

CYBERSECURITY GRANTS FOR SCHOOLS ACT OF 2022

MAY 13, 2022.—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. 6868]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 6868) to amend the Homeland Security Act of 2002 to provide for financial assistance to fund certain cybersecurity and infrastructure security education and training programs and initiatives, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	2
Background and Need for Legislation	2
Hearing	3
Committee Consideration	4
Committee Votes	4
Committee Oversight Findings	5
C.B.O. Estimate, New Budget Authority, Entitlement Authority, and Tax Expenditures	5
Federal Mandates Statement	x
Duplicative Federal Programs	x
Statement of General Performance Goals and Objectives	x
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	x
Advisory Committee Statement	x
Applicability to Legislative Branch	x
Section-by-Section Analysis of the Legislation	x
Changes in Existing Law Made by the Bill, as Reported	x

The amendment is as follows:

Strike out all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “Cybersecurity Grants for Schools Act of 2022”.

SEC. 2. STRENGTHENING CYBERSECURITY EDUCATION SUPPORT.

(a) **IN GENERAL.**—Section 2220 of the Homeland Security Act of 2002 (6 U.S.C. 665f) is amended by adding at the end the following new subsection:

“(e) **GRANTS AND COOPERATIVE AGREEMENTS.**—The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

“(1) carry out the purposes of CETAP; and

“(2) enhance CETAP to address the national shortfall of cybersecurity professionals.”

(b) **BRIEFINGS.**—Paragraph (2) of subsection (c) of section 2220 of the Homeland Security Act of 2002 (6 U.S.C. 665f) is amended—

(1) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E) respectively; and

(2) by inserting after subparagraph (B) the following new subparagraph:

“(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;”.

PURPOSE AND SUMMARY

H.R. 6868, the “Cybersecurity Grants for Schools Act of 2022,” authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to provide grants or cooperative agreements to States, local governments, institutions of higher education, nonprofit organizations, and other non-Federal entities to carry out the purposes of the Cybersecurity Education and Training Assistance Program (CETAP), as authorized last year.¹ CETAP’s purpose is to support CISA’s efforts to build and strengthen “a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education.”² To further the CETAP program, this legislation grants CISA the authority to provide grants to organizations to carry out the program to help enhance cybersecurity education at the elementary and secondary levels.

BACKGROUND AND NEED FOR LEGISLATION

Cybersecurity expertise is a critical component of national security; however, the U.S. has struggled to cultivate a cybersecurity talent pipeline, develop academic curriculum, and promote awareness and interest among potential job candidates.

The cybersecurity workforce shortage is a global problem. Research conducted by (ISC)², the world’s largest nonprofit association of cybersecurity professionals, estimates there is gap of 3.1 million between the number of skilled professionals needed and the number individuals trained to perform that work.³ According to National Institute for Standards and Technology (NIST)-funded research, in the U.S. alone, there is a deficit of 464,420 cybersecurity employees; this is a sizable gap considering that the total employed in the U.S. cyber workforce is just 956,341.⁴

¹ Pub. L. 116–283, § 1719 (2021).

² *Id.*

³ “Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study, 2000,” (ISC)², available at <https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx>.

⁴ “Cybersecurity Supply/Demand Heat Map,” CyberSeek, (accessed July 25, 2021), available at <https://www.cyberseek.org/heatmap.html>.

Moreover, the demographic composition of the cybersecurity workforce lacks the diversity of the U.S. population. A 2018 deep-dive analysis of the gender, age, tenure, ethnicity, and race of the U.S. cyber workforce, carried out by the International Information System Security Certification Consortium, (ISC)², and the International Consortium of Minority Cybersecurity Professionals, found that women comprised just 11 percent of the workforce and that African Americans and Hispanic Americans accounted for 9 and 4 percent respectively.⁵ In 2019, (ISC)² expanded the scope of the survey beyond traditional cybersecurity professionals to IT professionals who spend at least 25 percent of their time on cybersecurity. In that survey, some of these statistical averages seemed to increase (e.g., women in cybersecurity jumped to 24 percent), but (ISC)² concluded that the change may be linked more to methodological differences between surveys than an increase in the number of women in the field.⁶ These numbers demonstrate that, despite the range of government- and industry-driven initiatives to grow the cybersecurity workforce, many talent pipelines remain untapped.

