Calendar No. 551

118TH CONGRESS *2d Session*	SENATE	REPORT 118–238

FEDERAL CYBER WORKFORCE TRAINING ACT OF 2024

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 4715

TO REQUIRE THE NATIONAL CYBER DIRECTOR TO SUBMIT TO CONGRESS A PLAN TO ESTABLISH AN INSTITUTE WITHIN THE FEDERAL GOVERNMENT TO SERVE AS A CENTRALIZED RESOURCE AND TRAINING CENTER FOR FEDERAL CYBER WORKFORCE DEVELOPMENT

NOVEMBER 12, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
59–010 WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA R. BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A, FERGUSON, *Professional Staff Member*
DEVIN M. PARSONS, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 551

118TH CONGRESS *2d Session* | SENATE | REPORT 118–238

FEDERAL CYBER WORKFORCE TRAINING ACT OF 2024

NOVEMBER 12, 2024.—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. 4715]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4715) to require the National Cyber Director to submit to Congress a plan to establish an institute within the Federal Government to serve as a centralized resource and training center for Federal cyber workforce development, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 4715, the *Federal Cyber Workforce Training Act of 2024*, would require that the National Cyber Director submit a plan to Congress to establish an institute to serve as a centralized resource and training center for federal cyber workforce development.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Defending the nation's networks and systems from cyberattacks requires investments in hardware and software, and also invest-

ments in the personnel running the networks.[1] Cybersecurity personnel serve to protect the nation from cyberattacks and ensure confidentiality, integrity, and access to information for citizens and employees. The International Information System Security Certification Consortium (ISC2) estimated that in 2019 the global cyber workforce constituted 2.8 million people; in 2023, those numbers increased to an all-time high of 5.5 million people.[2]

The demand for a skilled cyber workforce has led to more cyber positions open than workers available to fill those positions—creating a cybersecurity workforce gap. In 2023, ISC2 estimated that there were 482,985 unfilled cyber positions in the United States, an increase of 17.6% from 2022.[3] The impact of this cyber workforce gap impacts all levels of personnel and management.[4]

The challenge of developing or attracting a sufficient cybersecurity workforce is a significant issue in the United States that continues to affect industries and organizations struggling to recruit skilled personnel.[5] The federal government is not immune to the difficulties of developing, attracting, or retaining skilled cybersecurity personnel. Since 2016, federal agencies such as the Department of Defense (DOD) and the Department of Homeland Security (DHS) have created or expanded programs for special pay for cyber and IT professionals to close the workforce gap.[6] In June 2024, DHS's Chief Information Officer and Chief Artificial Intelligence Officer, Eric Hysen, testified before the United States House of Representatives Committee on Homeland Security that despite DHS employing over 8,000 cybersecurity professionals, the Department had 2,000 vacancies and struggles to recruit and retain talent, particularly talent with the skills needed to maintain a competitive edge amid rapid advances in technology. His testimony also noted that it is important for DHS to not only attract and hire technical talent, but also to invest in and continually train the existing workforce.[7]

The Office of the National Cyber Director (ONCD), building on previous efforts such as National Security Memorandum 3, Execu-

---

[1] Government Accountability Office, *National Initiative Needs to Better Assess Its Performance* (GAO–23–105945) (Jul. 27, 2023); *The Cybersecurity Workforce Gap*, Center for Strategic and International Studies (Jan. 2019) (csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf).

[2] ISC2, *ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap* (Nov. 3, 2023) (https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap).

[3] ISC2, ISC2 Cybersecurity Workforce Study, at 12 (2023) (https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf).

[4] *The Cybersecurity Workforce Gap*, Center for Strategic and International Studies (Jan. 2019) (https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf); ISC2, *Workforce Data Shows the Need for Cyber Staff Development Programs* (blog) (Sep. 20, 2024) (www.isc2.org/Insights/2024/09/Workforce-Data-Shows-the-Need-for-Cyber-Staff-Development-Programs).

[5] Office of the National Cyber Director, *National Cyber Workforce and Education Strategy* (Jul. 31, 2023) (www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf); M. Hogan et al., *Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Supply and Demand Report*, National Science Foundation (May 2024) (ncses.nsf.gov/about/cybersecurity-workforce-data-initiative).

[6] *DoD Looks to Expand Cyber Excepted Service, Won't Implement New SSR for IT Workforce, Federal News Network* (May 26, 2023) (https://federalnewsnetwork.com/federal-report/2023/05/dod-looks-to-expand-cyber-excepted-service-wont-implement-new-ssr-for-it-workforce/); and *DHS' Cyber Talent Management System Slowly Gaining Traction*, Federal News Network (Apr. 28, 2023) (https://federalnewsnetwork.com/cybersecurity/2023/04/dhs-cyber-talent-management-system-slowly-gaining-traction/).

