Calendar No. 256

117TH CONGRESS *2d Session*	SENATE	REPORT 117–59

CYBERSECURITY OPPORTUNITY ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2305

TO ENHANCE CYBERSECURITY EDUCATION

JANUARY 20, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
29–010 WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
MICHAEL A. GARCIA, *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. 256

117TH CONGRESS *2d Session* | SENATE | REPORT 117–59

CYBERSECURITY OPPORTUNITY ACT

JANUARY 20, 2022.—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. 2305]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2305) to enhance cybersecurity education, having considered the same, reports favorably with an amendment (in the nature of a substitue) and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2305, the Cybersecurity Opportunity Act, authorizes the Department of Homeland Security (DHS) to enhance the nation's cybersecurity workforce by awarding grants to establish or expand cybersecurity programs at institutions of higher education that serve a high proportion of Pell Grant-receiving students, Historically Black Colleges and Universities (HBCUs), and other minority-serving institutions. Eligible applicants can use these grants to build and improve institutional capacity to support new or existing cybersecurity programs, provide hands-on cybersecurity research and training experiences, and strengthen public-private partnerships to further cybersecurity research, training, and educational

opportunities. These grants will also help institutions qualify to be designated a National Center of Academic Excellence in Cybersecurity.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Some estimates put the nation at having roughly half-a-million vacant cybersecurity jobs.[1] However, the Homeland Security and Commerce Departments found that it is difficult to place an accurate number on the amount of vacant cybersecurity positions as "reliable, quantitative information about the cybersecurity workforce is lacking."[2] Yet, despite the lack of a concrete figure, DHS and the Commerce Department concluded that "there is a real need for improvement in the U.S. cybersecurity workforce's development and that today's situation warrants both immediate and sustained attention."[3]

The lack of cybersecurity professionals is a challenge that pervades federal, local, and private organizations, which harms their cybersecurity posture. While government and private organizations have initiated programs to educate, train, and recruit personnel, individuals from underrepresented groups—such as women, people of color, and other minorities—continue to comprise a small portion of the cybersecurity workforce.[4] Although public data is limited regarding the diversity of the cybersecurity workforce, broader federal workforce demographics show that minority groups and women remain underrepresented.[5] For instance, Black and Latin employees make up less than 20 percent of the Federal Bureau of Investigation's (FBI) workforce, and women comprise only a third of the DHS workforce.[6] The lack of a diverse, equitable, and inclusive workforce could be detrimental to organizations as "diverse workforces produce better outcomes and more informed decision-making."[7]

DHS and the Department of Commerce identified the task of creating a diverse, equitable, and inclusive workforce as a key priority in their joint report on *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce.*[8] They found that "a successful cybersecurity workforce strategy for the Nation should include an enhanced focus upon the value of diversity and inclusion and convert it into a potent resource that can be used to great advantage. Fostering and sustaining a diverse workforce will support the ability to find new talent to carry out this effort and to uncover novel ways to solve problems."[9] They recommend that the federal

---

[1] *See* Cyber Seek, Home Page (https://www.cyberseek.org/index.html#aboutit) (accessed Dec. 9, 2021).

[2] *See* National Institute of Standards and Technology, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, at 23 (Jul. 24, 2018) (https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf) (hereinafter "NIST").

[3] *See Id.* at 24.

[4] *See Id.* at 29.

[5] NIST did, however, find that "In comparison to the national workforce, minorities and women are underrepresented among those working in cybersecurity." *See Id*. at 26.

[6] *See* Federal Bureau of Investigation, *Diversity at the FBI* (https://www.fbijobs.gov/working-at-FBI/diversity) (accessed Dec. 9, 2021); and US Department of Homeland Security, *EEO Diversity Management* (https://www.dhs.gov/dhs-diversity-planning) (accessed Dec. 9, 2021).

[7] *See* Third Way, *A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?* (Nov. 12, 2020) (https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here).

[8] *See* NIST, *supra* note 2.

[9] *See Id*. at 4.

government recruit cybersecurity workers from "large and diverse pools of candidates who are underutilized or underrepresented in the cybersecurity workforce." [10]

DHS is uniquely situated to identify the nation's cybersecurity needs and to bolster its cybersecurity workforce. The Cybersecurity and Infrastructure Security Agency (CISA), a component of the Department, is the lead federal civilian agency responsible for protecting the homeland against cyber threats, and Congress has recognized CISA's critical role in cybersecurity education by authorizing the agency to build and strengthen a national cybersecurity workforce pipeline through the Cybersecurity and Education and Training Assistance Program.[11]

S. 2305 allows DHS to award grants to HBCUs, institutions of higher education that have an enrollment of "needy students'", and other minority-serving institutions.[12] Grant recipients can use these funds to support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, to train qualified cybersecurity professionals, and establish National Centers of Academic Excellence (NCAEs) in Cybersecurity. The purpose of the NCAE program is to create standard cybersecurity curriculum and establish a workforce pipeline from NCAE institutions to select federal agencies.[13] S. 2305 ensures that NCAEs are established in higher educational institutions that serve underrepresented communities, which will enhance the number of diverse cybersecurity personnel in the federal government.

This legislation continues to strengthen DHS's leadership role in cybersecurity workforce education, while recognizing that appropriate coordination with other government agencies is important to developing a comprehensive approach to cybersecurity education.

