Calendar No. 446

117TH CONGRESS *2d Session*	SENATE	REPORT 117–131

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. 2274

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

JULY 18, 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*
LENA C. CHANG, *Director of Governmental Affairs*
DEVIN M. PARSONS, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
CARA G. MUMFORD, *Minority Director of Governmental Affairs*
ANDREW J. HOPKINS, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 446

117TH CONGRESS
2d Session

SENATE

REPORT
117–131

FEDERAL CYBERSECURITY WORKFORCE EXPANSION ACT

JULY 18, 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. 2274]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2274) 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 an amendment (in the nature of a substitute) and recommends that the bill, as amended, do pass.

CONTENTS

		Page
I.	Purpose and Summary	1
II.	Background and Need for the Legislation	2
III.	Legislative History	4
IV.	Section-by-Section Analysis of the Bill, as Reported	4
V.	Evaluation of Regulatory Impact	7
VI.	Congressional Budget Office Cost Estimate	8
VII.	Changes in Existing Law Made by the Bill, as Reported	10

I. PURPOSE AND SUMMARY

S. 2274, the Federal Cybersecurity Workforce Expansion Act, augments cybersecurity workforce development pathways by adding two new pilot programs. The bill establishes a five-year cybersecurity registered apprenticeship pilot program within the Department of Homeland Security (DHS). The bill also directs the Secretary of Homeland Security, in coordination with the Secretary of

Veterans Affairs, to establish a pilot program to provide cybersecurity training at no cost to veterans and military spouses.

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 nearly 600,000 cybersecurity job openings in the United States, including nearly 40,000 in the public sector.[1]

The consistent shortage of cybersecurity personnel represents a high risk to national security. Federal cyber workforce management challenges have been on the High-Risk List of the Government Accountability Office (GAO) since 2003.[2] In a 2003 High-Risk Series report, GAO stated:

> Agencies 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. The availability of adequate technical and audit expertise is a continuing concern to agencies.[3]

In a March 2021 High-Risk Series report, GAO noted that "federal agencies continue to face challenges in addressing needs related to their cyber workforce" and that the Office of Management and Budget and DHS need to take dedicated action to address the cybersecurity workforce shortage.[4]

The problem of cybersecurity workforce shortages has taken on new urgency as the United States faces escalating threats from hostile cyber actors. On May 12, 2021, multiple high-profile cybersecurity incidents including the SolarWinds security breach, Microsoft Exchange Server hack, and Colonial Pipeline ransomware attack prompted President Biden to issue an Executive Order aimed at improving the nation's cybersecurity preparedness systems.[5] As part of the Biden Administration's cyber preparedness efforts, DHS Secretary Mayorkas launched a 60–Day Cybersecurity Workforce Sprint in early May 2021.[6] On July 1, 2021, the Secretary announced that 12% of over 2,000 vacancies had been filled as a result of the hiring sprint, noting that although progress has been made, "we still have more work to do."[7]

The Senate Committee on Homeland Security and Governmental Affairs has held multiple hearings in the 117th Congress to ad-

---

[1] Cyberseek, Interactive Map (www.cyberseek.org/heatmap.html) (accessed Dec. 14, 2021).

[2] 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).

[3] *Id.*

[4] Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO–21–288) (Mar. 2021) (www.gao.gov/assets/gao-21-288.pdf).

[5] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

[6] Department of Homeland Security, *Secretary Mayorkas Urges Small Businesses to Protect Themselves Against Ransomware* (May 5, 2021) (www.dhs.gov/news/2021/05/05/secretary-mayorkas-urges-small-businesses-protect-themselves-against-ransomware).

[7] Department of Homeland Security, *Secretary Mayorkas Announces Most Successful Cybersecurity Hiring Initiative in DHS History* (July 1, 2021) (www.dhs.gov/news/2021/07/01/secretary-mayorkas-announces-most-successful-cybersecurity-hiring-initiative-dhs).

dress the government's preparedness, response, and recovery efforts with regard to cybersecurity.[8] During one such hearing on September 23, 2021, entitled *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems*, Senator Margaret Hassan asked Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), about how an apprenticeship program would help address workforce challenges at CISA.[9] 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.[10]

Fellow witness Chris Inglis, National Cyber Director in the Executive Office of the President, agreed with Director Easterly's remarks and added that:

> [A]pprenticeships 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]

The Federal Cybersecurity Workforce Expansion Act will help 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 excepted service positions within a federal agency. Appointed participants then 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.

The Federal Cybersecurity Workforce Expansion Act also directs the Secretary of Homeland Security, in partnership with the Secretary of Veterans Affairs, to establish a pilot program to provide cybersecurity training at no cost to veterans and military spouses. The pilot program will incorporate coursework, virtual learning opportunities, and federal work-based learning opportunities and will lead to a recognized postsecondary credential.

