Calendar No. 255

118TH CONGRESS *1st Session*	SENATE	REPORT 118–117

FEDERAL CYBERSECURITY WORKFORCE EXPANSION ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2256

TO AUTHORIZE THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO ESTABLISH AN APPRENTICESHIP PROGRAM AND TO ESTABLISH A PILOT PROGRAM ON CYBERSECURITY TRAINING FOR VETERANS AND MEMBERS OF THE ARMED FORCES TRANSITIONING TO CIVILIAN LIFE, AND FOR OTHER PURPOSES

NOVEMBER 30, 2023.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

49–010 WASHINGTON : 2023

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*
LENA C. CHANG, *Director of Governmental Affairs*
DEVIN M. PARSONS, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 255

118TH CONGRESS *1st Session* | SENATE | REPORT 118–117

FEDERAL CYBERSECURITY WORKFORCE EXPANSION ACT

NOVEMBER 30, 2023.—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. 2256]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2256) to authorize the Director of the Cybersecurity and Infrastructure Security Agency to establish an apprenticeship program and to establish a pilot program on cybersecurity training for veterans and members of the Armed Forces transitioning to civilian life, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

PURPOSE AND SUMMARY

S. 2256, the *Federal Cybersecurity Workforce Expansion Act*, would establish two new pilot programs related to the cybersecurity workforce. It would create a five-year cybersecurity apprenticeship pilot program within the Department of Homeland Security (DHS). Up to 25 apprentices could participate in this program each year and enter into service agreements with the federal government upon completion of the program. The bill also directs DHS, in coordination with the Department of Veterans Affairs, to estab-

lish a five-year pilot program to provide cybersecurity training at no cost to veterans and military spouses. Under the bill, DHS would submit annual reports to Congress on each of these pilot programs, and the Government Accountability Office (GAO) would conduct an assessment of each program within four years after it is established. Finally, the bill would extend from 2022 to 2027 the requirement that federal agencies submit an annual report to the Office of Personnel Management (OPM) identifying cyber-related work roles in the agency's workforce.[1]

II. Background and Need for the Legislation

There is a national shortage of qualified cybersecurity personnel. According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST), there are over 660,000 cybersecurity job openings in the United States, including over 8,000 at the federal level, as of August 2023.[2] A September 2022 *State of the Federal Cyber Workforce* report by the Federal Cyber Workforce Management and Coordinating Working Groups noted that "[s]ystemic changes to the development of our cyber workforce are vital for our nation to sufficiently govern and maintain our critical infrastructures and data security." The report also found that "increasing cyber attacks and a heightened talent shortage serves as a wake-up call that the federal government must reenergize and promote how it is a premier place of employment for cyber professionals."[3]

The consistent shortage of cybersecurity personnel represents a high risk to national security. Federal cyber workforce management challenges have been on the GAO High-Risk List since 2003.[4] In that report, GAO stated:

> [A]gencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. . . . [T]he availability of adequate technical and audit expertise is a continuing concern to agencies.[5]

Since 2003, the need for a developed and expansive cyber workforce has continued to intensify. As GAO Director of Information Security Issues, Gregory C. Wilshusen, stated in March 2018 testimony before the House Committee on Homeland Security Subcommittees on Cybersecurity and Infrastructure Protection and Oversight and Management Efficiency during a hearing examining the cybersecurity workforce:

> The Office of Management and Budget has noted that the federal government and private industry face a persistent

---

[1] On November 3, 2021, the Committee approved S. 2274, the *Federal Cybersecurity Workforce Expansion Act.* That bill, as reported, is substantially similar to S. 2256. Accordingly, this committee report is, in many respects, similar to the committee report for S. 2274. *See* S. Rept. 117–131.

[2] Cyberseek, Interactive Map (www.cyberseek.org/heatmap.html) (accessed Aug. 9, 2023).

[3] Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action* (Sept. 2022) (digital.va.gov/wp-content/uploads/2022/10/State-of-the-Federal-Cyber-Workforce-Report_2022.pdf).

