

INDEPENDENT ASSESSMENT OF CIVILIAN CYBERSECURITY RESERVE FOR DEPARTMENT OF DEFENSE

Cyber Mission Readiness Directorate, CERT Division

October 2025

Submitted in compliance with the reporting requirement contained in Section 1540 of the James M. Inhofe National Defense Authorization Act (NDAA) for Fiscal Year 2023 (Public Law 117-263)

[Distribution Statement A. Approved for public release; distribution is unlimited.]

Copyright 2025 Carnegie Mellon University.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

DM25-0762

Table of Contents

EXECUTIVE SUMMARY	1
BACKGROUND AND METHODOLOGY.....	3
LITERATURE REVIEW	5
CYBERSPACE WORKFORCE OVERVIEW	8
1 FEASIBILITY OF CCR CONCEPT	11
2 LIKELIHOOD OF UTILIZING A CCR TO AUGMENT THE DOD WORKFORCE.....	16
3 OUTREACH TO INDUSTRY AND GOVERNMENT AGENCIES	21
4 NECESSITY AND COST FOR SECURITY CLEARANCES	26
5 APPROPRIATE MEMBER COMPENSATION AND BENEFITS	30
6 ACTIVITIES CCR MEMBERS MAY UNDERTAKE	35
7 METHODS FOR IDENTIFYING AND RECRUITING	40
8 PREVENTING CONFLICTS OF INTEREST OR ETHICAL CONCERNS.....	44
9 RESOURCES NECESSARY FOR A CCR.....	46
10 PENALTIES FOR NON-ACTIVATION RESPONSE	54
SUMMARY OF FINDINGS	56
LIST OF ACRONYMS	60
APPENDIX A: COMPILED SURVEY RESULTS.....	63

List of Figures

FIGURE 1: DOD CMF RELATIONSHIPS	9
FIGURE 2: DOD SURVEY RESULTS REGARDING PLACEMENT OF A CCR	12
FIGURE 3: USBLS 10-YEAR OUTLOOK FOR INFORMATION SECURITY ANALYSTS.....	13
FIGURE 4: DOD SURVEY RESULTS REGARDING VALUE OF A CCR	15
FIGURE 5: DOD SURVEY RESULTS REGARDING SKILLS AND CAPABILITIES IN HIGH DEMAND	22
FIGURE 6: DOD SURVEY RESULTS REGARDING THE NEED FOR SECURITY CLEARANCES	26
FIGURE 7: DOD SURVEY RESULTS REGARDING MONTHLY VIRTUAL ASSEMBLIES	32

List of Tables

TABLE 1: ACTIVATION CONDITIONS AND AUTHORITIES.....	19
TABLE 2: COST ESTIMATION	34
TABLE 3: COMPARISON OF SUPPORT	48
TABLE 4: ESTIMATED PERSONNEL SUPPORT COST	51
TABLE 5: ESTIMATED ANNUAL COST FOR 200 MEMBERS	52

Congressional Reporting Requirement

This report was prepared by the Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC), at the direction of the Office of the Under Secretary of Defense for Policy (OUSD(P)) and in response to Section 1540 of the James M. Inhofe National Defense Authorization Act (NDAA) for Fiscal Year 2023 (Public Law 117-263) requiring an independent assessment of Civilian Cybersecurity Reserve for Department of Defense.

Executive Summary

This report is in response to Section 1540 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263) (hereinafter Section 1540). The structure of this report aligns with the itemized elements required for analysis per Section 1540.

The United States faces increasingly sophisticated and complex cyberattacks targeting critical infrastructure as well as federal and Department of Defense (DOD) networks. The government requires the ability to quickly mobilize a highly qualified, mission-ready cyber workforce capable of operating in contested environments. While progress has been made in developing this workforce, gaps remain in effectively leveraging and deploying this talent during major cyber incidents or assisting in exceptionally difficult cyber workforce-related challenges.

In response to this challenge, Congress tasked the DOD with assessing flexible options to address these staffing needs. This report details the findings of the feasibility and advisability study of creating a civilian cybersecurity reserve (CCR) as a potential solution. For the scope of this paper, "qualified civilian staffing" refers to non-government employees or uniformed personnel possessing the skills and experience to effectively respond to significant cyber incidents.

Criteria to assess the feasibility and advisability of creating a DOD CCR to address this challenge was informed through in-depth review of existing literature related to CCRs, interviews with over 50 cyber professionals who have broad and extensive experience in both public and private sectors, as well as responses from almost 1600 survey participants in DOD civilian and military roles. The information gathered from these sources was collated and analyzed to compile relevant insights for each Section 1540 element, as well as deliberated to form conclusions on advisability.

Information assembled soundly demonstrated a need for, and strong interest in, a mechanism to harness cyber expertise from the private sector. However, there are complexities with DOD calling upon civilian talent on a limited or as-needed basis. These potential impediments, such as logistical issues, conflicts of interest, and legal authorities were common concerns raised in previous reports, interviews, and the Section 1540 assessment criteria elements.

A key finding from this study is that creating a CCR as a potential solution to address DOD staffing needs is feasible and also advisable under certain conditions. The assessment shows a CCR is feasible to address the need for talent and there is ample interest from civilian experts in contributing to national cybersecurity interests.

Furthermore, creating a CCR is advisable if it is carefully constructed around several decisive factors with distinction being the primary driving force. Distinction of mission is important to avoid duplicating or interfering with DOD active and reserve component responsibilities, and distinction of member criteria will ensure the highest qualifications and avoid conflicting with other recruitment efforts. Further, the member service requirements and compensation for joining a CCR requires differentiation from the reserve components so that it appeals to civilians without impeding reserve recruitment and retention goals.

Additional recommendations born of the study suggest the need for a talent identification and management system to expedite coordination of mission or incident skill needs with individuals who match the criteria.

Also, conducting a CCR pilot is recommended to validate the effectiveness and necessity of the program. Feedback from the pilot would provide empirical information on program governance, activation success, and impact on employers. The lessons learned would also help refine models that optimize the use of civilian cybersecurity expertise across mission profiles, including surge response, training, and public education initiatives.

Background and Methodology

The United States remains vulnerable to disruptive cyberattacks from well-resourced and highly capable nation-state adversaries. While the DOD contains the nation's largest and most capable cyberspace workforce, it is challenged to compete with China's Peoples Liberation Army (PLA), which reportedly outnumbers the DOD's Cyber Mission Force (CMF) by a factor of 10.¹ Moreover, China effectively supplements its newly reorganized PLA Cyberspace Force² with numerous state-sponsored hacking groups (e.g., Volt Typhoon). Other near-peer cyber adversaries such as Russia, Iran, and North Korea threaten U.S. interests at home and abroad, and the DOD must counter these actors as well. As such, the U.S. Congress tasked the DOD with investigating alternative cyberspace workforce management strategies.

In 2020, the Cyberspace Solarium Commission released its report that proposed numerous legislative actions. This report was organized around six pillars. One of these, called *Preserve and Employ the Military Instrument of Power*, recommended that Congress require the DOD to assess the establishment of a military cyber reserve.³ This recommendation resulted in the enactment of Section 1730 of the FY21 NDAA.

In response, the DOD produced a report entitled *Evaluation of Reserve Models Tailored to the Support of Cyberspace Operations*. This report (herein referred to as the 1730 Report) includes an analysis of alternative cyber reserve force models but concludes that the existing CMF structure (to include uniformed military reserves and national guard) provides sufficient cyberspace workforce capacity and capabilities to accomplish its mission.