[7] United States House of Representatives Committee on Homeland Security, Testimony Submitted for the Record of Eric Hysen, Dept. of Homeland Security, *Finding 500,000: Addressing America's Cyber Workforce Gap*, 118th Cong. (Jun. 26, 2024).

tive Order 14119, and Executive Order 14110, has expanded overall federal efforts to address the workforce gap.[8] In July 2023, ONCD released the National Cyber Workforce and Education Strategy, aiming to align ONCD's efforts with the President's Management Agenda, and with investments in workforce and technology hubs across the nation. The National Cyber Workforce and Education Strategy specifically advocates for "a skills-based approach to build more robust cyber career pathways" and lays out several objectives to address federal hiring, upskilling, and retaining cyber talent.[9]

S. 4715 would address the federal cyber workforce gap by requiring that the National Cyber Director create a plan for a federal institute to serve as a centralized resource and training center for federal cyber workforce development. This workforce training institute would provide a new pipeline for cyber talent to enter federal service. Additionally, the institute would help provide current federal employees with upskilling and training opportunities, increasing the federal government's ability to retain an experienced and skilled workforce. Having one centralized resource for cyber training would also decrease the burden on individual federal agencies to create their own training programs and would help ensure that all federal cyber and IT employees have the same, high-quality education and skills needed for their jobs.

III. LEGISLATIVE HISTORY

Senator Mike Rounds (R–SD) introduced the *Federal Cyber Workforce Training Act of 2024* on July 11, 2024, with original cosponsor Senator Jon Ossoff (D–GA). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. Senator Jacky Rosen (D–NV) joined as an additional cosponsor on July 23, 2024.

The committee considered S. 4715 at a business meeting on July 31, 2024. At the business meeting, Senator Ossoff offered a substitute amendment. The substitute amendment changed the date on which the National Cyber Director must brief congressional committees on the required plan, to 280 days after enactment, rather than 270 days after enactment. The Committee adopted the substitute amendment by unanimous consent, with Senators Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Blumenthal, Butler, Paul, Lankford, and Scott present.

The bill, as amended by the Ossoff substitute amendment, was ordered reported favorably by roll call vote of 10 yeas to 1 nay, with Senators Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Blumenthal, Butler, Lankford, and Scott voting in the affirmative, and Senator Paul voting in the negative. Senators Johnson, Romney, Hawley, and Marshall voted yea by proxy, for the record only.

---

[8] National Security Memorandum "Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships" (Feb. 4, 2021) (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships/); Exec. Order No. 14119, 89 Fed. Reg. 17265 (Mar. 11, 2024); and Exec. Order No. 14110, 88 Fed. Reg. 75191, (Nov. 1, 2023).

[9] Office of the National Cyber Director, *National Cyber Workforce and Education Strategy* (Jul. 31, 2023) (www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf).

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

Section 1. Short title

This section establishes the short title of the bill as the "Federal Cyber Workforce Training Act of 2024."

Section 2. Federal Cyber Workforce Development Institute

Subsection (a) defines the terms "agency," "appropriate congressional committees," "cyber work role," "director," "federal institute," "NICE framework," and "work-based learning."

Subsection (b) paragraph (1) requires that not later than 180 days after enactment, the National Cyber Director, in consultation with DHS, DOD, and the Office of Personnel Management (OPM), and other agencies as necessary, submit to Congress and make publicly available a plan to establish an institute for training federal personnel with cyber work roles. The plan must provide for the institute to offer modularized cyber training aligned with work roles, address the training needs of entry-level and mid-career employees, and incorporate training for human resources staff and hiring managers.

Subsection (b) paragraphs (2)–(3) requires that the plan recommend an organizational placement for the institute, and align the institute's training and tools with NIST's "Workforce Framework for Cybersecurity" (the NICE framework) and other relevant guidance. The plan must also recommend a course curriculum, delivery method, and length of curriculum for the training, using existing programs as models. Additionally, the plan must establish a policy for individuals who do not complete the required training, describe a security clearance process for appropriate individuals, recommend a governance structure for the institute, and estimate the funding and new authorities required. The plan must also identify how the institute would provide some or all of the training through academic institutions.

Subsection (b) paragraph (4) requires the National Cyber Director to consult with the Director of OPM, the Chief Human Capital Officers Council, the Chief Information Officers Council, and the Chief Learning Officers Council in developing the plan.

Subsection (c) requires that within 280 days of enactment, the National Cyber Director provide a briefing to Congress on the plan.

Subsection (d) stipulates that no additional funds are authorized to be appropriated for the purpose of carrying out this 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

S. 4715, Federal Cyber Workforce Training Act of 2024
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 31, 2024

By Fiscal Year, Millions of Dollars	2024	2024-2029	2024-2034
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	*	*

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2035?	No	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 2035?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 4715 would require the National Cyber Director to develop a plan for the federal government to establish a cybersecurity training institute. The bill would require that the plan include recommendations for in-person and virtual courses for federal cyber professionals. For purposes of this estimate, CBO assumes the bill will be enacted in 2025.

Based on the costs of similar efforts, CBO estimates that creating and publishing the plan would cost less than $500,000 over the 2024–2029 period. Any 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 Christina Hawley Anthony, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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.

○