Other factors may be exacerbating the shortage of cybersecurity expertise, such as the relative difficulty of teaching cybersecurity in a classroom, the shortage of teachers who are able to confidently teach cybersecurity to students, and the daunting task, particularly in higher education, of constantly updating curriculum and syllabi to keep pace with a rapidly changing field.⁷ At the K–12 level, a 2020 survey found that fewer than half of the participating districts and schools had cybersecurity education programs and that rural and low-income school districts were less likely to have cybersecurity education resources for students.⁸

To address the long-standing struggles to grow the cyber talent pipeline, CISA launched CETAP to deliver free cybersecurity, STEM, and computer science curricula and resources to K–12 educators. H.R. 6868 would enhance participation in CETAP by authorizing the CISA Director to award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher learning, nonprofit organizations, and other non-Federal entities for the purpose of funding cybersecurity and infrastructure security education, training programs, and initiatives.

HEARING

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. 6868:

⁵Jason Reed and Jonathan Acosta-Rubio, “Innovation Through Inclusion: The Multicultural Cybersecurity Workforce,” Frost & Sullivan (with (ISC)², the International Consortium of Minority Professionals, and the Center for Cyber Safety and Education), (2018), available at <https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx>.

⁶“Women in Cybersecurity: Young, Educated and Ready to Take Charge,” (ISC)², (2019), available at <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx>.

⁷Laura Bate, “Cybersecurity Workforce Development: A Primer,” New America, (Nov. 1, 2018), available at <https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/>.

⁸“The State of Cybersecurity Education in K–12 Schools,” EdWeek Research Center and CYBER.ORG, (2020), available at <https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf>.

• On July 29, 2021, the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled “The Cyber Talent Pipeline: Educating a Workforce to Match Today’s Threats.” The Subcommittee received testimony from Mr. Kevin Nolten, Director of Academic Outreach at CYBER.ORG; Dr. Tony Coulson, Executive Director of the Cybersecurity Center and Lead at the National Centers of Academic Excellence in Cybersecurity Community, California State University, San Bernardino; Mr. Ralph Ley, Department Manager of National and Homeland Security Workforce Development and Training at the Idaho National Laboratory; and Mr. Max Stier, President and CEO, Partnership for Public Service.

COMMITTEE CONSIDERATION

The Committee met on March 2, 2022, a quorum being present, to consider H.R. 6868 and ordered the measure to be favorably reported to the House, as amended, by a recorded vote of 33–0.

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.

1. A motion by Mr. Cleaver to favorably report H.R. 6824, H.R. 6868, and H.R. 6873, as amended, en bloc, to the House was agreed to by a recorded vote of 33 ayes to 0 noes (Rollcall No. 32).

Committee Rollcall No. 32

Motion by Mr. Cleaver to Favorably Report H.R. 6824, H.R. 6868, and H.R. 6873, As Amended, En Bloc
Agreed to: 33 ayes to 0 noes

Majority Members	Vote	Minority Members	Vote
Ms. Jackson Lee	Mr. Katko	Aye
Mr. Langevin	Aye	Mr. McCaul
Mr. Payne	Aye	Mr. Higgins (LA)	Aye
Mr. Correa	Aye	Mr. Guest	Aye
Ms. Slotkin	Aye	Mr. Bishop (NC)	Aye
Mr. Cleaver	Aye	Mr. Van Drew	Aye
Mr. Green (TX)	Aye	Mr. Norman	Aye
Ms. Clarke (NY)	Aye	Mrs. Miller-Meeks	Aye
Mr. Swalwell	Aye	Mrs. Harshbarger	Aye
Ms. Titus	Aye	Mr. Clyde	Aye
Mrs. Watson Coleman	Aye	Mr. Gimenez	Aye
Miss Rice (NY)	Aye	Mr. LaTurner	Aye
Mrs. Demings	Aye	Mr. Meijer	Aye
Ms. Barragán	Aye	Mrs. Cammack	Aye
Mr. Gottheimer	Aye	Mr. Pfluger	Aye
Mrs. Luria	Aye	Mr. Garbarino	Aye