Congress returned to the question of alternative cyber reserve forces with Section 1540 of the FY23 NDAA, which requires an independent assessment of civilian cybersecurity reserve for DOD. This report fulfills the requirements of Section 1540.

The methodology for this study to inform the feasibility and advisability of establishing a CCR included surveying related materials and gathering insights from industry members and stakeholders. For the literature review, analysts read and summarized dozens of journal articles, congressional hearings and committee reports, media recordings, and other CCR-related publications. Emphasis was placed on enacted or introduced legislation, United States government (USG) reports in response to legislation, DOD cyber workforce directives and instructions, and testimony of senior USG and DOD leaders. Additionally, over 50 interviews were conducted with a wide swath of USG and private-sector cyber-thought leaders, congressional staff members, DOD commanders at various levels, technical directors, military lawyers, as well as active duty, reserve component, and former DOD cyber operators and defenders. Transcripts of these interviews were

¹ SECTION 2: CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES, 2022, Page 438. https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf

² REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 118 Congress Second Session, 2024, Page 100. https://www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf

³ King, Angus (Senator), Gallagher, Mike (Representative), United States of America Cyberspace Solarium Commission, March 2020, Page 117. <https://www.solarium.gov/report>

summarized, and congruent points were identified and collated. These common themes are referenced, and specific interview quotes are incorporated into this report.

Furthermore, an online survey of DOD civilian and military service members was employed. The survey was made available for 30 days and resulted in 1591 total submissions. Qualitative analysis was performed on responses to the 15 Likert-style questions. Of the 1591 surveys completed, 852 respondents left textual comments as offered by the last open-ended question. Analysis of these comments was conducted with the help of keyword and sentiment-matching techniques.

Literature Review

Section 1540(1) directs consideration of the results of the evaluation of nontraditional cyber support to the Department of Defense required by Section 1730 of the National Defense Authorization Act (NDAA) for fiscal year 2021, Public (Law 116-283).

The concept of a CCR to summon support during an incident or significant event has been previously explored and documented from a variety of perspectives. A major source informing feasibility analysis for this study was the plethora of reports, briefings, and articles related to proposals and solutions aligning with a CCR. This section provides a summary of findings from selections of published literature related to civilian auxiliary force support and reveals their common themes.

Findings from previous reporting were consulted to synthesize and aid in informing feasibility and advisability criteria for this paper as directed per FY23 NDAA Section 1540, (Public Law 117-263). It specifically calls out the need to consider the results of the evaluation of nontraditional cyber support to the DOD required by Section 1730 of the NDAA for fiscal year 2021, Public (Law 116-283). The report, again herein referred to as the 1730 Report, was completed in 2023, and it used published sources in the public domain to provide responses to the evaluation requirements as stated in its subsections (b)1-(9).

In addition, the Army Cyber Institute (ACI) was tasked with providing a framework for analysis of the creation of a CCR. ACI's internal report, *Practical Challenges in Implementing a Civilian Cyber Reserve*, hereafter referred to as the ACI Report, was provided for this study, but is not publicly available as of this writing. The ACI Report was carefully analyzed and is referenced throughout this report.

Common Themes Observed in Literature

Scarcity of Cyber Talent

Literature related to a CCR is predicated on the belief that the U.S. armed forces lack the cyber troops needed to adequately handle difficult or urgent cyber missions. The shortage is more finely described as involving specific talent rather than the need for quantity broadly. In fact, the inability to retain highly trained operators is a common observation of the literature. The 1730 Report cites several RAND studies to highlight this concern over the shortage of best quality personnel. The authors pull from a 2019 RAND study in which U.S. Air Force cyber officers were interviewed about the cyber workforce, and they noted that the problem is not so much of retention, but of retention of the right people. Specifically, they call out officers with offensive and defensive cyber designations as harder to retain, proclaiming, “some of the most talented and technically competent members of the community are being lost at high rates.”⁴

General Nakasone, speaking before the House of Representatives in 2021, is cited widely for asserting that the CMF needs to grow, but that he worried most about retaining the very top operators. “I think the most about is how do I retain this superior force, particularly those individuals that are so much more capable than their

⁴ RAND Corporation, *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings*, 2019, <https://www.dmi-ida.org/knowledge-base-detail/attracting-recruiting-and-retaining-successful-cyberspace-operations-officers>

peers.”⁵ The authors provide recommendations that advocate for improving utilization of reserve component (RC) talent and identify those with 99th percentile skills, placing them where they’re best utilized, and better compensating them to help slow the attrition.

This scarcity of top cyber talent is the primary justification for new workforce initiatives and recommendations. For instance, the USCYBERCOM Tailored Strategic Retention program’s initial targets were high-end cyber talent in the CMF. A DAF working group exploring possibilities for an AF cyber civilian auxiliary force identified four COAs as viable options. Each COA described the civilian capabilities criteria as highly trained, skilled roles.

Benefits of a Public-Private Partnership

The shortage of talented cyber professionals is reported to plague both the private sector as well as the government. There are opinions that CCR recruitment activities would compete for the same small talent pool, but the DOD would have less compensation to offer than companies do. The 1730 Report references data from the cybersecurity workforce labor resource, CyberSeek, to correlate the high number of unfilled cybersecurity jobs to a highly competitive recruiting environment for an alternate cyber reserve. However, “cooperation, not competition, offers the greatest potential for maintaining the health of the Nation’s cyber-related career fields and strengthening national security,” as summarized in an Air War College cyber workforce research paper.⁶ Both parties stand to gain from the expertise and information exchange (as permissible) from such a relationship. The reciprocal risks are recognized as well—that is, proprietary technology leak while serving, and using insider intel to shape business offerings to better target government contracts. Those risks were especially concerning to the American Federation of Government Employees union regarding a CCR. As explained in the 1730 Report, the union feared a for-profit company could be motivated to allow an employee to participate in a CCR in an effort to obtain insider information and increase competitive advantage.

Questions of Mission and Authority

While much of the literature touts the potential benefits of a CCR addressing workforce gaps, either capacity or capability, there are few details about what members of a CCR would actually do. The ACI Report phrased it as, “a solution in search of a problem.” Without clear indication of what the mission gaps are, all that is available to hypothesize CCR mission scenarios is the language in NDAA proposals as well as what actions a civilian is authorized to perform while operating under DOD authorities. The 1730 Report proclaims that traditional Reserve Component (RC) already successfully integrate into cyberspace operations and have models where defensive and offensive cyber units departing active duty can transfer into part time. This allows top talent to be retained in an RC while they work in the civilian sector. As previously mentioned, the authors recommend strategies to improve utilization of the RC talent, specifically retention of the top percentile talent. The ACI Report calls out in the recommendations the need for gap analysis to identify where a CCR would be used.

⁵ Nakasone, Paul, Retired General, 117th Congress/House event LC67392, May 2021, p.13, <https://www.congress.gov/event/117th-congress/house-event/LC67392/text>

⁶ Kaloostian, Michael R., author.; Air University (U.S.). Air War College. (2020), *DOD’s cyber workforce : strength through retention and volunteerism*. Air War College, https://aul.primo.exlibrisgroup.com/discovery/fulldisplay/alma995965484406836/01AUL_INST:AUL

Complexities to Manage

A CCR as proposed within NDAs seems like an intuitive concept—identifying where resources are located to fill gap areas. However, implementing the concept is more complex. The reports recognize the practical challenges, several of which are itemized elements for feasibility assessment in Section 1540. A few examples include a means to identify and certify individuals for qualifications and clearance, managing and maintaining a talent data store, employer-related issues with activation, geographic and compensation questions, and inactive duty training.

