

Calendar No. 107

117TH CONGRESS }
1st Session }

SENATE

{ REPORT
117-32

K-12 CYBERSECURITY ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 1917

TO ESTABLISH A K-12 EDUCATION CYBERSECURITY
INITIATIVE, AND FOR OTHER PURPOSES



JULY 26, 2021.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

19-010

WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

CHRISTOPHER J. MULKINS, *Director of Homeland Security*

KATIE A. CONLEY, *Professional Staff Member*

PAMELA THIESSEN, *Minority Staff Director*

ANDREW C. DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*

CARA G. MUMFORD, *Minority Professional Staff Member*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 107

117TH CONGRESS }
1st Session }

SENATE

{ REPORT
117-32

K-12 CYBERSECURITY ACT OF 2021

JULY 26, 2021.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and
Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 1917]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1917) 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

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	3
IV. Section-by-Section Analysis of the Bill, as Reported	3
V. Evaluation of Regulatory Impact	4
VI. Congressional Budget Office Cost Estimate	4
VII. Changes in Existing Law Made by the Bill, as Reported	5

I. PURPOSE AND SUMMARY

S. 1917, the K-12 Cybersecurity Act of 2021, provides cybersecurity guidance to K-12 educational institutions across the United States. It directs the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a study of cybersecurity risks and challenges facing schools. Following completion of the study, the bill directs CISA to use the findings to create a set of cybersecurity recommendations and an online toolkit for educational institutions. The bill also instructs CISA to consult with teachers, school administrators, Federal agencies, non-Federal cybersecurity entities, and private sector organizations when conducting the study and developing the recommendations and online

toolkit and exempts such consultation from the Federal Advisory Committee Act.

Additionally, S. 1917 requires CISA to make the findings of the study, its cybersecurity recommendations, and the online toolkit publicly available on the Department of Homeland Security (DHS) website. Finally, S. 1917 specifies that these K–12 cybersecurity recommendations are voluntary.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Like other sectors, cyber attacks on K–12 educational institutions are increasing.¹ There were more than 408 publicly disclosed cyber attacks on schools in 2020, an 18 percent increase from 2019, which is a rate of more than two incidents per school day.² Reports of cyber attacks in the beginning of the 2020 school year led the Federal Bureau of Investigation, CISA, and the Multi-State Information Sharing and Analysis Center to issue a Joint Cybersecurity Advisory.³ The impacts on schools that face attacks can be severe⁴ and pervasive;⁵ for example, a series of ransomware attacks in Louisiana in 2019 led the Governor to declare a state-wide emergency.⁶ The COVID–19 pandemic and the shift to remote learning exacerbated this trend, making schools more vulnerable and creating new challenges.⁷

School systems contain significant quantities of personal information on students and staff, including academic records, medical information, financial information, as well as personally identifiable information like social security numbers.⁸ Cyber attacks risk unauthorized access to these records and ransomware attacks can force school closures and class cancellations for days and disrupt school system operation.⁹ Despite these significant challenges, many districts may not have the dedicated staff or resources necessary to identify and implement solutions.¹⁰ Organizations representing teachers, school administrators, and school technology advocates across the country have expressed support for S. 1917 to better understand the challenges schools face and use that informa-

¹See Douglas A. Levin, K–12 Cybersecurity Research Center and the K–12 Security Information Exchange, *The State of K–12 Cybersecurity: 2020 Year in Review*, at 3 (Mar. 10, 2021).

²See *id.*

³See 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) (us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf) (hereinafter “Cybersecurity Advisory”).

⁴See, e.g., *FBI, Michigan State Police Investigating Cyber Attack on Saginaw Township Schools*, ABC 12 News (Feb. 25, 2021) (<https://www.abc12.com/2021/02/25/fbi-state-police-probing-cyber-hack-on-saginaw-township-schools/>).

⁵Senate Subcommittee on Federal Spending Oversight and Emergency Management, Testimony Submitted for the Record of Dr. Leslie Torres-Rodriguez, Superintendent, Hartford Public Schools, *State and Local Cybersecurity: Defending Our Communities from Cyber Threats Amid COVID–19*, 116th Cong., at 1 (Dec. 2, 2020) (S. Hrg. 116–461) (describing a ransomware attack on Hartford, Connecticut public schools as “extremely disruptive” and resulting in postponement of the first day of school) (hereinafter “Torres-Rodriguez Testimony”).