Committee Rollcall No. 32—Continued

Motion by Mr. Cleaver to Favorably Report H.R. 6824, H.R. 6868, and H.R. 6873, As Amended, En Bloc
 Agreed to: 33 ayes to 0 noes

Majority Members	Vote	Minority Members	Vote
Mr. Malinowski	Aye		
Mr. Torres (NY)	Aye		
Mr. Thompson (MS), Chairman.	Aye		

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.

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, April 27, 2022.

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. 6868, the Cybersecurity Grants for Schools Act of 2022.

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

Sincerely,

PHILLIP L. SWAGEL,
 Director.

Enclosure.

H.R. 6868, Cybersecurity Grants for Schools Act of 2022			
As ordered reported by the House Committee on Homeland Security on March 2, 2022			
By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
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. 6868 would authorize the Cybersecurity and Infrastructure Security Agency (CISA) to award grants to cyber education and training programs. The bill also would require the agency to report to the Congress on the effectiveness of its efforts.

CISA is already providing the grants that would be authorized under H.R. 6868 through the Cybersecurity Education and Training Assistance Program; thus, the bill would codify those responsibilities and would not impose any new grant requirements on the agency.

The agency could expand a report provided under current law to satisfy the new reporting requirement in the bill. CBO estimates that doing so would cost less than \$500,000 over the 2022–2026 period; such spending would be subject to the availability of appropriated funds.

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. 6868 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. 6868 is to enhance CISA's ability to support cybersecurity education programs and grow the cybersecurity talent pipeline.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED
TARIFF BENEFITS

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.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 6868 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 “Cybersecurity Grants for Schools Act of 2022”.

Sec. 2. Strengthening cybersecurity education support.

This section authorizes the CISA Director to award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher learning, nonprofit organizations, and other non-Federal entities for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to carry out the purposes of CETAP and enhance CETAP to address the national shortfall of cybersecurity professionals.

This section also amends the Secretary of Homeland Security’s obligations to brief relevant congressional committees about CETAP’s activities and requires such briefings to include information on any grants or cooperative agreements entered into, including how any such grants or cooperative agreements are being used to enhance cybersecurity education in underserved populations or communities.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * *

SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS..

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Cybersecurity Education and Training Assistance Program (referred to in this section as “CETAP”) is established within the Agency.

(2) PURPOSE.—The purpose of CETAP shall be to support the effort of the Agency in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

(A) providing foundational cybersecurity awareness and literacy;

(B) encouraging cybersecurity career exploration; and

(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) REQUIREMENTS.—In carrying out CETAP, the Director shall—

(1) ensure that the program—

(A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

(D) provides direct student engagement opportunities through camps and other programming;

(E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(F) integrates with existing post-secondary education and workforce development programs at the Department;

(G) promotes and supports national standards for elementary and secondary cyber education;

(H) partners with cybersecurity and education stakeholder groups to expand outreach; and

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

(2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) BRIEFINGS.—

(1) IN GENERAL.—Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) CONTENTS.—Each briefing conducted under paragraph (1) shall include—

(A) estimated figures on the number of students reached and teachers engaged;

(B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);

(C) *information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;*

[(C)] (D) information on new curricula offerings and teacher training platforms; and

[(D)] (E) information on coordination with post-secondary education and workforce development programs at the Department.

(d) MISSION PROMOTION.—The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

(e) GRANTS AND COOPERATIVE AGREEMENTS.—*The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—*

(1) carry out the purposes of CETAP; and

(2) enhance CETAP to address the national shortfall of cybersecurity professionals.

* * * * *