Abridged Conclusions from Literary Review

The studies assessing concepts related to establishing a CCR were largely in consensus on areas that needed more information to conclusively offer feedback, as well as on recommendations to fortify known deficiencies.

The studies justly call out the uncertainty of the central problem that a CCR is meant to help solve. As such, calls for mission gap analysis and more specifics about the specialties outside the CMF construct, is needed. This includes itemizing potential missions and the authorities required to support it.

A byproduct of gap analysis is the need for human capital management, which includes the identification of critical skillsets needed in the CMF, training and certification qualifiers, and an inventory of personnel and reserve candidate credentials. The 1730 Report highlighted the DOD Cyber Workforce Framework (DCWF) as a tool for talent identification and management. The DCWF was adapted from the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework), a lexicon to describe cybersecurity work roles and related attributes. While there is some overlap between the two frameworks, the civilian NICE Framework does not include DOD-specific categories like Cyberspace Effects and Cyberspace Intelligence. Should skillsets related to those roles be identified as a gap area within the DOD, filling that gap with civilian expertise would require translation of what those skillsets are called within private-sector cyber operations, or their closest commonality to upskill.

The theme of doing better with what already exists is prevalent among studies. There are existing RC models that provide capability and capacity in support of CMF requirements per the 1730 Report. There will be additional growth required in the RC for CMFs as the number of CMF teams increase, but that is yet to be an issue. Prioritizing, incentivizing, and recognizing highly-skilled cyber talent to increase retention are highlighted in recommendations.

Finally, similar existing auxiliary models are presented to consider. The Coast Guard Auxiliary, Civil Air Patrol, and the Marine Corps Cyber Auxiliary are initiatives for augmenting force needs. As described in the 1730 Report, Estonia has a national-level CCR model that is being adopted as an example for several other nations.

The reports considering a CCR solution to support the DOD in an urgent situation arrived at similar conclusions given the information provided. The existing literature informed this report and can serve to aid future work regarding inquiries about how civilians can be used to supplement the USG.

Cyberspace Workforce Overview

When considering the establishment of a CCR, it is essential to first understand the organization and staffing of the existing DOD cyberspace workforce. This subject was covered in the 1730 report; however, some updates to the workforce have occurred since its publication in 2023. Additionally, the DCWF has also been updated in that time. Therefore, the following section provides an overview of the changes.

The U.S. military's Cyberspace Operations Forces⁷ (COF) contains about 225,000⁸ personnel. The vast majority of these forces perform cyberspace information technology (IT) and IT security tasks and are assigned to and retained within the separate military services. A more recent U.S. Government Accountability Office (GAO) report states that “according to data provided by DOD components, DOD has established 434 organizations (consisting of 60,763 personnel and 9,501 contractors) that conduct cyberspace operations.”⁹ Narrowing the scope even more, the CMF plans, directs, coordinates, and executes cyber operations. The CMF falls under U.S. Cyber Command (USCC) and contains roughly 3 percent of the COF, with an authorized strength of approximately 6,200 DOD civilians and uniformed service members. As of this writing, the CMF is organized into 147 mission-specific teams.¹⁰ Note that in 2021, the DOD proposed and was authorized to create 14 new teams beyond the original 133 established in 2012. Currently, the Army, Navy, Air Force, and Marines separately man, train, and equip these teams and provide them to USCC for the conduct of cyber operations.

About half of the CMF is made up of Cyber Protection Teams (CPT). CPTs hunt for adversaries on DOD information networks and also support USCC's Defend Forward strategy outside of the United States. The remainder of the CMF are made up of National Mission Teams (NMT), Combat Mission Teams (CMT), and Combat Support Teams (CST).¹¹ NMTs “defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.” CMTs “conduct [offensive] military cyber operations in support of combatant commands,”¹² and CSTs provide analytic, intelligence, and planning support” to NMTs and CMTs. Figure 1 offers more information about these relationships.

⁷ Joint Publication 3-12 Cyberspace Operations, 2012, https://irp.fas.org/doddir/dod/jp3_12.pdf

⁸ Doubleday, Justin, After years of growth, DoD cyber workforce braces for reductions, 2025, <https://federalnewsnetwork.com/cybersecurity/2025/05/after-years-of-growth-dod-cyber-workforce-braces-for-reductions/>

⁹ GOA Report to Congressional Committees DOD CYBERSPACE OPERATIONS, September 2025, <https://www.gao.gov/assets/gao-25-107121.pdf>

¹⁰ DEFENSESCOOP Pomerleau, Mark, 12 of 14 new cyber mission force teams now established, 2025, <https://defensescoop.com/2025/05/12/new-cyber-mission-force-teams-12-of-14-now-established/>

¹¹ U.S. Cyber Command Public Affairs, Cyber 101 – Cyber Mission Force, Nov. 2022, <https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/>

¹² Murphy, Patrick (Honorable), Borghard, Erica, To Defend Forward, US Cyber Strategy Demands a Cohesive Vision, Fall 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2002_Murphy_Borghard.pdf