III. LEGISLATIVE HISTORY

Senator Jon Ossoff (D–GA) introduced S. 2305, the Cybersecurity Opportunity Act, on June 24, 2021. Cosponsors who joined the bill after introduction include: Senators Thom Tillis (R–NC), Tim Scott (R–SC), Angus S. King (I–ME), John Cornyn (R–TX), Catherine Cortez Masto (D–NV), Mark Kelly (D–AZ), Mike Rounds (R–SD), and John Boozman (R–AR),

The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs on June 24, 2021, and the Committee considered S. 2305 at a business meeting on August 4, 2021. During the business meeting, Senator Ossoff offered a modified substitute amendment which would do the following: allow private, non-profit schools that serve the specified target student populations to participate; reserve no less than 50 percent of grant funds specifically for HBCUs and minority-serving institutions; remove a five-year sunset provision; add student outreach and recruitment as an authorized activity; add reporting requirements; and authorize an appropriation of $50 million per fiscal year. The modification to the amendment would remove the authorization for

[10] *See Id.* at 36.

[11] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116–283, Sec. 1719 (2020).

[12] "Needy students" is defined the Higher Education Act of 1965, Pub. L. 89–329, Sec. 312(d).

[13] *See* National Security Agency and Central Security Service, Home Page (https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/) (accessed Dec. 9, 2021).

appropriations, require DHS to develop performance metrics to evaluate the grants, and include a 5-year sunset clause. The Ossoff substitute amendment, as modified, was adopted by unanimous consent.

Senator Johnson offered an amendment, as modified, that would strike the authorization of appropriations designated for grants to assist higher education institutions that have higher numbers of enrollment of needy students, HBCUs, and other minority-serving institutions, and instead require the use of unobligated funds from the American Rescue Plan to implement the bill. The amendment, as modified, was not adopted by voice vote with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present.

The Committee ordered the bill, as amended by the modified substitute amendment, reported favorably by voice vote with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present.

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

Section 1. Short title

This section designates the name of the bill as the "Cybersecurity Opportunity Act."

Section 2. Dr. David Satcher Cybersecurity Education Grant Program

Subsection (a) defines the terms "enrollment of needy students," "historically Black college or university," "institution of higher education," "minority-serving institution," and "Secretary."

Subsection (b) authorizes the DHS Secretary to award grants to assist institutions of higher education that have an enrollment of needy students, HBCUs, and minority-serving institutions, to: establish or expand cybersecurity programs; build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities; support the training of qualified cyber workforce candidates; and be designated as a National Center of Academic Excellence in Cybersecurity. This subsection allows the Secretary to award grants to the aforementioned entities to expand cybersecurity education opportunities, technology and programs, research, and partnerships with public and private entities. In awarding the grants, 50 percent of the funds shall be made available for HBCUs and minority-serving institutions, and the Secretary is required to coordinate with the National Initiative for Cybersecurity Education. The Secretary's authority to award grants expires five years after the Secretary awards the first grant.

Subsection (c) requires an eligible institution seeking a grant to submit an application to the Secretary, including a statement of how the institution will use the funds awarded by the grant to expand cybersecurity education opportunities at the eligible institution.

Subsection (d) specifies how an eligible institution can use grants for increasing research, education, technical, partnership, and innovation capacity.

Subsection (e) requires the Secretary to submit to Congress a report on the status and progress of implementation of the grant program.

Subsection (f) requires the Secretary to establish performance metrics for grants awarded under this section.

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

CONGRESSIONAL BUDGET OFFICE,
U.S. CONGRESS,
Washington, DC, September 24, 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. 2305, the Cybersecurity Opportunity Act.

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. 2305, Cybersecurity Opportunity Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on August 4, 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)	0	16	not estimated

		Mandate Effects	
Statutory pay-as-you-go procedures apply?	No		
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

S. 2305 would require the Department of Homeland Security (DHS) to distribute grants to colleges and universities to expand

their cybersecurity research programs and class offerings. Under the bill, DHS would award at least half of the grant funding to Historically Black Colleges and Universities and other minority-serving institutions. The bill also would require DHS to report to the Congress annually on the effectiveness of the new grant program.

Based on funding for similar grant programs, CBO estimates that implementing S. 2305 would cost $16 million over the 2021–2026 period (detailed in Table 1). That estimate includes $12 million for grants and $4 million for salaries and expenses over the 2021–2026 period for the administrative costs of reviewing grant applications and reporting on the program's implementation. Such spending would be subject to the availability of appropriations. For this estimate, CBO assumes that the bill will be enacted in fiscal year 2022.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 2305

	By fiscal year, millions of dollars—						
	2021	2022	2023	2024	2025	2026	2021–2026
Cybersecurity Grants:							
Estimated Authorization	0	4	4	4	4	4	20
Estimated Outlays	0	*	1	3	4	4	12
Administrative Costs:							
Estimated Authorization	0	*	1	1	1	1	4
Estimated Outlays	0	*	1	1	1	1	4
Total Changes:							
Estimated Authorization	0	4	5	5	5	5	24
Estimated Outlays	0	*	2	4	5	5	16

* = between zero and $500,000.

The CBO staff contact for this estimate is Aldo Prosperi. 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.

○