This bill incorporates recommendations from a report published by the Cyberspace Solarium Commission in March 2020. The report recommends that the federal government "develop work-based learning programs and apprenticeships to supplement classroom

---

[8] *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); 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); *and* 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).

[9] 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) (https://plus.cq.com/doc/congressionaltranscripts-6351036?4&searchId=9Svfjbqf).

[10] *Id.*

[11] *Id.*

learning" as a step to improve cyber-oriented education.[12] Another recommendation calls for designing "cybersecurity-specific upskilling and transition assistance programs for veterans and transitioning military service members to move into federal civilian cybersecurity jobs."[13] The Federal Cybersecurity Workforce Expansion Act will help bring these expert recommendations to fruition and improve our national security by augmenting cybersecurity workforce development pathways.

III. Legislative History

Senator Margaret Hassan (D–NH) introduced S. 2274, the Federal Cybersecurity Workforce Expansion Act, on June 24, 2021, with Senator John Cornyn (R–TX). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2274 at a business meeting on November 3, 2021. During the business meeting, Senator Hassan offered a modification to her substitute amendment that was adopted by unanimous consent. The substitute amendment made a number of changes to the underlying bill, including a change to establish the veterans' cybersecurity training pilot program at the Department of Homeland Security rather than the Department of Veterans Affairs and setting a cap on the number apprentices in the cybersecurity apprenticeship pilot program. The modification to the substitute amendment cut the language authorizing "such sums as necessary" to carry out the cybersecurity apprenticeship pilot program. As modified, Senator Hassan's substitute amendment was adopted by unanimous consent.

Senator Lankford offered an amendment to change the standard by which agencies can use direct hire authority, which was not adopted by voice vote.

The bill, as amended by the Hassan modified substitute amendment, was ordered reported favorably by voice vote *en bloc*, with Senators Peters, 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 establishes the short title of the bill as the "Federal Cybersecurity Workforce Expansion Act."

Sec. 2. Findings

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

Sec. 3. Definitions

This section defines "Department," "institution of higher education," and "Secretary" in the context of this bill.

Sec. 4. Cybersecurity apprenticeship pilot program

Subsection (a) defines "area career and technical education school," "community college," "competitive service," "cyber work-

[12] Cyberspace Solarium Commission, *A Warning From Tomorrow* (Mar. 2020) (drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).
[13] *Id.* at 44.

force 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," "qualified intermediary," "partnerships," "provider of adult education," "related instruction," "sponsor," "state," "state apprenticeship agency," "state workforce development board," and "WIOA terms" in the context of this section.

Subsection (b) directs the Secretary of Homeland Security to establish an apprenticeship pilot program within three years of this bill's enactment. There can be up to 25 apprentices who will be employed in cyber workforce positions within DHS while participating in the program. The learning opportunities in the program will be based on the NICE Workforce Framework for Cybersecurity, or a successor framework, and prepare the participant for a cyber workforce position within a federal agency. The program must be a registered apprenticeship and approved by the Department of Veterans Affairs as an apprenticeship where veterans can use their educational assistance.

Subsection (c) directs the Secretary of Homeland Security to consult with the Secretary of Labor, the Director of NIST, the Secretary of Defense, the Director of the National Science Foundation, and the Director of the Office of Personnel Management (OPM) when developing the apprenticeship pilot program.

Subsection (d) outlines options available to the DHS Secretary for getting help implementing the apprenticeship program including contracts, cooperative agreements, or grants. The entity chosen to provide the program must have demonstrated experience in implementing apprenticeship programs, have knowledge of cybersecurity workforce development, have an ability 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 program.

Subsection (e) describes how eligible entities seeking a contract, cooperative agreement, or grant under subsection (d) must submit an application to the DHS Secretary with such information as the Secretary may require.

Subsection (f) states that the Secretary may prioritize an eligible entity in the context of subsection (d) that: (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 Armed Forces 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) has focused on recruiting women, minorities, and individuals from other underrepresented communities.

Subsection (g) directs the DHS Secretary 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 individuals who successfully complete the apprenticeship program to enter into an agreement in which they accept an offer for a cyber workforce position within a federal agency and serve in that position 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 will be required to repay the cost of the education and training provided, reduced by an amount factoring in the extent to which any service obligations were met. The Secretary is authorized to provide a waiver of service or repayment requirements as appropriate.

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 position in the excepted service.