⁶See *Louisiana Declares State Emergency After Cyberattacks on School Districts*, The Hill (July 26, 2019) (<https://thehill.com/homenews/state-watch/454928-louisiana-declares-state-emergency-after-cyber-attacks-on-school>).

⁷See Levin, *supra* note 1, at 4; see also Cybersecurity Advisory, *supra* note 3, at 1.

⁸See Government Accountability Office, *Data Security: Recent K–12 Data Breaches Show That Students are Vulnerable to Harm*, at 12 (GAO 20–644) (Sept. 15, 2020).

⁹See *State and Local Cybersecurity*, *supra* note 5, at 19 (describing a ransomware attack on Hartford, Connecticut public schools as “extremely disruptive” and resulting in postponement of the first day of school).

¹⁰See *Hackers Latest Target: School Districts*, New York Times (July 28, 2019) (<https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html>).

tion to develop and make available tailored tools to help schools improve their cyber posture.¹¹

S. 1917 addresses the rising risk of cyber attacks by requiring CISA to study specific cybersecurity challenges K–12 educational institutions face and to create tailored resources that schools can use to improve cyber hygiene. First, the bill directs CISA to conduct a study, in consultation with teachers, school administrators, other Federal agencies, and the private sector on the specific cybersecurity risks facing K–12 educational institutions. S. 1917 also requires the results of that study to be shared with Congress and posted publicly. Finally, the bill directs CISA to develop voluntary cybersecurity recommendations in response to the findings of the study and develop an online, publicly available cybersecurity training toolkit to educate school officials on implementing those recommendations.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 1917, the K–12 Cybersecurity Act of 2021, on May 27, 2021, with Senator Scott (R–FL). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. Senators Rosen (D–NV) and Cassidy (R–LA) later joined as cosponsors on June 21, 2021. The Committee considered S. 1917 at a business meeting on July 14, 2021. The Committee ordered the bill reported favorably without amendment *en bloc* by voice vote. Senators present for the vote were: Peters, Hassan, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the name of the bill as the “K–12 Cybersecurity Act of 2021.”

Section 2. Findings

This section identifies congressional findings that K–12 educational institutions are facing cyber attacks and that cyber attacks place the information systems of those institutions at risk of possibly disclosing sensitive student and employee information. This section also finds that providing resources to K–12 educational institutions will help schools prevent, detect, and respond to cyber attacks.

Section 3. Education cybersecurity initiative

Subsection (a) defines the terms “cybersecurity risk,” “director,” “information system,” and “K–12 educational institution.”

Subsection (b) provides that, within 120 days of enactment, the Director of CISA will conduct a study analyzing how cybersecurity risks specifically impact schools. This study will evaluate the challenges that schools face in securing their information systems and sensitive student and employee records, as well as the challenges

¹¹See Senators Gary Peters, Rick Scott: *Peters, Scott Reintroduce Bipartisan Legislation to Help Protect K–12 School Systems from Cyberattacks* (May 27, 2021) (<https://www.hsgac.senate.gov/media/majority-media/peters-scott-reintroduce-bipartisan-legislation-to-help-protect-k-12-school-systems-from-cyber-attacks>).

they face in implementing cybersecurity protocols. The study will also identify cybersecurity challenges to remote learning, and evaluate the most accessible ways to communicate cybersecurity recommendations and tools. Within 120 of enactment, CISA must provide a briefing to Congress on this study.

Subsection (c) requires CISA to develop, within 60 days after completion of the study in subsection (b), recommendations for addressing cybersecurity risks in schools using the findings of the study.

Subsection (d) requires CISA to create, within 120 days after the development of the recommendations in subsection (c), an online training toolkit to educate school officials on the recommendations and provide implementation strategies for those recommendations.

Subsection (e) requires CISA to publicly post the findings of the study, the recommendations developed by CISA, and the online training toolkit on DHS' website, co-located with other school safety information.

Subsection (f) establishes that the recommendations in subsection (c) are voluntary.

Subsection (g) directs CISA to consult with teachers, school administrators, Federal agencies, non-Federal cybersecurity entities, and private sector organizations to assist with the study and the development of the recommendations required by subsection (c) and exempts those consultations from the Federal Advisory Committee Act.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 21, 2021.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1917, 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.

S. 1917, K-12 Cybersecurity Act of 2021			
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 14, 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.			

S. 1917 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.

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

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.