[4] Government Accountability Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures* (GAO–03–121) (Jan. 2003) (www.gao.gov/assets/gao-03-121.pdf).

[5] *Id.*

shortage of cybersecurity and IT talent to implement and oversee information security protections. This shortage may leave federal IT systems vulnerable to malicious attacks. Experienced and qualified cybersecurity professionals are essential in performing DHS's work to mitigate vulnerabilities in its own and other agencies' computer systems and to defend against cyber threats.[6]

In the April 2023 High-Risk Series report, GAO recommended that federal agencies "take additional actions to address the federal cybersecurity workforce shortage" and that the Office of Management and Budget develop a governmentwide workforce plan to address the issues facing the cyber workforce.[7]

The problem of cybersecurity workforce shortages has taken on increased urgency as the United States faces escalating threats from hostile cyber actors. In 2021, multiple high-profile cybersecurity incidents, including SolarWinds, Microsoft Exchange, and Colonial Pipeline, prompted President Biden to issue an Executive Order aimed at improving the nation's cybersecurity preparedness systems.[8] Furthermore, critical infrastructure, such as healthcare systems, face an ever-growing threat from cyber incidents that affect operations and patient care, illustrated by recent attacks in early 2023 on Tallahassee Memorial HealthCare in Florida and the University of Michigan Health System.[9] These cyber attacks further underscore the urgent need to advance skills of the nation's cybersecurity workforce.

The Committee on Homeland Security and Governmental Affairs has held multiple hearings in the wake of cybersecurity attacks to address the government's preparedness, response, and recovery efforts.[10] During a hearing on September 23, 2021, entitled *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems,* Senator Margaret Wood Hassan (D–NH) asked Jen Easterly, Director of the Cyber and Infrastructure Security Agency (CISA), if an apprenticeship program would help address workforce challenges at CISA. Director Easterly said, "We've already started talking about how we could implement apprenticeships at CISA. . . . I think we need to be as creative as possible in all our approaches to deal with the deficit that we have across the country and then across the federal cyber workforce." Fellow witness Chris Inglis, National Cyber Director in the Executive Office of the President, agreed with Director Easterly's remarks and

---

[6] Government Accountability Office, *Cybersecurity Workforce: DHS Needs to Take Urgent Action to Identify Its Position and Critical Skills Requirements* (GAO–18–430T) (Mar. 2018) (www.gao.gov/assets/gao-18-430t.pdf).

[7] Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas* (GAO–23–106203) (Apr. 2023) (www.gao.gov/assets/gao-23-106203.pdf).

[8] Executive Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

[9] Senate Committee on Homeland Security and Governmental Affairs, Opening Statement of Chairman Gary Peters, *Hearing on In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector*, 118th Cong. (Mar. 16, 2023) (S. Hrg. 118–XX).

[10] *See* Senate Committee on Homeland Security and Governmental Affairs, *Hearing on Prevention, Response and Recovery: Improving Federal Cybersecurity Post-SolarWinds*, 117th Cong. (May 11, 2021) (S. Hrg. 117–XX); Senate Committee on Homeland Security and Governmental Affairs, *Hearing on Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack,* 117th Cong. (June 8, 2021) (S. Hrg. 117–429); Senate Committee on Homeland Security and Governmental Affairs, *Hearing on National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems,* 117th Cong. (Sep. 23, 2021) (S. Hrg. 117–266); *and* Senate Committee on Homeland Security and Governmental Affairs, *Hearing on In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector*, 118th Cong. (Mar. 16, 2023) (S. Hrg. 118–XX).

added that "apprenticeships are essential, not simply because they provide experience for its own sake, but they bridge the gap between aspiration that is often supported by training and education and the real experience that employers need or want when you show up at that door." [11]

In March 2023, the Biden Administration continued efforts to expand the cyber workforce through the release of a *National Cybersecurity Strategy*. The strategy recognized "the need for cybersecurity expertise across all sectors of the economy" and seeks to "strengthen and diversify the Federal cyber workforce, addressing the unique challenges the public sector faces in recruiting, retaining, and developing the talent and capacity needed to protect Federal data and IT infrastructure." [12]

In July 2023, the White House published an additional strategy document focused on strengthening cyber education and training opportunities. The *National Cyber Workforce and Education Strategy* highlights the importance of skills-based approaches like apprenticeship programs:

> Integrated education and training models that include work-based learning, paid internships, externships, pre-apprenticeships, or registered apprenticeships have proven to be effective. Through these and other work-based learning opportunities, cyber workers can earn a wage as they gain hands-on experience and develop their skills.