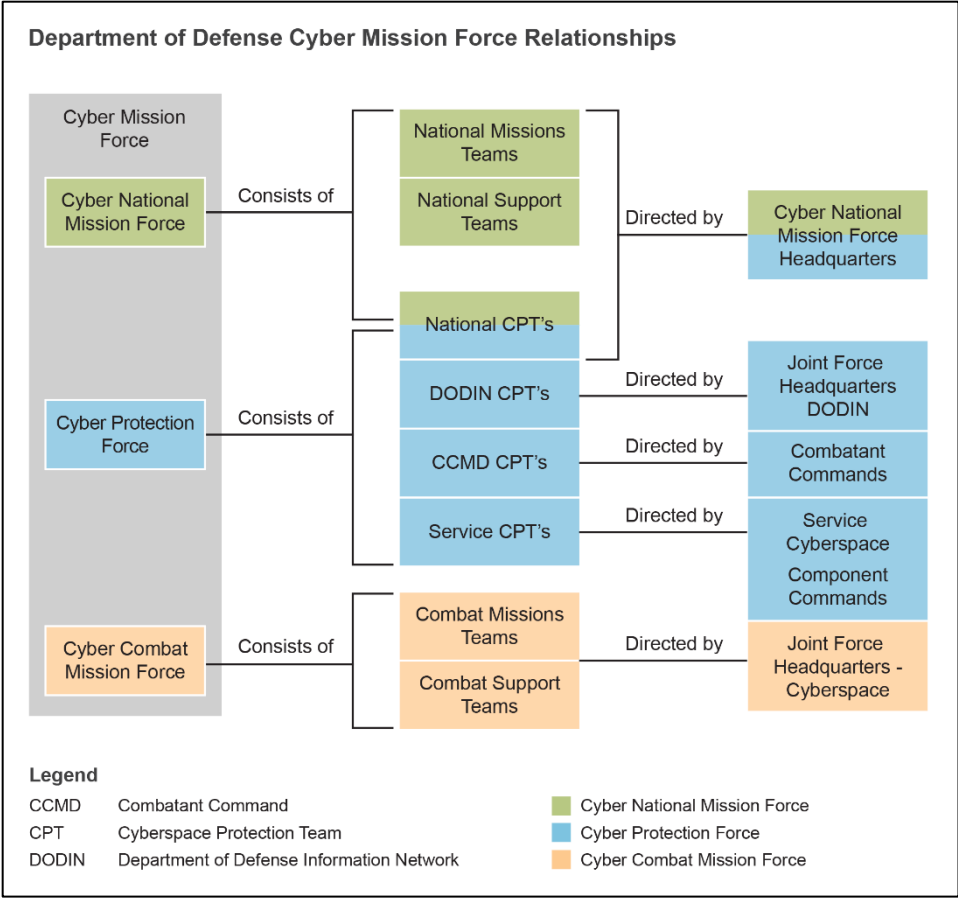


Figure 1: DOD CMF Relationships¹³

As stipulated in the 1730 Report, these active component (AC) CMF teams are complemented by reserve and national guard forces that are occasionally activated to serve alongside or within USCC’s active-duty teams and watch floors. For example, the Air National Guard stood up an entire cyberspace wing in 2023¹⁴ and has over two dozen cyber squadrons whose members supplement CMF teams when activated. Furthermore, the U.S. Army Reserves (USAR) Cyber Protection Brigade (CPB) and the Army National Guard’s 91st Cyber Brigade maintain 10 and 11 CPTs respectively. Moreover, in a recent interview with the commander of the USAR CPB, the authors of this report learned that the command’s authorized staffing is being expanded significantly. Other RC units from the Air Force, Navy, and Marine Corps add further capacity to USCC’s total force construct.

Beyond covering COF strength and structure, it is valuable to describe how the DOD manages training and readiness standards for individual cyber service members. The DCWF is “the authoritative lexicon for the uniform identification, tracking, data collection, and reporting of DOD cyber staffing positions.” The DCWF also serves as “the foundation for standardized enterprise DOD cyber workforce qualification criteria to

¹³ Department of Defense CMF Relationships, https://irp.fas.org/doddir/dod/jp3_12.pdf

¹⁴ Wade, Alexis, 179th Airlift Wing becomes first cyberspace wing in the Air National Guard, Sept. 2023, <https://www.179cw.ang.af.mil/News/Features/Display/Article/3522947/179th-airlift-wing-becomes-first-cyberspace-wing-in-the-air-national-guard/>

improve interoperability and unity of action...”¹⁵ The DCWF’s qualification criteria includes knowledge, skills, abilities, and tasks (KSAT) statements for all established cyberspace work roles and each billet or position can contain up to three work roles. DCWF implementation is following a phased approach, with compliance requirements fully in place by February 2027.¹⁶ The DCWF is mandatory for the DOD’s active and reserve component units and service-run training programs and schoolhouses. The DOD used two primary source documents for initially constructing the DCWF: the National Institute of Science and Technology’s (NIST) NICE Workforce Framework for Cybersecurity and the DOD’s Joint Cyber Training and Certification Standards (JCT&CS). The Defense Cyber Workforce Management Board (CWMB) reviews and approves DCWF updates regularly to ensure the currency and inclusion of emerging technologies and work roles. For example, the Red Team Specialist work role was added to the DCWF on April 29, 2025. While the DCWF informs qualification criteria and standardization of the workforce, each service must interpret and apply its guidance to service-specific military occupational specialties, civilian position codes, and service command structures. These vary widely across the COF. Therefore, forces generated by the individual services and provided to USCC are not fully interchangeable despite DOD efforts at workforce standardization.

In a hearing before the House Armed Services Committee on May 16, 2025, the acting commander of USCC (Lt General Hartman) stated that talent management is the command’s top priority.¹⁷ To that end, significant efforts are in progress to refactor and modernize the force to include a rework of the Cybercom 2.0 initiative.¹⁸ As such, potential changes to USCC’s current models of force generation and possibly force structure are under consideration. Finally, some members of Congress and other organizations are calling for the creation of a new military service, United States Cyber Force.¹⁹ While the topic of a distinct military cyber service came up in interviews with study participants, this subject is beyond the scope of reporting requirements outlined in Section 1540 of the FY23 NDAA.

All this legislative and policy activity demonstrates the increasing focus on the DOD’s role in defending the country against powerful nation-state adversaries in cyberspace. This report considers the potential for leveraging civilians to bolster DOD forces during “significant cyber incidents or to assist in solving other exceptionally difficult cyber workforce-related challenges.”²⁰

¹⁵ Office of the DoD Deputy Chief Information Officer, DoD Cyber Workforce Framework (DCWF) Military & Civilian Workforce Identification & Coding Guide Version 1.4, Sept. 2024, https://www.cool.osd.mil/usn/ia_documents/DCWF_Workforce_Identification_and_Coding_Guide.pdf

¹⁶ DoD 8140 Implementation Timelines (2025-2027), CLEARED for Open Publication 2023, <https://dodcio.defense.gov/Portals/0/Images/Cyber/DoD8140-ImplementationTimeline.pdf>

¹⁷ House Committee Hearing, House Armed Services Subcommittee on Cyber, Information Technologies, and Innovation, May 2025, <https://www.congress.gov/event/119th-congress/house-event/118262>

¹⁸ DEFENSESCOOP, Pomerleau, Mark, DOD leadership asks for Cybercom 2.0 relook, May 2025, <https://defensescoop.com/2025/05/20/cybercom-2-0-relook-dod-leadership/>

¹⁹ Foundations for Defense of Democracies, Lonergan, Erica, Montgomery, Mark, United States Cyber Force, *A Defense Imperative, March 2024*, <https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force/>

²⁰ FY23 NDAA SEC. 1540. INDEPENDENT ASSESSMENT OF CIVILIAN CYBERSECURITY RESERVE FOR DEPARTMENT OF DEFENSE, excerpt from subsection (a) IN GENERAL, <https://www.govinfo.gov/content/pkg/PLAW-117publ263/pdf/PLAW-117publ263.pdf>

1 Feasibility of CCR Concept

Section 1540(c)(1) asks for an analysis of the feasibility of the concept of a CCR program, including an analysis of the available talent pool, potential impact on employers, and propensity to serve.

If a CCR were created, is the DOD the right place in USG?

Most proposals and legislative acts suggest a CCR could successfully augment the DOD and the Department of Homeland Security (DHS). Arguments for both are viable and are separated primarily by perceived threat priorities, legislative authorities, and the realities of politics and budgets.

Feedback from our interviews for this report was mixed on this question. One senior official suggested that CISA was the right place to house a CCR based on the gravity of the threat to the U.S. homeland and its supporting critical infrastructure. Another agreed and said that a significant cyber attack on the U.S. homeland would “almost certainly” precede a military strike on U.S. national interests abroad. As such, administering a CCR under CISA would bifurcate the response along the proper authorities, allowing DHS to assign CCR resources internally while the DOD prepares for or engages in both a cyber and kinetic war overseas.

A different interview respondent described the DOD as the “backstop of the nation” and said the DOD controls over half of the federal budget and the vast majority of the best-qualified cyber operators and defenders. Consequently, placing a CCR within the DOD would assure appropriate resources, doctrine, command and control, and operational experience in the cyberspace domain. This individual also stipulated that the DOD would likely be given the defend the nation mission in the event of a major cyber attack on the United States.

Congress first proposed a CCR in 2021 with the introduction of S. 1324 (117th): the *Civilian Cybersecurity Reserve Act*.²¹ In April of 2022, the report to accompany this bill was released.²² It describes how a CCR would be established under DHS/CISA. The report references the Solarium Commission Report, and other previous congressional testimonies, to address the shortage of cybersecurity professionals within the USG.

