

Calendar No. 177

117TH CONGRESS }
1st Session }

SENATE

{ REPORT
117-47

FEDERAL ROTATIONAL CYBER WORKFORCE
PROGRAM ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 1097

TO ESTABLISH A FEDERAL ROTATIONAL CYBER WORKFORCE
PROGRAM FOR THE FEDERAL CYBER WORKFORCE



DECEMBER 6, 2021.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

29-010

WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	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*

ANDREW C. DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*

AMANDA H. NEELY, *Minority Director of Governmental Affairs and General Counsel*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 177

117TH CONGRESS }
1st Session }

SENATE

{ REPORT
117-47

FEDERAL ROTATIONAL CYBER WORKFORCE PROGRAM
ACT OF 2021

DECEMBER 6, 2021.—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. 1097]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1097), to establish a Federal rotational cyber workforce program for the Federal cyber workforce, having considered the same, reports favorably thereon without amendment and recommends that the bill 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	6
VI. Congressional Budget Office Cost Estimate	6
VII. Changes in Existing Law Made by the Bill, as Reported	7

I. PURPOSE AND SUMMARY

S. 1097, the Federal Rotational Cyber Workforce Program Act of 2021, creates a rotational cyber workforce program in which Federal employees in cyber workforce positions can be detailed to another agency to perform cyber functions. This program will enable Federal cyber workforce employees to enhance their cyber skills

with experience from executing the cyber missions of other agencies.¹

II. BACKGROUND AND NEED FOR THE LEGISLATION

Federal cyber workforce management challenges have been on the High-Risk List of the Government Accountability Office (GAO) since 2003.² 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.³

In 2011, GAO reported that many Federal agencies still experienced difficulty hiring employees for more technical cyber positions or for positions that require other more specialized skills.⁴ In its 2017 High Risk List, GAO reported:

[T]he federal government needs to expand its cyber workforce planning and training efforts. Federal agencies need to enhance efforts for recruiting and retaining a qualified cybersecurity workforce and improve cybersecurity workforce planning activities.⁵

The Federal Cybersecurity Workforce Assessment Act of 2015 initiated cyber workforce planning efforts by requiring agencies to identify cyber positions in the Federal workforce.⁶ The Office of Personnel Management (OPM), the agency tasked with managing human resources of the Federal Government, issued guidance for Federal agencies to identify their current cyber workforce positions.⁷ OPM's guidance included a deadline of April 2019 for Federal agencies to "report their greatest skill shortages; analyze the root cause of the shortages; and provide action plans, targets and measures for mitigating the critical skill shortages."⁸ OPM stated it would use these agency reports to "identify common needs to address from the Governmentwide perspective."⁹

¹On February 13, 2019, the Committee approved S. 406, Federal Rotational Cyber Workforce Program Act of 2019. That bill is substantially similar to S. 1097. Accordingly, this committee report is in large part a reproduction of Chairman Johnson's committee report for S. 406, S. Rep. No. 116-15.

²Government Accountability Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures* (GAO-03-121) (Jan. 2003) (<https://www.gao.gov/assets/gao-03-121.pdf>).

³*Id.*

⁴Government Accountability Office, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, (GAO-12-8) (Nov. 2011) (<https://www.gao.gov/assets/gao-12-8.pdf>).

⁵Government Accountability Office, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, (GAO-17-317) (Feb. 2017) (<https://www.gao.gov/assets/gao-17-317.pdf>).

⁶Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, § 303, 129 Stat. 2242, 2975, 2975-77 (2015) (<https://www.congress.gov/113/plaws/publ246/PLAW-113publ246.pdf>).

⁷Memorandum from Mark D. Reinhold, Associate Director, Employee Services, Office of Personnel Management, to Human Resource Directors, U.S. Government regarding Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need (Apr. 2, 2018) (<https://www.chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need>).