The *Federal Cybersecurity Workforce Expansion Act* aims to strengthen the cybersecurity talent pipeline within the federal government by establishing a registered apprenticeship pilot program at DHS in which participants receive on-the-job cybersecurity training. Upon successful completion of the program, participants may be appointed to cybersecurity-specific positions within a federal agency. The appointed program graduates would enter into a service agreement, in which they commit to working in the federal government for a period of service equal to the length of the apprenticeship. Under the bill, DHS and the Department of Veterans Affairs also would establish a pilot program to provide cybersecurity training at no cost to veterans and military spouses. This pilot program would incorporate coursework, virtual learning, and work-based learning opportunities and lead to a recognized postsecondary credential.

This bill incorporates recommendations from a report published by the Cyberspace Solarium Commission in March 2020. The report recommended that the federal government "develop work-based learning programs and apprenticeships to supplement classroom learning" as a step to improve cyber-oriented education.[13] Another recommendation called for designing "cybersecurity-specific upskilling and transition assistance programs for veterans and transitioning military service members to move into federal civilian cybersecurity jobs." [14] The *Federal Cybersecurity Workforce Expan-*

---

[11] Senate Committee on Homeland Security and Governmental Affairs, Transcript, *Hearing on National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems*, 117th Cong. (Sep. 23, 2021) (S. Hrg. 117–266) (https://plus.cq.com/doc/congressionaltranscripts-6351036?4&searchId=9Svfjbqf).

[12] The White House, *National Cybersecurity Strategy* (Mar. 2023) (www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf).

[13] Cyberspace Solarium Commission, *A Warning From Tomorrow* (Mar. 2020) (drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

[14] *Id.* at 44.

sion Act reflects these recommendations and would augment cybersecurity workforce development pathways.

III. Legislative History

Senator Hassan (D–NH) introduced S. 2256, the *Federal Cybersecurity Workforce Expansion Act*, on July 12, 2023, with Senator John Cornyn (R–TX) as an original cosponsor. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2256 at a business meeting on July 26, 2023. During the business meeting, S. 2256 was ordered reported favorably by roll call vote of 7 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Ossoff, Lankford, and Scott voting in the affirmative and Senator Paul voting in the negative. Senators Carper, Padilla, Blumenthal, Johnson, Romney, Hawley, and Marshall voted yea by proxy, for the record only.

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 Cybersecurity Workforce Expansion Act."

Section 2. Findings

This section includes findings indicating the need for additional federal cybersecurity professionals.

Section 3. Definitions

This section defines the terms "Department," "institution of higher education," and "Secretary" for the purposes of this bill.

Section 4. Cybersecurity apprenticeship pilot program

Subsection (a) defines the terms "area career and technical education school," "community college," "competitive service," "cyber workforce position," "early college high school; educational service agency; local educational agency; secondary school; state educational agency," "education and training provider," "eligible entity," "excepted service," "local workforce development board," "minority-serving institution," "nonprofit organization," "provider of adult education," "qualified intermediary," "related instruction," "sponsor," "state," "state apprenticeship agency," "state workforce development board," and additional terms from the Workforce Innovation and Opportunity Act for the purposes of this section.

Subsection (b) directs the Secretary of Homeland Security to establish an apprenticeship pilot program within three years of the bill's enactment. DHS would employ up to 25 apprentices in cyber workforce positions during each year of the program. The pilot program would offer learning opportunities based on the NICE Workforce Framework for Cybersecurity, or a successor framework, and prepare the participants for cyber workforce positions within federal agencies. DHS or an eligible entity receiving a contract, cooperative agreement, or grant would sponsor the registered apprenticeship program and veterans would be able to use their educational assistance toward the program.