The Bill S. 1324 authorizes “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.” The implementation of the bill was estimated to cost \$63M over the 2021-2026 period.

While S. 1324 passed the Senate by unanimous consent, it was not voted on in the House and therefore did not become law. As such, CISA does not have authority or appropriations to conduct the pilot program.

The next two pieces of legislation (S.1540 and S.1730) imply that the DOD may be the preferred home of a CCR. This question, as well as where a CCR should be placed within the department, are subject to further

²¹ “S. 1324 — 117th Congress: Civilian Cybersecurity Reserve Act.” [www.GovTrack.us](https://www.govtrack.us/congress/bills/117/s1324). 2021. August 1, 2025, <https://www.govtrack.us/congress/bills/117/s1324>

²² CIVILIAN CYBERSECURITY RESERVE ACT, Report of the Committee on Homeland Security and Governmental Affairs United States Senate to accompany S. 1324, April 27, 2022, <https://www.govinfo.gov/content/pkg/CRPT-117srpt97/html/CRPT-117srpt97.htm>

consideration with ongoing department restructuring. However, the strategic risk to national security of adversarial cyber attacks lends weight to the argument of choosing the DOD. Figure 2 provides the results of this study’s survey on this question.

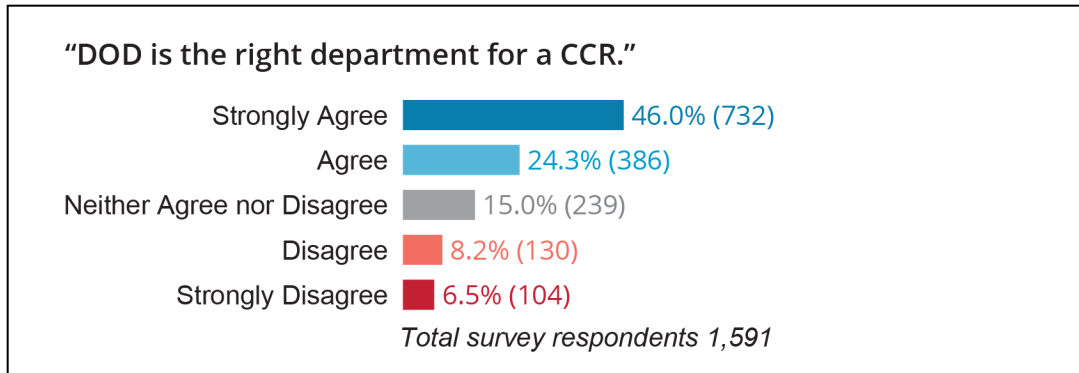


Figure 2: DOD survey results regarding placement of a CCR

Civilian Talent Pool and Job Market Analysis

The current data show that the U.S. cybersecurity job market is still competitive where demand for talent outstrips supply. Estimates place the U.S. cybersecurity workforce at roughly 1.3 million professionals.²³ Concurrently, U.S. employer demand for cybersecurity professionals is still strong, but the market is shifting in some categories. Specifically, early career information technology and software engineering job candidates are struggling to break into the market, as artificial intelligence (AI) predictions and investments are impacting hiring at major tech companies.²⁴ CyberSeek is a commonly referenced cybersecurity workforce statistics aggregator.²⁵ The site’s job market data suggests that 0.47–0.51 million U.S. cybersecurity jobs were posted each year between 2023-2025. Additionally, this site estimates that only about 75 percent of cybersecurity positions are filled with qualified staff, implying a large shortfall. As of this writing, the CyberSeek dashboard (which contains data from the previous 12 months) shows that there are 1,337,400 employed cybersecurity workers in the U.S. job market and that 514,359 cybersecurity positions are posted but unfilled.

Recent Hiring Trends

Cybersecurity hiring is increasing following a slowdown in 2022-2024. In a September 2024 ISC2 survey, 67 percent of organizations cited cybersecurity staffing shortages as a problem, making “worker shortage” the top challenge.²⁶ Overall, despite some short-term dips, cyber job openings are outpacing the current supply of qualified candidates. Conversely, USG and DOD cybersecurity job postings have dwindled considerably in 2025.

²³ NSF Cybersecurity Workforce Data Initiative, *Cybersecurity Workforce Supply and Demand Report*, May 2024, <https://nces.nsf.gov/760/assets/0/files/nces-cwdi-supply-demand-report.pdf>

²⁴ J.P. Morgan, *Is AI already impacting job growth?* August 15, 2025, <https://www.jpmorgan.com/insights/global-research/artificial-intelligence/ai-impact-job-growth>

²⁵ Cyberseek Heatmap, <https://www.cyberseek.org/heatmap.html>

²⁶ ISC2 Cybersecurity Workforce Study, *Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists*, Sept. 2024, <https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look>

Projections and Market Outlook

The U.S. Bureau of Labor Statistics' (USBLS) information security job outlook is positive but much less glowing than the CyberSeek data. While both indicate a high demand based on unfilled cybersecurity jobs, USBLS demonstrates a demand of roughly 16,000 job openings per year over the next 10 years.

The following excerpt from the USBLS site²⁷ details this trend:

Employment of information security analysts is projected to grow 29 percent from 2024 to 2034, much faster than the average for all occupations. About 16,000 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labor force, such as to retire.

Figure 3 (extracted from the same site) illustrates this observation and compares the cybersecurity 10-year market outlook to other computer occupations and the overall U.S. job market for all occupations.

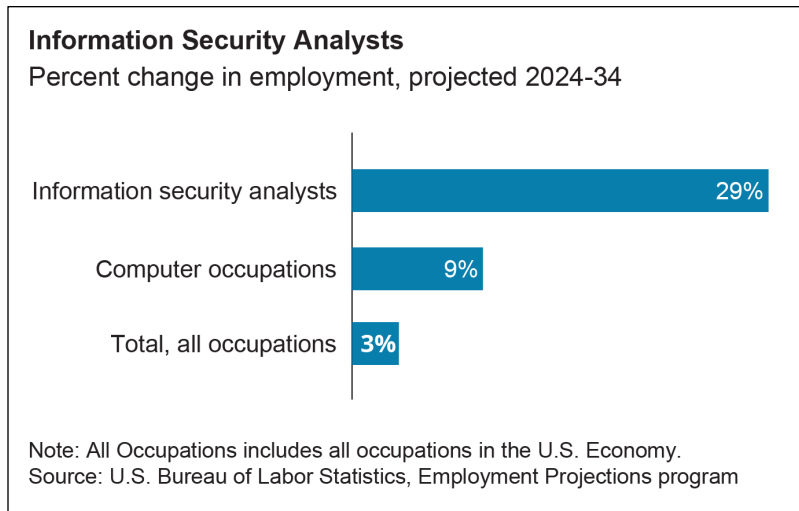


Figure 3: USBLS 10-year Outlook for Information Security Analysts

Virtually all analyses agree the workforce gap will persist. ISC2's latest study found the global cyber workforce gap grew 19 percent in 2024 (to approximately 4.8 million unfilled positions), and while that is a world figure, it underscores the global shortage. In the U.S., CyberSeek data suggests roughly 265,000 additional cybersecurity workers are needed now—a gap that will only widen if education and hiring fail to keep up. Emerging skills (AI, cloud security, zero trust) are increasingly in demand, indicating higher long-term market growth in positions that require these highly technical skillsets. In summary, the cybersecurity job market in 2025 remains active, with steady growth expected and strong, persistent shortfalls of qualified workers projected into the next decade.

