Calendar No. 348

117TH CONGRESS *2d Session*	SENATE	REPORT 117–97

CIVILIAN CYBERSECURITY RESERVE ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1324

TO ESTABLISH A CIVILIAN CYBER SECURITY RESERVE AS A PILOT PROJECT TO ADDRESS THE CYBER SECURITY NEEDS OF THE UNITED STATES WITH RESPECT TO NATIONAL SECURITY, AND FOR OTHER PURPOSES

APRIL 27, 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*
DEVIN PARSONS, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
CARA G. MUMFORD, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 348

117TH CONGRESS *2d Session* | SENATE | REPORT 117–97

CIVILIAN CYBERSECURITY RESERVE ACT

APRIL 27, 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. 1324]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1324) to establish a Civilian Cyber Security Reserve as a pilot project to address the cyber security needs of the United States with respect to national security, 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

I. PURPOSE AND SUMMARY

S. 1324, the Civilian Cybersecurity Reserve Act, establishes a Civilian Cybersecurity Reserve as a four-year pilot project to provide the Cybersecurity and Infrastructure Security Agency (CISA) with qualified civilian personnel to respond to significant cyber incidents.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Federal agencies are experiencing a significant shortage of cybersecurity talent. According to CyberSeek, a project supported by the

National Initiative for Cybersecurity Education at the National Institute of Standards and Technology within the Department of Commerce, the supply of cybersecurity workers in the public sector relative to demand is "very low."[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 that 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 stated, "federal agencies continue to face challenges in addressing needs related to their cyber workforce" and that the Office of Management and Budget and the Department of Homeland Security (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 SolarWinds, Microsoft Exchange, and Colonial Pipeline, prompted President Biden to issue an Executive Order aimed at improving the nation's cybersecurity preparedness systems.[5] 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.[6] These cyber-attacks further underscored the urgent need to advance skills of the nation's cybersecurity workforce.

As part of the Biden Administration's cyber preparedness efforts, DHS Secretary Mayorkas launched a 60-Day Cybersecurity Workforce Sprint in early May 2021.[7] On July 1, 2021, the Secretary announced that 12 percent 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."[8]

---

[1] Cyberseek, Interactive Map (www.cyberseek.org/heatmap.html) (accessed Aug. 26, 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] Executive Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

[6] 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).

[7] 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).

[8] 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).

The Civilian Cybersecurity Reserve Act will help address the continued federal cyber personnel shortages by establishing a surge capacity to better ensure that the U.S. cyber workforce is well-positioned to respond to significant cyberattacks. This bill authorizes civilian cybersecurity personnel to serve in temporary positions, for up to six months, as federal civil service employees to supplement CISA's cybersecurity personnel. Participation in the Civilian Cybersecurity Reserve would be voluntary and by invitation. CISA is authorized to activate up to 30 reserve personnel at a time.

The Civilian Cybersecurity Reserve Act is modeled after recommendations from the National Commission on Military, National, and Public Service as well as the Cyberspace Solarium Commission. In March 2020, the National Commission on Military, National, and Public Service released a Final Report recommending that Congress authorize a pilot program to create a "Federal Civilian Cybersecurity Reserve."[9] The report states:

> A reserve program that permits agencies to call up cybersecurity experts could ensure additional cyber capacity at times of greatest need. By building the reserve program around cybersecurity experts who have left Government service for other opportunities, the program would also help the Government to maximize the value of taxpayer investment in developing their expertise.[10]

A report by the Cyberspace Solarium Commission, also released in March 2020, similarly recommends that Congress assess the need for a military cyber reserve to "play a central role in mobilizing a surge capacity" while utilizing preexisting links with the private sector.[11] The Civilian Cybersecurity Reserve Act would help bring these expert recommendations to fruition and improve our national security by bolstering the federal cybersecurity workforce.

III. LEGISLATIVE HISTORY

Senator Jacky Rosen (D–NV) introduced S. 1324, the Civilian Cybersecurity Reserve Act on April 22, 2021, with Senator Marsha Blackburn (R–TN). The bill was referred to the Committee on Homeland Security and Governmental Affairs on April 22, 2021.

The Committee considered S. 1324 at a business meeting on July 14, 2021. The legislation was passed by voice vote *en bloc* as amended by a Rosen Substitute Amendment as modified, with Senators Peters, Hassan, 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 established the short title of the bill as the "Civilian Cybersecurity Reserve Act."