Subsection (c) directs the Secretary of Homeland Security to consult with the Secretary of Labor, the Director of NIST, the Sec-

retary of Defense, the Director of the National Science Foundation, and the Director of OPM when developing the apprenticeship pilot program.

Subsection (d) outlines options available to DHS for entering into a contract or cooperative agreement with or a making a grant to an eligible entity for assistance sponsoring the apprenticeship program. The entity chosen to sponsor the program must have demonstrated experience in implementing apprenticeship programs, have knowledge of cybersecurity workforce development, be able to provide participants with one or more recognized postsecondary credentials, use instruction that is specifically aligned with the needs of federal agencies, and have demonstrated success in connecting apprenticeship participants with careers relevant to the pilot program.

Subsection (e) requires any entity seeking a contract, cooperative agreement, or grant under subsection (d) to submit an application to DHS with such information as the Secretary may require.

Subsection (f) allows DHS to prioritize an eligible entity in the context of subsection (d) if the entity: (1) is a member of an industry or sector partnership that sponsors or participates in an apprenticeship program; (2) provides related instruction for a registered apprenticeship program; (3) works to transition members of the military and veterans to apprenticeship programs in a relevant sector; (4) plans to carry out the apprenticeship program with an entity that receives state funding or is operated by a state agency; (5) has successfully increased the representation of women, minorities, and individuals from other underrepresented communities in cybersecurity; or (6) focuses on recruiting women, minorities, and individuals from other underrepresented communities.

Subsection (g) directs DHS to provide technical assistance to eligible entities selected under subsection (d) to leverage any existing and relevant federal job training and education programs.

Subsection (h) requires pilot program participants to enter into a service agreement in which they agree to serve in a cyber workforce position within a federal agency, if offered such a position after completion of the apprenticeship program, for a length of time equal to the length of the apprenticeship program. If an individual does not satisfy the requirements of the service agreement, they would need to repay the cost of the education and training provided, reduced by an amount factoring in the period of service they completed. The Secretary may waive the service or repayment requirements in certain circumstances, such as if compliance would involve hardship to the individual.

Subsection (i) specifies that participants in the apprenticeship program may be appointed to cybersecurity positions in the excepted service.

Subsection (j) specifies that individuals who successfully complete the apprenticeship program may be appointed to cybersecurity positions in the excepted service.

Subsection (k) provides that federal service following the apprenticeship program would be subject to the completion of a trial period in accordance with any applicable law or regulation.

Subsection (l) requires DHS to submit an annual report starting two years after the beginning of the apprenticeship pilot program that includes: (1) any activity carried out by DHS under this sec-

tion; (2) any eligible entity selected under subsection (d) and activities carried out by that entity; (3) best practices used; and (4) an assessment of the results achieved by the apprenticeship program, including the rate of continued employment within a federal agency, the demographics of participants in the apprenticeship, the rate of completion by program participants, and the return on investment of the pilot program. This subsection also directs GAO to conduct a study on the apprenticeship pilot program within four years after the program is established.

Subsection (m) sunsets the apprenticeship pilot program after five years.

Section 5. Pilot program on cybersecurity training for veterans and military spouses

Subsection (a) defines the terms "eligible individual," "recognized postsecondary credential," "veteran," and "work-based learning" for the purposes of this section.

Subsection (b) directs the DHS Secretary, in consultation with the Secretary of Veterans Affairs, to establish a pilot program within three years of the bill's enactment to provide cybersecurity training to veterans and military spouses.

Subsection (c) requires the pilot program to incorporate: (1) coursework and training that qualifies toward postsecondary credit; (2) virtual learning opportunities; (3) hands-on learning and performance-based assessments; (4) federal work-based learning opportunities; and (5) the provision of recognized postsecondary credentials to participants who complete the pilot program.

Subsection (d) requires the pilot program to align with the NICE Workforce Framework for Cybersecurity or a successor framework.