²⁷ U.S. Bureau of Labor of Statistics, Occupational Outlook Handbook, Computer and Information Technology Occupations, Information Security Technology, <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6>

Current USG Hiring Freeze and Reductions in Force

While the private-sector cybersecurity job market continues to struggle with an insufficient talent pool and qualified candidate scarcity, the DOD and broader USG federal civilian agencies are currently dealing with a hiring freeze within the government civilian workforce and an expected reduction in authorized cybersecurity and IT positions. The Defense Information Systems Agency “expects to lose nearly 10% of its civilian workforce” and the DOD’s “goal is to reduce the civilian workforce by 5% to 8%, or approximately 50,000 to 60,000 employees.”²⁸ These DOD staffing issues were corroborated in our interviews with USCC component command leaders who expressed frustration with the hiring freeze and said that they prefer to hire permanent government civilians prior to investing in a CCR.

Potential Impact on Employers

The 1730 Report from 2023 briefly addresses this concern in Section 8: Impact of Alternate Cyber Reserve Force Models on Private Sector. The report states that “employers may express concern about activating members during periods of instability or risk when those employees are needed most.” It also cites a New America report from 2018 that proposed a Civilian Cybersecurity Corps akin to the Civil Air Patrol but housed under DHS. That report does not cover impact on private-sector employers but rather says “security is not a zero-sum game and any actions to increase the overall security of the ecosystem serve to benefit public and private sector actors.”²⁹

For this study, interviews were conducted with members of six state-level civilian cyber auxiliary organizations. One of the interview questions addressed private-sector employer support and protections. The responses similarly reported that employers generally supported employee participation given the all-volunteer models and short timeframes of crisis response missions. However, the general feedback on this topic noted that “tensions may arise when skilled personnel are called to serve, potentially leaving critical workforce gaps during cyber incidents.”

Propensity to Serve

Research into voluntary state-level cybersecurity response organizations and teams demonstrates that, under the right conditions, a desire and propensity to serve the country exists. These state-level service initiatives are covered in depth later in this report. At the federal level, a propensity to serve is further illustrated by cyber auxiliary programs sponsored by the U.S. Marine Corps³⁰ and the U.S. Coast Guard.³¹ More broadly, voluntary participation in non-cyber civilian auxiliaries such as the Civil Air Patrol and Coast Guard Auxiliary have been sufficiently staffed with volunteers for decades. A corollary model of voluntary enlistment and part-

²⁸ Doubleday, Justin, After years of growth, DoD cyber workforce braces for reductions, 2025, <https://federalnewsnetwork.com/cybersecurity/2025/05/after-years-of-growth-dod-cyber-workforce-braces-for-reductions/>

²⁹ Cohen, Natasha, Singer Peter, New America The Need for C3 A Proposal for a United States Cybersecurity Civilian Corps, Oct. 2018, <https://www.newamerica.org/cybersecurity-initiative/reports/need-c3/1-summary>

³⁰ Public Web Site for Headquarters Marine Corps, Cyber Auxiliary, Marine Corps Cyber Auxiliary, April 2019, <https://www.hqmc.marines.mil/Agencies/Deputy-Commandant-for-Information/Information-Maneuver-Division/Marine-Corps-Cyber-Auxiliary/>

³¹ U.S. Coast Guard Auxiliary Cybersecurity Web Site, <https://wow.uscgaux.info/content.php?unit=y-dept>

time service of civilians in the DOD’s reserve components also support a reasonable conclusion that patriotism and service to the country is alive and well in the United States.

Additionally, there are existing programs in the USG and the DOD that use educational incentives to attract civilians into extended government service in cybersecurity. The Office of Personnel Management’s CyberCorps® Scholarship for Service³² and the DOD’s Cyber Service Academy³³ programs are successful examples. A different approach for enabling civilians to temporarily support the DOD’s cyber mission is realized through the Cyber Information Technology Exchange Program (CITEP). This initiative is an industry partnership program that enables companies to lend employees to the DOD for periods of three months to one year.³⁴

Furthermore, numerous interviewees for this report, including senior members of the DOD, private-sector executives, and the former director of the Cyber Solarium Commission, cite examples that support the existence of an untapped pool of cybersecurity professionals from industry who are willing to serve as temporary civilian volunteers if certain fitness and other traditional DOD service standards are relaxed.

As of this writing, limited quantitative evidence in the literature supports an affirmation that a propensity to serve in a CCR exists, however survey data collected as part of this study indicates that over 80 percent of the survey audience agrees the CCR concept has value. Figure 4 illustrates that finding.

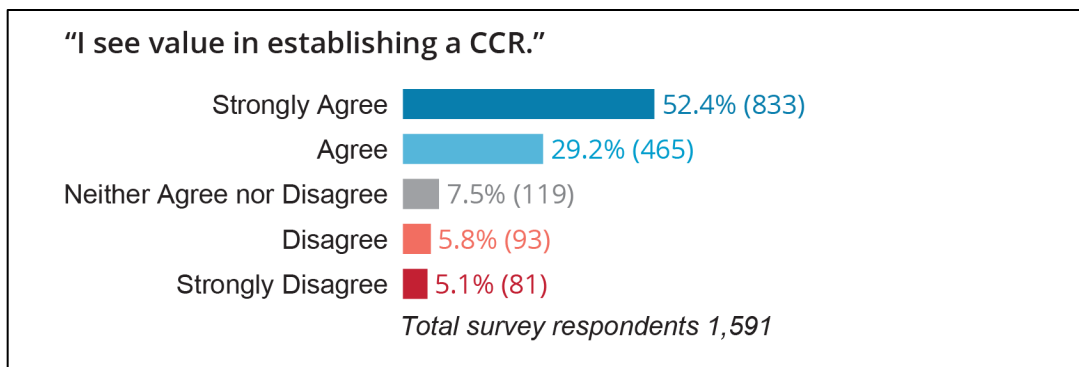


Figure 4: DOD survey results regarding value of a CCR

Lastly, experienced cybersecurity professionals from the USG and the private sector were interviewed and the general feedback suggests a broad interest and willingness to participate in a CCR under certain conditions. These conditions include virtual versus physical assemblies, voluntary and consensual activation periods, and receiving compensation while performing CCR duties.

³² CyberCorps: Scholarship for Service, Designed to INCREASE AND STRENGTHEN the cadre of federal information assurance professionals that protect the government's critical information infrastructure, <https://sfs.opm.gov/>

³³ DoD Cyber Service Academy (DoD CSA), <https://www.cyber.mil/dod-workforce-innovation-directorate/csa/>

³⁴ Chief Information Officer, FOR DOD PARTICIPANTS, <https://dodcio.defense.gov/Cyber-Workforce/CITEP/For-DoW-Participants/>

2 Likelihood of Utilizing a CCR to Augment the DOD Workforce

Section 1540(c)(2) requires an analysis of the likelihood of utilizing civilian cybersecurity reservists to augment the existing DOD workforce, including an assessment of the duration of periods of activation.