---

[9] National Commission on Military, National, and Public Service, *Inspired to Serve: The Final Report of the National Commission on Military, National, and Public Service* (Mar. 2020).

[10] *Id.*

[11] Cyberspace Solarium Commission (Mar. 2020) (drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

Sec. 2. Civilian Cybersecurity Reserve pilot project

Subsection (a) includes definitions of the terms "Agency," "appropriate congressional committees," "competitive service," "Director," "excepted service," "significant incident," "temporary position," and "uniformed services."

Subsection (b) authorizes the Director of CISA to establish a Civilian Cybersecurity Reserve pilot project for the purpose of effectively responding to significant incidents. When a significant incident occurs, the Director may activate reservists by appointing up to 30 individuals to temporary positions for up to six months in the competitive service or excepted service, notifying Congress whenever a reservist is activated. The reservists are considered federal civil service employees when deployed. The Department of Labor (DOL) would promulgate regulations related to job protections for reservists before and after a temporary appointment to the federal civil service.

Subsection (c) instructs the Director of CISA to develop criteria for eligibility and the application and selection process for the Civilian Cybersecurity Reserve. The eligibility requirements must include an individual's previous employment and cybersecurity expertise. CISA is directed to prioritize the appointment of individuals previously employed by the executive branch or within the uniformed services. Individuals who have worked for a federal contractor within the executive branch or for a state, local, tribal, or territorial government would also be eligible. If an individual has previously served in the Civilian Cybersecurity Reserve, at least 60 days must pass before a subsequent temporary appointment. Prior to being appointed, each individual will be screened for anything that might create a conflict of interest. A member of the Selected Reserve may not be a member of the Civilian Cybersecurity Reserve, nor can individuals who are currently employed by the executive branch.

Subsection (d) instructs the Director of CISA to ensure that all members of the Civilian Cybersecurity Reserve undergo appropriate personnel vetting and adjudication commensurate with the duties of the position, including access to classified information where a security clearance is needed. CISA will be responsible for any costs related to a member of the Civilian Cybersecurity Reserve obtaining their security clearance.

Subsection (e) directs CISA to begin a study within 60 days after enactment on the design and implementation of the pilot project, including on the following: (1) compensation and benefits for reservists; (2) activities that reservists may undertake as part of their duties; (3) methods for identifying and recruiting reservists; (4) methods for preventing conflicts of interest; (5) resources needed to carry out the pilot project; (6) possible penalties for individuals who fail to respond to activation; and (7) processes and requirements for training and onboarding reservists. Within one year after beginning the study, CISA must submit and provide a briefing on an implementation plan to the appropriate congressional committees.

Subsection (f) instructs the Director of CISA to consult with the Office of Personnel Management and Office of Government Ethics and issue guidance on implementing the pilot project within two years after enactment.

Subsection (g) directs CISA to provide a briefing on the pilot project to the appropriate congressional committees once per year starting within one year of enactment on subjects including: (1) participation in the Civilian Cybersecurity Reserve, including the number of participants, diversity of participants, and barriers to recruitment or retention; (2) an evaluation of the ethical requirements of pilot project; (3) whether the Civilian Cybersecurity Reserve has been effective in providing additional capacity to CISA during significant incidents; and (4) an evaluation of eligibility requirements for the pilot project. Between six months to three months before the pilot project terminates, CISA must submit a report and a provide briefing to Congress on recommendations relating to the pilot project.

Subsection (h) directs the GAO to evaluate the pilot project within three years after it is established.

Subsection (i) states that the pilot project shall terminate four years after the date on which it is established.

Subsection (j) states 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 some regulatory impact within the meaning of the rules. The bill requires:

> DOL to prescribe antidiscrimination and employment protections at least as stringent as those in the Uniformed Services Employment and Reemployment Rights Act. That act requires employers to provide employees with the same benefits, pay, and seniority when returning from deployment that they would have received had they not been away. The act also requires employers to treat workers on active military duty as furloughed employees or as employees on a leave of absence, entitling them to any compensation or benefits otherwise available to them in that status.[12]

The Committee agrees with the Congressional Budget Office's statement that because the bill limits the Civilian Cybersecurity Reserve to 30 members at a time, the cost to employers would be small and well below the annual threshold established in Unfunded Mandates Reform Act (UMRA) for intergovernmental and private-sector mandates.

[12] Congressional Budget Office, *S. 1324, Civilian Cybersecurity Reserve Act Cost Estimate* (Aug. 13, 2021) (https://www.cbo.gov/system/files/2021-08/s1324.pdf).