Subsection (e) directs the DHS Secretary to coordinate with the Secretary of Veterans Affairs, Secretary of Defense, Secretary of Labor, Director of NIST, and Director of OPM to leverage existing training, platforms, and frameworks within the federal government for cybersecurity education and training, to prevent duplication of efforts. DHS must coordinate with the Department of Veterans Affairs to ensure that eligible individuals can use existing educational assistance to the greatest extent possible. DHS must coordinate with the Departments of Veterans Affairs, Defense, and Labor, as well as OPM and any other appropriate agencies, to identify and create interagency opportunities that allow program participants to acquire competencies and capabilities necessary to qualify for federal employment.

Subsection (f) authorizes the DHS Secretary, in coordination with the Secretary of Veterans Affairs, to expand existing training, platforms, and frameworks or develop and procure resources as necessary to carry out the program. DHS may provide additional funding, staff, or other resources to: (1) recruit and retain women, minorities, and individuals from other underrepresented communities; (2) provide administrative support; (3) ensure ongoing engagement and success of eligible individuals participating in the program; (4) connect participants who complete the program with job opportunities in the federal government; and (5) allocate dedicated positions for term employment to enable federal work-based learning opportunities.

Subsection (g) requires the DHS Secretary to submit an annual report starting two years after the beginning of the pilot program that includes a description of: (1) any activity carried by DHS under this section; (2) existing training, platforms, and frameworks used; and (3) the results achieved by the apprenticeship program, including the admittance rate into the pilot program, the demographics of program participants, the rate of completion by program participants, transfer rates to other academic or vocational programs, the rate of continued employment within a federal agency, and the median annual salary of participants employed after completing the program. This subsection also directs GAO to conduct a study on the pilot program within four years after the program is established.

Subsection (h) sunsets the pilot program established by this section after five years.

Section 6. Federal cybersecurity workforce assessment extension

This section extends from 2022 to 2027 the requirement that each federal agency submit an annual report to OPM identifying cyber-related work roles of critical need in the agency's workforce.

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

At a Glance

S. 2256, Federal Cybersecurity Workforce Expansion Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 26, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	0	30	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	No	Statutory pay-as-you-go procedures apply?	Yes
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between -$500,000 and $500,000.

The bill would:

- Establish a cybersecurity apprenticeship program
- Create a cybersecurity training program for veterans and spouses of military personnel
- Extend reporting requirements for federal positions related to information technology and cybersecurity

Estimated budgetary effects would mainly stem from:

- Hiring and training cybersecurity apprentices
- Developing cybersecurity training courses for veterans and military spouses
- Spending veterans' education benefits on cybersecurity training

Bill summary: S. 2256 would require the Department of Homeland Security (DHS) to establish a cybersecurity apprenticeship program to recruit and hire people to perform information technology and cybersecurity roles for the department. DHS also would provide apprentices with training courses and career development materials.

In addition, S. 2256 would require DHS to establish a program to provide cybersecurity training without charge to veterans who are eligible for education benefits administered by the Department of Veterans Affairs (VA).

Estimated Federal cost: The estimated budgetary effects of S. 2256 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 2256

	By fiscal year, millions of dollars—						
	2023	2024	2025	2026	2027	2028	2023–2028
Cybersecurity Apprentices							
Estimated Authorization	0	0	2	5	5	5	17
Estimated Outlays	0	0	2	5	5	5	17
Curriculum and Training							
Estimated Authorization	0	0	8	0	0	0	8
Estimated Outlays	0	0	5	3	0	0	8
Program Management Staff							
Estimated Authorization	0	*	1	1	1	2	5
Estimated Outlays	0	*	1	1	1	2	5
Total Changes							
Estimated Authorization	0	*	11	6	6	7	30
Estimated Outlays	0	*	8	9	6	7	30

* = between zero and $500,000.

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2256 would have insignificant effects on direct spending and the deficit over the 2023–2033 period.

Basis of estimate: For this estimate, CBO assumes that S. 2256 will be enacted early in fiscal year 2024 and that the required pilot programs would begin to operate in 2025. CBO also expects that cybersecurity apprentices would serve for a two-year term. Under S. 2256, the authority to operate the pilot programs would terminate five years after their establishment. Outlays are estimated using historical spending patterns for existing or similar programs.