According to Section 1540(a) of the 2023 NDAA, civilian cybersecurity reservists would be activated to respond to significant cyber incidents or to assist in solving other exceptionally difficult cyber workforce-related challenges. There are several practical and logistical challenges that make it unlikely that civilian reservists would be able to effectively augment the existing DOD CMF. However, it is feasible for civilians to provide support to the existing DOD cyberspace workforce through alternative means. For the purpose of augmenting (i.e., backfilling) the CMF, the RCs are in a better position to do so. Regarding the duration of periods of activation, the DOD RCs and various state cyber reserve programs provide a frame of reference for how activation periods could be handled for a civilian cybersecurity reserve. Activation periods for the various programs and organizations reviewed for this study ranged from hours to years.

Conditions for Activating Civilian Cybersecurity Reservists

Section 1540(a) states that the purpose of the civilian cybersecurity reserve corps would be to enable the DOD and military services to provide qualified civilian staffing to the DOD to effectively respond to “significant cyber incidents or to assist in solving other exceptionally difficult cyber workforce-related challenges”.³⁵

For this report, a significant cyber incident and an exceptionally difficult cyber workforce-related challenge are defined as follows:

- **Significant cyber incident:** a cyber incident, or a group of related cyber incidents, that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States³⁶
- **Exceptionally difficult cyber workforce-related challenge:** an issue related to identifying, recruiting, developing, and retaining members of the DOD’s CMF that prevents the CMF from successfully performing its mission³⁷

The following attacks are a few examples that meet the criteria for a significant cyber incident:

- **SolarWinds (2019/2020):** A threat actor, later confirmed to be the Russian Foreign Intelligence Service, compromised the software development environment for the SolarWinds company. The threat actor subsequently injected malicious code into SolarWinds’ Orion application suite, which is used for monitoring and managing networks. This malicious code was distributed to SolarWinds

³⁵ Inhofe, James, H.R. 7776 National Defense Authorization Act for FY 2023, 117th Congress 2021-2022 Became Law, <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, Section 1540(a)

³⁶ GOVREGS, 681.Definitions (9) Significant cyber incident, Proactively identify opportunities, 6 U.S.C. § 681(9)

³⁷ 2023-2027 DoD Cyber Workforce Strategy, page 4, This definition is partially based on cyber workforce development functions defined in the, <https://dodcio.defense.gov/Portals/0/Documents/Library/CW-StrategyImplementationPlan.pdf>

customers—including the DOD—via software updates and enabled the threat actors to gain access to federal government networks and systems.³⁸

- **Microsoft Exchange Server Vulnerabilities (2021):** In March 2021, the FBI and CISA released a Joint Cybersecurity Advisory warning that threat actors, to include nation-state actors and cyber criminals, had been exploiting multiple zero-day exploits with Microsoft Exchange to gain unauthorized and persistent access to the on-premise Microsoft Exchange servers of U.S. entities. The White House later confirmed that malicious cyber actors affiliated with the People’s Republic of China’s Ministry of State Security conducted operations utilizing these vulnerabilities. The use of multiple zero-day exploits in this incident is particularly alarming because they can cause significant and widespread damage due to the fact that they take advantage of vulnerabilities that were previously unknown.³⁹
- **Colonial Pipeline Ransomware Attack (2021):** Threat actors carried out a ransomware attack against the Colonial Pipeline Company, which supplies about 45 percent of all fuel consumed on the East Coast. While the attack only affected the company’s IT systems used for business purposes, Colonial Pipeline proactively disconnected operational technology (OT) systems that controlled and operated their oil pipelines out of an abundance of caution. The incident highlights the impact a cyber attack can have on U.S. critical infrastructure.⁴⁰

Practical Challenges for Civilians to Augment the DOD Cyber Mission Force

As outlined earlier in the report, the DOD CMF plans, directs, coordinates and executes cyberspace operations. This report defines *augmenting the DOD workforce* as backfilling or performing the same job duties as those in the CMF. Given this definition, there are several practical and logistical challenges that make it unlikely that civilian reservist would be able to effectively augment the existing DOD CMF.

While it is unlikely for civilian reservists to augment the existing DOD cybersecurity workforce by performing the same job duties and functions as CMF team members, it is feasible for civilians to provide support to the existing workforce through alternative means, which are outlined in Section 6 of this report.

Background Checks and Clearances

In the survey sent to DOD personnel as a part of this study, a majority of survey respondents (63.9 percent) strongly agreed that civilian reservists must hold a security clearance to add value to the DOD’s cyber mission. The following intent statement was provided to survey respondents to set a common understanding of the role of a CCR for the purpose of the survey: “The intent of a CCR is to provide temporary, qualified civilian staffing to effectively respond to significant cyber incidents or exceptionally difficult cyber workforce-related challenges impacting US national security.”

³⁸ Report to Congressional Addressees, CYBERSECURITY *Federal Response to SolarWinds and Microsoft Exchange Incidents*, Page 16, January 2022, <https://www.gao.gov/assets/gao-22-104746.pdf>

³⁹ Report to Congressional Addressees, CYBERSECURITY *Federal Response to SolarWinds and Microsoft Exchange Incidents*, January 2022, <https://www.gao.gov/assets/gao-22-104746.pdf>

⁴⁰ Cybersecurity Advisory, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Last Revised: July 08, 2021, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>

Additionally, during interviews with DOD officials, active-duty service members, and former CMF service members, background checks and clearances came up as potential challenges. Issues that came up included concerns about clearance eligibility and the practicality of maintaining clearances for civilians.

Loss of Pay and Time Commitment

During interviews conducted with former active-duty CMF service members, some interviewees cited potential loss of their private-sector pay during periods of activation as an issue that would discourage them from participating in a CCR. Some interviewees stated that their employers had policies in place to help bridge the gap in pay compensation during periods of activation. However, these policies were company specific and intended for service with the reserve components. Other interviewees mentioned that the prospect of prolonged time away from home during periods of activation would dissuade them from participating in a CCR. One interviewee plainly stated, “I already served my time.”

Authorities and Legal Issues

Many DOD officials who were interviewed cited the lack of or unclear legal authorities for calling up civilians as a potential challenge. Others stated that there are issues around liability that would need to be sorted out such as if a civilian cyber reservist damages a critical system while on duty.

Access to DOD Systems

Another challenge identified by DOD officials in interviews was granting civilians access to DOD systems and maintaining it through periods of inactivity.

Duration of Periods of Activation

The second part of Section 1540(c)(2) requires an assessment of the duration of periods of activation for civilian cybersecurity reserve. The best starting point for this assessment is to look at activation periods for the DOD reserve components and to review how various state cyber reserves handle activation.

DOD Reserve Component Activation

The reserve components of the armed forces are comprised of the Army Reserve, the Navy Reserve, the Marine Corps Reserve, the Air Force Reserve, the Coast Guard Reserve, the Army National Guard, and the Air National Guard.⁴¹ Reservists, including for the National Guard, fall into one of three categories: the Ready Reserve, the Standby Reserve, or the Retired Reserve. Within the Ready Reserve is a subcategory called the Selected Reserve⁴², which includes the individuals that drill one weekend a month and train two weeks a year. When reservists are activated, they usually come from the Selected Reserves. As of June 2025, there are 766,252 individuals in the Selected Reserve across all seven reserve components.⁴³

⁴¹ [10 U.S. Code § 10101](https://www.law.cornell.edu/uscode/text/10/10101), <https://www.law.cornell.edu/uscode/text/10/10101>

⁴² Defense Primer: Reserve Forces, Congressional Research Service, <https://www.congress.gov/crs-product/IF10540>

⁴³ Department of Defense, Defense Manpower Data Center, Selected Reserve Personnel by Reserve Component and Rank/Grade, June 2025, <https://dwp.dmdc.osd.mil/dwp/app/dod-data-reports/workforce-reports>

Members of the Reserve and National Guard can be activated under the conditions and authorities outlined in Table 1.

