Calendar No. 204

118TH CONGRESS *1st Session*	SENATE	REPORT 118–96

DEPARTMENT OF HOMELAND SECURITY 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. 885

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

SEPTEMBER 11, 2023.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 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
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	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*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 204

118TH CONGRESS *1st Session* | SENATE | REPORT 118–96

DEPARTMENT OF HOMELAND SECURITY CIVILIAN CYBERSECURITY RESERVE ACT

SEPTEMBER 11, 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. 885]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 885), to establish a Civilian Cybersecurity Reserve in the Department of Homeland Security as a pilot project to address the cybersecurity 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. 885, the *Department of Homeland Security (DHS) 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. When a significant incident occurs, the Director of CISA may activate reservists by appointing up to 30 individuals to temporary positions for up to six

months, and they must notify Congress whenever a reservist is activated. The bill also directs CISA to begin a study within 60 days after enactment on the design and implementation of the pilot project, present an implementation plan to Congress within one year of beginning the study, and provide an annual briefing on the pilot project. Finally, the bill directs the Government Accountability Office (GAO) to evaluate the pilot project within three years after the pilot is established.[1]

II. BACKGROUND AND NEED FOR THE LEGISLATION

Federal agencies are experiencing a significant shortage of cybersecurity talent. According to CISA's September 2022 *State of the Federal Cyber Workforce* report, CISA has concluded: "[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 notes that "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."[2]

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.[3] 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.[4]

Since 2003, the need for a developed cyber workforce has continued to grow. As GAO Director of Information Security Issues, Gregory C. Wilshusen, stated in a March 2018 testimony report:

> The Office of Management and Budget has noted that the federal government and private industry face a persistent 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.[5]

In an April 2023 High-Risk Series report, GAO stated that "federal agencies need to take additional actions to address the federal

---

[1] On July 14, 2021, the Committee approved S. 1324, the *Civilian Cybersecurity Reserve Act*, with an amendment in the nature of a substitute. That bill, as reported, is substantially similar to S. 885. Accordingly, this committee report is, in many respects, similar to the committee report for S. 1324. *See* S. Rept. 117–97.

[2] Cybersecurity and Infrastructure Security Agency, Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action* (Sept. 2022) (www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf).

[3] 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).

[4] *Id*.

[5] 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).

cybersecurity workforce shortage" and that the Office of Management and Budget needs to develop a governmentwide workforce plan to address the issues facing the cyber workforce.[6]

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.[7] In March of 2023, the Biden Administration continued its efforts to expand the cyber workforce through release of a *National Cybersecurity Strategy*. The National Cyber Workforce and Education Strategy recognizes "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."[8]

Furthermore, critical infrastructure, like 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] This Committee held multiple hearings in the wake of cybersecurity attacks to address the government's preparedness, response, and recovery efforts.[10] These cyber attacks further underscore the urgent need to advance skills of the nation's cybersecurity workforce.

The *DHS Civilian Cybersecurity Reserve Act* attempts to address the continued federal cyber personnel shortages by establishing a surge capacity to better ensure the U.S. is well-positioned to respond to significant cyber attacks. 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 DHS Civilian Cybersecurity Reserve would be voluntary and by invitation. CISA is authorized to activate up to 30 reserve personnel at a time.

The *DHS 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

---

[6] 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).

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

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

[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).

[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–XX); 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).

that Congress authorize a pilot program to create a "Federal Civilian Cybersecurity Reserve." [11] 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.[12]

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.[13] The Cyberspace Solarium Commission released an updated report in August 2021 about the initiatives laid out in its previous report, and recognized "a great deal of progress in implementing the original 82 recommendations" but noted there is "monumental work still ahead." [14] The *DHS 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. 885, the *DHS Civilian Cybersecurity Reserve Act*, on March 21, 2023, with Senator Marsha Blackburn (R–TN). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 885 at a business meeting on May 17, 2023. At the business meeting, Senator Rosen offered a substitute amendment that made technical edits regarding appointment terminology and added language to specify that when the pilot project sunsets, activated reserve members can serve to the end of their temporary appointment. In addition, the amendment struck language referencing existing appropriations. The substitute amendment was adopted by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, and Scott present. The bill, as amended, was ordered reported favorably by roll call vote of 10 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, Scott voting in the affirmative and Senator Paul voting in the negative. Senators Carper, Johnson, Hawley, and Marshall voted yea by proxy, for the record only.

Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

---

[11] 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).

[12] *Id.*

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

[14] Cyberspace Solarium Commission (Aug. 2021) (drive.google.com/file/d/19V7Yfc5fvEE6dGIoU_7bidLRf5OvV2__/view).

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 "Department of Homeland Security Civilian Cybersecurity Reserve Act."

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 in the competitive service or excepted service for up to six months, notifying Congress whenever a reservist is activated. The reservists are considered federal civil service employees when deployed. This subsection directs the Department of Labor (DOL) to 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 processes for the Civilian Cybersecurity Reserve. The eligibility requirements must include an individual's previous employment and cybersecurity expertise. This subsection also directs CISA 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 any topic or product that might create a conflict of interest. Appointed individuals must notify CISA if a potential conflict of interest arises during the appointment. An individual must enter into an agreement with CISA that sets forth the rights and obligations of the individual and agency in order to become a member of the Civilian Cybersecurity Reserve. 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 a determination of eligibility for 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 this bill's enactment on the design and implementation of the pilot project, including on the following: (1) compensation and benefits for members of the Civilian Cybersecurity Reserve; (2) activities that members may undertake as part of their duties; (3) methods

for identifying and recruiting members; (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 members. 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 Government Ethics and issue guidance on implementing the pilot project within two years after this bill's 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 the bill's 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 the 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 provide a briefing to Congress on recommendations relating to the pilot project.

Subsection (h) directs GAO to evaluate the pilot project within three years after the pilot project is established and submit a report to Congress.

Subsection (i) states that the pilot project shall terminate four years after the date on which it is established. Upon the pilot project's termination, an activated member of the Civilian Cybersecurity Reserve may continue to serve until the end of that individual's temporary appointment.

Subsection (j) states that no additional funds are authorized to be appropriated for the purpose of carrying out 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 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.[15]

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

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.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

S. 885, Department of Homeland Security Civilian Cybersecurity Reserve Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on May 17, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
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	65	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?	No
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	Yes, Under Threshold
		Contains private-sector mandate?	Yes, Under Threshold

Bill summary: S. 885 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. CISAwould be required to report regularly to the Congress on the program's effectiveness.

Estimated Federal cost: For this estimate, CBO assumes that S. 885 will be enacted near the end of fiscal year 2023. The costs of the legislation, detailed in Table 1, fall within budget function 050 (national defense). Implementing the bill would cost $65 million over the 2023–2028 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. 885

	By fiscal year, millions of dollars—						
	2023	2024	2025	2026	2027	2028	2023–2028
Civilian Cybersecurity Reserve:							
Estimated Authorization	0	0	8	15	16	16	55
Estimated Outlays	0	0	8	15	16	16	55
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	10	17	18	19	65
Estimated Outlays	0	1	10	17	18	19	65

Under S. 885, 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 2025.

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 $55 million over the 2023–2028 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 2023–2028 period.

Uncertainty: Areas of uncertainty in this estimate include identifying the conditions under which CISA would activate the reserve. S. 885 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. 885 would impose intergovernmental and private-sector mandates 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 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 ($99 million and $198 million in 2023, 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; Chad Chirico, 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

Because S. 885 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.

○