⁸*Id.*

⁹*Id.*

GAO has consistently highlighted the urgent need to address cybersecurity workforce management challenges, including the continuing cybersecurity workforce shortage.¹⁰ GAO also encouraged Congress and the Executive Branch to pass legislation and implement policies that would help recruit, develop, and retain cyber talent.¹¹ On May 11, 2017, President Trump issued an Executive Order with the goal of strengthening the cybersecurity of Federal networks and critical infrastructure.¹² The order required the Secretaries of Commerce and Homeland Security, in consultation with others, to conduct a joint assessment of the scope and sufficiency of efforts to fortify the American cybersecurity workforce, including education, training, and apprenticeship programs.¹³

On May 2, 2019, President Trump signed a subsequent Executive Order requiring the Secretary of Homeland Security, in consultation with the Directors of OMB and OPM, to establish a cybersecurity rotational assignment program aimed at strengthening the skills and capabilities of the Federal cybersecurity workforce.¹⁴ The program would detail cybersecurity professionals from other agencies to the Department of Homeland Security (DHS), as well as detail DHS cybersecurity professionals to other agencies.¹⁵ The order also required the Director of OPM to generate a list of cybersecurity aptitude assessments for agencies to use in identifying employees who would excel in these rotational programs.¹⁶

A memorandum issued by the Acting Director of OPM on November 19, 2020, further called on Federal agencies to utilize rotational programs to enhance the Federal cybersecurity workforce.¹⁷ The Director highlighted three existing rotational programs: the President's Management Council Interagency Program, the Cybersecurity Reskilling Detail Program, and the Federal Cybersecurity Rotation Program (as established by Executive Order 13870).

On May 12, 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.¹⁸ The Senate Committee on Homeland Security and Governmental Affairs held multiple hearings in the wake of these cybersecurity attacks to address the Government's preparedness, response, and recovery efforts.¹⁹ These cyber-attacks further underscored the urgent need to advance skills of the Nation's cybersecurity workforce.

This bill would complement the Federal cyber workforce initiatives begun under the Federal Cybersecurity Workforce Assessment

¹⁰ Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, (GAO-21-288) (2021) (<https://www.gao.gov/assets/gao-21-288.pdf>)

¹¹ *Id.*

¹² Executive Order No. 13,800, 82 Fed. Reg. 22,397 (May 11, 2017).

¹³ *Id.*

¹⁴ Executive Order No. 13,870, 84 Fed. Reg. 20,523 (May 9, 2019).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ Memorandum from Michael J. Rigas, Acting Director, U.S. Office of Personnel Management, to the Heads of Executive Departments and Agencies regarding Guidance for Federal Cybersecurity Rotational Assignments (Nov. 18, 2020) (<https://www.chcoc.gov/content/guidance-federal-cybersecurity-rotational-assignments>).

¹⁸ Executive Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

¹⁹ See *Prevention, Response and Recovery: Improving Federal Cybersecurity Post-SolarWinds before the Senate Committee on Homeland Security and Governmental Affairs*, 117th Cong. (2021); *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack before the Senate Committee on Homeland Security and Governmental Affairs*, 117th Cong. (2021).

Act of 2015 and subsequent Executive Orders by creating a Federal rotational cyber workforce program in which cyber personnel can detail to other agencies to help fill skills gaps for agencies' cyber-related functions. Though similar in many ways to existing rotational programs, the Federal rotational cyber workforce program is distinct in its scope and purpose: this program would allow for rotational details government-wide for cybersecurity professionals in both the competitive and excepted services. This bill also houses the program at OPM, recognizing its function as the leader in strategic human capital planning for the Federal government.

S. 1097 requires Federal agencies to determine which cyber positions should be eligible for the rotation and report those positions to OPM. OPM will then distribute a list of positions available for participation in the program to each agency. It also requires OPM, the Chief Human Capital Officers Council, the Chief Information Officers Council, and DHS to develop an operation plan for the Federal rotational cyber workforce program that establishes the procedures and requirements for the program, including the employee application and selection process and agency management of cyber employees participating in the program.

The bill limits an employee's participation in the Federal rotational cyber workforce program to a period of one year, with the option for a 60-day extension. Once a cyber employee completes participation in the program, the employee is required to return to the Federal agency from which he or she was detailed to serve for a period of time that is equal in length to the period of the detail.

The Federal rotational cyber workforce program sunsets five years after the date of enactment of this bill. This bill also requires GAO to issue a report on the program and any effect the program has on improving Federal employees' cyber-related skills or on intra-agency and interagency coordination of cyber functions and personnel management.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 1097, the Federal Rotational Cyber Workforce Program Act of 2021 on April 13, 2021, with Senators John Hoeven (R–ND), and Jacky Rosen (D–NV). The bill was referred to the Committee on Homeland Security and Governmental Affairs on April 13, 2021.

The Committee considered S. 1097 at a business meeting on May 12, 2021. The legislation was passed by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley present.

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

Section 1. Short title

This section established the short title of the bill as the “Federal Rotational Cyber Workforce Program Act of 2021.”