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

Subsection (l) requires the Secretary to submit an annual report starting two years after the beginning of the apprenticeship program that includes a description of: (1) any activity carried out by DHS under this section; (2) any eligible entity selected and activity carried out under subsection (d); (3) best practices used; (4) an assessment of the results achieved by the apprenticeship program, including the rate of continued employment within a federal agency, the demographics of the apprenticeship participants, the rate of completion by program participants, and the return on investment of the pilot program. This subsection also directs the 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 in five years.

Sec. 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."

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

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 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 and prevent duplication of existing training, platforms, and frameworks within the federal government for cybersecurity education and

training. The DHS Secretary is directed to coordinate with the Secretary of Veterans Affairs to ensure that eligible individuals can use existing educational assistance to the greatest extent possible. The DHS Secretary is directed to coordinate with the Secretary of Veterans Affairs, Secretary of Defense, Secretary of Labor, Director of OPM, and any other appropriate agencies to identify and create interagency opportunities to allow program participants to demonstrate competencies necessary to qualify for federal employment.

Subsection (f) authorizes the Secretary to expand existing training, platforms, and frameworks or develop and procure resources as necessary to carry out the program. The Secretary 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 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; (3) the results achieved by the apprenticeship program, including the admittance rate into the 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 the GAO to conduct a study on the pilot program within four years after the program is established.

Subsection (h) sunsets the pilot program in five years.

Sec. 6. Federal cybersecurity workforce assessment extension

This section extends from 2022 to 2025 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

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, February 3, 2022.

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. 2274, the Federal Cybersecurity Workforce Expansion 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.

At a Glance

S. 2274, Federal Cybersecurity Workforce Expansion Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on November 3, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	*	25	not estimated

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 2032?	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. 2274 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.

S. 2274 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. 2274 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF S. 2274

	By fiscal year, millions of dollars—					
	2022	2023	2024	2025	2026	2022–2026
Cybersecurity Apprentices						
Estimated Authorization	0	2	5	5	5	17
Estimated Outlays	0	2	5	5	5	17
Curriculum and Training						
Estimated Authorization	0	4	0	0	0	4
Estimated Outlays	0	2	2	0	0	4
Program Management Staff						
Estimated Authorization	*	1	1	1	1	4
Estimated Outlays	*	1	1	1	1	4
Total Changes.						
Estimated Authorization	*	7	6	6	6	25
Estimated Outlays	*	5	8	6	6	25

* = between zero and $500,000.

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2274 would have insignificant effects on direct spending and the deficit over the 2022–2031 period.

Basis of estimate: For this estimate, CBO assumes that S. 2274 will be enacted in the middle of fiscal year 2022 and that the required pilot programs would begin in fiscal year 2023. CBO also expects that cybersecurity apprentices would serve for a two-year term. Outlays are based on historical spending patterns for existing or similar programs.

Spending subject to appropriation: CBO estimates that implementing the bill would cost $25 million over the 2022–2026 period. Such spending would be subject to the availability of appropriated funds.

Cybersecurity Apprentices. S. 2274 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 apprenticeships, CBO expects that each apprentice would serve for two years at an average annual cost of about $85,000 for salaries and benefits. CBO anticipates that DHS would hire the first cohort of apprentices in 2023 and that each cohort would include 25 people, the maximum annual number of new hires permitted under S. 2274. 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 salaries and benefits expenses of apprentices hired under S. 2274 would total $17 million over the 2023–2026 period.

Curriculum and Training. S. 2274 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 de-

sign the curricula for these courses and create the 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 $4 million.

Program Management Staff. Using information about similar training programs, CBO anticipates that DHS would need five full-time employees to create and manage these new programs. CBO estimates that staff salaries would average about $1 million annually over the 2022–2026 period.

Direct Spending: Several provisions in S. 2274 would have insignificant effects on direct spending over the 2022–2031 period.

Cybersecurity Training for Veterans and Military Spouses. CBO expects that some veterans who are eligible for education benefits administered by VA would increase their use of those benefits as a result of the cybersecurity training program. Conversely, 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 2022–2031 period.

Cyber Security Workforce Assessment Extension. S. 2274 would extend, from 2022 to 2025, 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 S. 2274 would have insignificant effects on direct spending and the deficit.

Increase in long-term 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, Leo Lex, Deputy Director of Budget Analysis; Theresa Gullo, Director of Budget Analysis.

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):

UNITED STATES CODE

* * * * * * *

TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES

* * * * * * *

PART I—THE AGENCIES GENERALLY

* * * * * * *

CHAPTER 3—POWERS

* * * * * * *

SEC. 301. DEPARTMENTAL REGULATIONS

* * * * * * *

STATUTORY NOTES

* * * * * * *

FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

* * * * * * *

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] *2025*, 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 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.

* * * * * * *

○