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 13, 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. 1324, the Civilian Cybersecurity Reserve Act.

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

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 1324, Civilian Cybersecurity Reserve Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 14, 2021

By Fiscal Year, Millions of Dollars	2021	2021-2026	2021-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	63	not estimated

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 2032?	No	Contains intergovernmental mandate?	Yes, Under Threshold
		Contains private-sector mandate?	Yes, Under Threshold

Bill summary: S. 1324 would authorize the Cybersecurity and Infrastructure Security Agency (CISA) to establish the Civilian Cybersecurity Reserve under a four-year pilot program. CISA would appoint cybersecurity professionals who are members of the reserve to temporary federal civilian positions within the agency to respond to significant national security threats. CISA would be required to report regularly to the Congress on the program's effectiveness.

Estimated Federal cost: For this estimate, CBO assumes that S. 1324 will be enacted near the beginning of fiscal year 2022. The costs of the legislation, detailed in Table 1, fall within budget function 050 (national defense). Implementing the bill would cost $63 million over the 2021–2026 period, CBO estimates; such spending would be subject to the availability of appropriated funds.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 1324

	By fiscal year, millions of dollars—						
	2021	2022	2023	2024	2025	2026	2021–2026
Civilian Cybersecurity Reserve:							
Estimated Authorization	0	0	7	15	15	16	53
Estimated Outlays	0	0	7	15	15	16	53
Program Management:							
Estimated Authorization	0	1	2	2	2	3	10
Estimated Outlays	0	1	2	2	2	3	10
Total Changes:							
Estimated Authorization	0	1	9	17	17	19	63
Estimated Outlays	0	1	9	17	17	19	63

Under S. 1324, CISA would recruit and train members of the reserve group and mobilize as many as 30 at a time to serve as federal civilian employees for up to six months within a year. Activated reservists would augment CISA's workforce by detecting and responding to malicious activity in federal and nonfederal information networks. The bill would require CISA to complete plans for the initiative within one year; CBO anticipates that the reserve would begin to operate in 2023.

CBO expects that the costs to pay and equip the reservists would be comparable to the costs incurred for CISA's Cyber Defense Teams—about $440,000 annually per employee, on average. About half of that amount would cover salaries and benefits; the rest would pay for network sensors, other equipment, and software licenses. CBO expects that CISA would activate reservists at a rate sufficient to keep the 30 authorized positions fully staffed each year. On that basis, CBO estimates, it would cost $53 million over the 2021–2026 period to staff and operate the reserve.

CBO also expects that a program management office would administer recruitment, training, logistics, and security clearances and the office would ensure that a sufficient pool of reservists was available to maintain 30 activated reservists at all times. Using information about the costs of similar efforts, CBO estimates that CISA would hire 10 new employees to manage the program at a total cost of $10 million over the 2021–2026 period.

Uncertainty: Areas of uncertainty in this estimate include identifying the conditions under which CISA would activate the reserve. S. 1324 would provide CISA broad latitude for making that determination. Although CBO expects that the agency would use the full number authorized under the bill, if fewer than 30 reservists were activated at any time, the budgetary effects would be proportionately smaller than estimated.

Mandates: S. 1324 bill would impose both an intergovernmental and a private-sector mandate as defined in the Unfunded Mandates Reform Act (UMRA) on public and private-sector employers of activated members of the Civilian Cybersecurity Reserve. The bill also would require the Department of Labor (DOL) to prescribe antidiscrimination and employment protections at least as stringent as those in the Uniformed Services Employment and Reemployment Rights Act. That act requires employers to provide employees with the same benefits, pay, and seniority when returning from deployment that they would have received had they not been away. The act also requires employers to treat workers on active military duty

as furloughed employees or as employees on a leave of absence, entitling them to any compensation or benefits otherwise available to them in that status.

The cost of the mandate would be the cost to the employers that provide the benefits as well as the cost of any other protections DOL requires. Although the mandate's ultimate cost would depend on those regulations, the bill limits the number of activated reservists to 30 at a time. Therefore, CBO estimates, the cost to employers would be small and well below the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($85 million and $170 million in 2021, respectively, adjusted annually for inflation).

Estimate prepared by: Federal Costs: Aldo Prosperi; 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; Leo Lex, Deputy Director of Budget Analysis; Theresa Gullo, Director of Budget Analysis.

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

Because S. 1324 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.

○