Section 2. Definitions

This section defines the terms “agency,” “competitive service,” “Councils,” “cyber workforce position,” “Director,” “employee,” “em-

ploying agency,” “excepted service,” “rotational cyber workforce position,” “rotational cyber workforce program,” and “Secretary.”

Section 3. Rotational cyber workforce positions

This section determines how agencies will select positions that are eligible for participation in the Federal rotational cyber workforce program.

Under subsection (a), the head of an agency determines whether a cyber workforce position is eligible for participation in the program and submits to the OPM Director a notice of such determination.

Subsection (b) requires the OPM Director, with assistance from the Chief Human Capital Officers Council, the Chief Information Officers Council, and the Department of Homeland Security, to develop a list of rotational cyber workforce positions in the program and information about each position.

Subsection (c) requires the OPM Director to distribute the list developed under subsection (b) on an annual basis to each agency.

Section 4. Rotational cyber workforce program

This section prescribes the development and operation of the Federal rotational cyber workforce program.

Subsection (a) requires the OPM Director to consult with the Chief Human Capital Officers Council, the Chief Information Officers Council, and the Secretary of Homeland Security and develop and issue an operation plan for the Federal rotational cyber workforce program, which may be implemented through existing mechanisms.

Subsection (b) lists requirements for the operation plan developed in subsection (a). The operation plan must identify agencies and establish procedures for participation in the program, such as requirements for training, education, and career development for participation and any other prerequisites or other requirements to participate. The operation plan for the program must also include performance measures and other accountability measures in order to evaluate the program. The plan must ensure voluntary participation in the program and agency approval of any participating employee. The operation plan must also establish the logistics of detailing employees between agencies or at other agencies on a non-reimbursable basis, of managing employees detailed in the program, and of returning program participants to their positions in their employing agencies after participating in the program.

Subsection (c) establishes the process by which employees are selected to participate in the program. An employee in a cyber workforce position must seek approval from their agency to apply for a rotational cyber workforce position included in the list of eligible program positions developed under subsection 3(b). Employees serving in the excepted service must get prior approval from OPM in order to be selected for a rotational cyber workforce position. When selecting participants for a rotational cyber workforce position, the agency in which that position is located must adhere to the merit system principles. The duration of a detail to a rotational cyber workforce position under this program is for a period of 180 days to up to 1 year, with an option to extend this period for up to an additional 60 days. Under this subsection, an employee par-

ticipating in the program must enter into a written service agreement with the employing agency to complete a period of employment after participating in the program.

Section 5. Reporting by GAO

This section requires GAO to assess and report on the operation of the Federal rotational cyber workforce program and any effect the program has on improving employees' cyber-related skills or on intra-agency and interagency coordination of cyber functions and personnel management.

Section 6. Sunset

Under this section, the Federal rotational cyber workforce program terminates five years after the date of enactment of this bill.

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

NOVEMBER 4, 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. 1097, the Federal Rotational Cyber Workforce Program Act of 2021.

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

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 1097, Federal Rotational Cyber Workforce Program Act of 2021			
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on May 12, 2021			
By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	*	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	*	*	*
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 zero and \$500,000.			

S. 1097 would direct the Office of Personnel Management to create policies and procedures to allow federal cybersecurity professionals to temporarily work for another agency for up to one year. That requirement would expire five years following enactment. In addition, the bill would require the Government Accountability Office to report to the Congress on the effectiveness of the rotational program.

CBO estimates that implementing S. 1097 would cost less than \$500,000 over the 2022–2026 period to issue regulations, train staff, and prepare the required report. Such spending would be subject to the availability of appropriations.

Enacting S. 1097 could affect direct spending by some agencies that can use fees, receipts from the sale of goods, and other collections to cover operating costs. Because most of those agencies can adjust amounts collected to reflect changes in operating costs, any net changes in direct spending by those agencies would be negligible, CBO estimates.

On July 21, 2021, CBO transmitted a cost estimate for H.R. 3599, the Federal Rotational Cyber Workforce Program Act of 2021, as ordered reported by the House Committee on Oversight and Reform on June 29, 2021. The two bills are similar, and CBO's estimates of their costs are similar. Differences in CBO's estimates of the cost of implementing the bills reflect the assumption that H.R. 3599 would have been enacted in 2021.

The CBO staff contact for this estimate is Aldo Prospero. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

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

Because S. 1097 would not repeal or amend any provision of current law, it would make no changes in existing law within the meaning of clauses (a) and (b) of paragraph 12 of rule XXVI of the Standing Rules of the Senate.