Spending subject to appropriation: CBO estimates that implementing the bill would cost $30 million over the 2023–2028 period. Such spending would be subject to the availability of appropriated funds.

Cybersecurity Apprentices. S. 2256 would require DHS to recruit and hire apprentices to fill a range of information technology and cybersecurity roles across the department. On the basis of information from the Department of Labor about the average duration and salaries of similar government apprenticeship programs, CBO expects that each apprentice would serve for two years at an average annual cost of about $92,000 for salaries and benefits. CBO anticipates that each cohort of apprentices would include 25 people, the maximum annual number of new hires permitted under S. 2256, and that DHS would hire the first cohort in 2025. Because each cohort would serve for two years, CBO expects that DHS would employ 50 cyber apprentices each year once the second cohort is hired. On that basis and accounting for the effects of anticipated inflation, CBO estimates that compensation for apprentices hired under S. 2256 would total $17 million over the 2023–2028 period.

Curriculum and Training. S. 2256 would require DHS to develop cybersecurity training courses for the apprenticeship and veteran training programs authorized under the bill. CBO expects that DHS would contract with private-sector cybersecurity firms to design the curricula for those courses and create online platforms to access the training. Based on the costs of similar programs at DHS, CBO estimates that cyber training services and materials would cost about $8 million over the 2023–2028 period.

Program Management Staff. Using information about similar training programs, CBO anticipates that DHS would need five full-time employees to create and manage the new programs. CBO estimates that their compensation would total $5 million over the 2023–2028 period.

Cybersecurity Workforce Assessment Extension. S. 2256 would extend, from 2022 to 2027, the reporting requirements established under the Federal Cybersecurity Workforce Assessment Act. Satisfying those requirements would increase spending subject to appropriation by less than $500,000 over the 2023–2028 period, CBO estimates. That extension also would affect some agencies that finance operations from sources other than discretionary appropriations; those effects are discussed below under the heading “Direct Spending.”

Direct spending: Several provisions in S. 2256 would have insignificant effects on direct spending over the 2023–2033 period, in CBO’s estimation.

Cybersecurity Training for Veterans and Military Spouses. CBO expects that some veterans and their spouses who are eligible for education benefits administered by VA would increase their use of those benefits as a result of the cybersecurity training program. At the same time, some veterans who otherwise would have used their benefits to enroll in a postsecondary education program would instead use them for cybersecurity training (which would typically cost less). The costs of VA education benefits are paid from mandatory appropriations. CBO estimates that the changes in the use of benefits would have insignificant net effects on direct spending over the 2023–2033 period.

Cybersecurity Workforce Assessment Extension. As described above under the heading “Spending Subject to Appropriation,” S. 2256 would extend the reporting requirements established under the Federal Cybersecurity Workforce Assessment Act. Enacting

that extension could affect direct spending by some agencies that use fees, receipts from the sale of goods, and other collections to cover operating costs. CBO estimates that any net changes in direct spending by those agencies would be negligible because most of them can adjust amounts collected to accommodate changes in operating costs.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting the bill would have insignificant effects on direct spending and the deficit over the 2023–2033 period.

Increase in long-term net direct spending and deficits: None.

Mandates: None.

Estimate prepared by: Federal Costs: Aldo Prosperi (Department of Homeland Security), Paul B.A. Holland (Department of Veterans Affairs), Mandates: Brandon Lever.

Estimate reviewed by: David Newman, Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit; Kathleen FitzGerald, Chief, Public and Private Mandates Unit; Christina Hawley Anthony, Deputy Director of Budget Analysis.

Estimate approved by: Phillip L. Swagel, Director, Congressional Budget Office.

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

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT ACT OF 2015

* * * * * * *

SEC. 304. IDENTIFICATION OF CYBER RELATED WORK ROLES OF CRITICAL NEED.

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 303(b)(2), and annually thereafter through [2022]*2027*, the head of each Federal agency, in consultation with the Director, the Director of the National Institute of Standards and Technology, and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

* * * * * * *

○