Are Another Prime Ransomware Target," *The Washington Post*, (July 12, 2021), Available at https://www.washingtonpost.com/politics/2021/07/12/cybersecurity-202-schools-are-another-prime-ransomware-target/.

[4] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Multi-State Information Sharing and Analysis Center, *Cyber Actors Target K–12 Distance Learning Education to Cause Disruptions and Steal Data*, (Dec. 10, 2020), Available at https://us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf.

[5] Scott Travis, "Hackers Post 26,000 Broward School Files Online," *South Florida Sun-Sentinel*, (April 19, 2021), Available at https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hackers-post-files-20210419-mypt2qtlc5a7xela4x6bcg5hdy-story.html.

[6] Mike LaBella, "Haverhill Schools Hit by Ransomware," *The Eagle-Tribune*, (April 7, 2021), Available at https://www.eagletribune.com/news/haverhill/haverhill-schools-hit-by-ransomware/article_763617ee-9735-5f74-82f8-9ddbe38ec363.html.

[7] Lillian Reed, "Cost of Ransomware Attack on Baltimore County Public Schools Climbs to $7.7M," *The Baltimore Sun*, (June 11, 2021), Available at https://www.baltimoresun.com/edu-

To assist K–12 educational institutions' efforts to enhance their cybersecurity, the "K–12 Cybersecurity Act" 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 toolkit for schools, and making the study and recommendations publicly available, CISA will be able to provide K–12 educational institutions with information they can use to better protect their networks and reduce their cybersecurity risk.

The Senate Homeland Security and Governmental Affairs Committee favorably reported an identical bill authored by Senator Gary C. Peters of Michigan, S. 1917, by voice vote on July 14, 2021. It passed the Senate by unanimous consent on August 9, 2021.

HEARINGS

For the purposes of clause 3(c)(6) of rule XIII of the Rules of the House of Representatives, the following hearing was used to develop H.R. 4691:

The Committee did not hold a legislative hearing on H.R. 4691 in the 117th Congress. However, the legislation was informed by an oversight hearing on May 5, 2021. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled, "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis." The Subcommittee received testimony from Maj. Gen. John Davis (Ret.), Vice President and Federal Chief Security Officer at Palo Alto Networks; Ms. Megan Stifel, Executive Director, Americas at the Global Cyber Alliance; Mr. Denis Goulet, Commissioner, Department of Information Technology and Chief Information Officer, State of New Hampshire (on behalf of the National Association of State Chief Information Officers); and Mr. Christopher Krebs, former Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

COMMITTEE CONSIDERATION

The Committee met on July 28, 2021, a quorum being present, to consider H.R. 4691 and ordered the measure to be favorably reported to the House, without amendment, by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 4691.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

---

cation/bs-md-ransomware-cost-schools-20210609-20210611-6fipdck3h5b5peli6vgbgfsqyy-story.html.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 10, 2021.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4691, the K–12 Cybersecurity Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 4691, K-12 Cybersecurity Act of 2021
As ordered reported by the House Committee on Homeland Security on July 28, 2021

By Fiscal Year, Millions of Dollars	2021	2021-2026	2021-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	*	not estimated

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 4691 would require the Cybersecurity and Infrastructure Security Agency (CISA) to study cybersecurity challenges that are unique to primary and secondary schools, such as safeguarding student records and securing remote-learning technology. The bill also would require CISA to make available on a public website its recommendations on how schools can mitigate cybersecurity threats and vulnerabilities.

On the basis of information from CISA about the costs of similar activities, CBO estimates that staff salaries and other expenses to

produce the required study and recommendations would be less than $500,000 over the 2021–2026 period. Such spending would be subject to the availability of appropriations.

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2021. Under that assumption, CISA could incur some costs in 2021, but CBO expects that most of the costs would be incurred in 2022 and later.

On July 21, 2021, CBO transmitted a cost estimate for S. 1917, the K–12 Cybersecurity Act of 2021, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 14, 2021. The two bills are similar, and CBO's estimates of their costs are the same.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 4691 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 4691 is to direct the Cybersecurity and Infrastructure Security Agency to study the specific cybersecurity risks facing K–12 educational institutions and to develop cybersecurity recommendations to assist K–12 educational institutions in securing their information systems and records.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS ADVISORY COMMITTEE STATEMENT

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 4691 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section states that the Act may be cited as the "K–12 Cybersecurity Act of 2021".

Sec. 2. Findings.

This section provides congressional findings that K–12 educational institutions in the United States are facing cyber attacks, that these cyber attacks put at risk the disclosure of sensitive student and employee information, and that providing resources to K–12 educational institutions will help them prevent, detect, and respond to cyber events.

Sec. 3. K–12 Education Cybersecurity Initiative.

Subsection (a) defines the terms "cybersecurity risk," "director," "information system," and "K–12 educational institutions."

Subsection (b) directs the CISA Director to conduct a study within 120 days on the cybersecurity risks facing K–12 educational institutions. The study will consider how cybersecurity risks impact K–12 educational institutions and will evaluate the challenges K–12 educational institutions face in securing systems and records and in implementing cybersecurity protocols. It will also identify the cybersecurity challenges in remote learning and will evaluate the most accessible ways to communicate cybersecurity recommendations and tools. The Committee expects the study to consider the unique cybersecurity risks facing rural and small K–12 educational institutions. Within 120 days of enactment, CISA must brief Congress on its findings.

Subsection (c) requires the CISA Director to develop, within 60 days of the study's completion, recommendations based on the study, including cybersecurity guidelines for K–12 educational institutions.

Subsection (d) requires the CISA Director to develop, within 120 days of the completion of the development of the recommendations, an online training toolkit for K–12 educational institutions to assist in implementing the recommendations.

Subsection (e) requires the CISA Director to make the findings of the study, the cybersecurity recommendations, and the online training toolkit publicly available on the Department of Homeland Security's website.

Subsection (f) clarifies that use of the cybersecurity recommendations is voluntary.

Subsection (g) directs the CISA Director to consult with teachers, school administrators, Federal agencies, non-Federal cybersecurity agencies with experience in education issues, and private sector organizations while conducting the required study and developing the cybersecurity recommendations. It also exempts those consultations from the Federal Advisory Committee Act.

○