Table 1: Activation conditions and authorities

Authority	Condition	Duration
10 U.S.C. § 12301(a)	In time of war or of national emergency declared by Congress	For the duration of the war or emergency and for six months thereafter
10 U.S.C. § 12302	In time of national emergency declared by the President (applies to the Ready Reserve only)	No more than 24 consecutive months
10 U.S.C. § 12304	When the president determines that it is necessary to augment the active forces	No more than 365 consecutive days
10 U.S.C. § 12304b	When the secretary of a military department determines that it is necessary to augment the active forces for a preplanned mission in support of a combatant command	No more than 365 consecutive days
10 U.S.C. § 12304a	When a governor requests federal assistance in responding to a major disaster or emergency (Army Reserve, Navy Reserve, Marine Corps Reserve, and Air Force Reserve only)	No more than 120 days

State Cyber Reserves Activation

State cyber reserves reviewed for this study provide insight into how these state programs utilize civilian talent for responding to cyber incidents. Activation periods for these programs are typically short term, directly linked to incident requirements, and come with significant flexibility to accommodate both public service and private-sector obligations.

- Maryland’s Cyber Reserve** integrates personnel from industry and government sectors, with activation providing insurance coverage, stipends, and legal protections during active missions. Activation lengths are determined by incident duration, likely ranging from a few days to several weeks depending on mission complexity.
- Michigan’s MiC3** relies on voluntary participation for incident response. Activation is designed to be incident specific, with deployments lasting from hours to a few days, reflecting the limited scope and targeted nature of most state cyber incidents.
- California State Defense Force** members serve on a volunteer basis during regular training periods; they can be activated for Emergency State Active Duty (ESAD) by the governor during state emergencies. In such cases, they are compensated in accordance with state law and policy and receive pay comparable to their National Guard counterparts. In the last year alone, California has activated its civilian cyber force in response to numerous ransomware attacks on its municipalities.
- Wisconsin’s Cyber Response Team** also functions on an incident-driven model, and activations are generally brief and designed to complement state emergency management structures.

RC are Better Suited for Augmenting the DOD CMF

The RCs are in a better position and more likely to augment (i.e., backfill) the DOD CMF for several reasons. First, the RCs are designed to augment and provide surge support to DOD’s active-duty force—including in the field of cyber. Examples of reserve cyber units include the Army Reserve Cyber Protection Brigade, the

Army National Guard 91st Cyber Brigade, the Air Force Reserve 960th Cyberspace Wing, and the Air National Guard 252nd Cyberspace Operations Group. The 1730 Report found that the RCs are an integral part of the DOD's cyberspace operations and ensure that the DOD is prepared to mobilize a surge capacity in times of crisis or conflict. Second, there are specific and clear authorities for activating reserve forces in the event of a cyber incident. In particular, 10 U.S.C. § 12304 authorizes the Secretary of Defense or the secretary of the department that operates the Coast Guard (currently DHS) to activate members of the reserve components to augment the active armed forces to respond to incidents that are likely to result in demonstrable harm to any of the following: national security interests, foreign relations, the economy of the United States, public confidence, civil liberties, or to the public health and safety of the people of the United States.⁴⁴ Third, reserve component cyber units follow the same training and qualification frameworks and pipelines as active units and are already organized into various CMF teams. Finally, utilizing reservists to backfill active-duty service members of the CMF is more straightforward from a legal point of view. According to a DOD staff judge advocate (SJA) that was interviewed for this study, the DOD already has a framework and processes in place to deal with legal issues that may occur when uniformed reservists are activated for duty such as dealing with conflicts of interest and handling liability issues in the event that a reservist gets injured or causes harm while activated.

⁴⁴ 10 U.S.C. § 12304(c) & 10 U.S.C. § 12304(k)(1), <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section12304&num=0&edition=prelim>

3 Outreach to Industry and Government Agencies

Section 1540(c)(3) asks for the result of outreach conducted with industry and State and Federal Government agencies employing individuals likely to meet qualification criteria for service in a CCR program.

To gain an understanding of how a CCR might be beneficial within the DOD construct as well as an indication for civilian interest in participating, stakeholders across the industry were consulted. The outreach included interviews with dozens of individuals actively employed in federal, state, or private-sector, cybersecurity-related job roles, most of whom also served the U.S. military in some capacity. Additionally, almost 1600 DOD cyber workforce members participated in a 16-question survey through which they provided anonymous feedback related to the CCR concept and its potential to fill cyber readiness shortfalls or gap areas. This section summarizes the results of this outreach. [Appendix A](#) contains the compiled output of the survey data.

Outreach Results

The consensus from interviews and surveys was that respondents shared a concern for the nation's cybersecurity posture, an enthusiasm that solutions such as a CCR are being considered, and an appreciation for the opportunity to provide their input. The number of people who participated in the survey exceeded expectations, with more than half also leaving comments with their survey submission. While the survey was active and interviews were taking place, individuals reached out with unsolicited requests to be interviewed, for information on how to get involved with the CCR, or to simply be updated on the status of the study and the CCR concept.

While respondents were nearly unanimous that a CCR was a worthwhile idea, they also highlighted complexities in relation to actual implementation. To leverage insight from these community stakeholders that would help inform the feasibility of the concept, their perspective on cyber needs and viable solutions was vital. The broad swath of participants from local to national levels, operators to senior leadership roles, and intermediate to extensive experience history, enabled a panoramic enumeration of challenges and potential remedies.

This section functions as a digest of the results from industry and state and federal outreach. It begins with a walkthrough of the gap areas identified in cyber mission readiness. It then itemizes common themes of challenges and concludes with suggestions that respondents provided, including lessons learned from existing initiatives comparable to the CCR concept.

Defining the Problem

“Some problems have only gotten worse over the years, no matter how hard we try to solve them,” a senior cyber leader of a government department confessed in light of decades of experience in both public and private sectors. While the interviews were crucial for learning about the problem areas in the cyber domain from community members, they also revealed aggravating factors that may require remedy in order for civilian expertise to provide value.

The top response to the question about gaps in cyber was that there is a lack of skilled cybersecurity professionals. This shortfall is said to increase the nation's vulnerability to threats, especially with respect to adversaries who prioritize and unleash their own cyber capabilities. Pressed further on specifics of whether the shortage was more capacity (numbers) or capability (skillsets), the responses were mixed. In terms of staffing,

interviewees described significant position vacancies, deprioritization of maintenance and non-mission critical duties, and teams stretched very thin on critical functions. For instance, an individual embedded in a service branch with a cyber planning role spoke of the imbalance of a handful of people being responsible for hundreds of assets and how that workload wasn't sustainable. The interviewee further added that "there is a team of us who are the only ones who can perform this one function that involves travel and time away from family and the typical day to day. The responsibility is typically rotated among a team of seven or eight members; that is now two."

When considering specific skill gaps, responses included lacking expertise with emerging technologies such as AI, shortage of crucial roles that are on the front lines of the cyber battle—offensive and defensive—and insufficient quantity of qualified personnel within certain DCWF work roles that are deemed critical. Example roles or skillsets identified as underrepresented include cloud security, data analytics, red-teaming, and offensive capability (effects) development. Figure 5 provides information about respondents' expectations about whether a CCR would address these skills shortages.

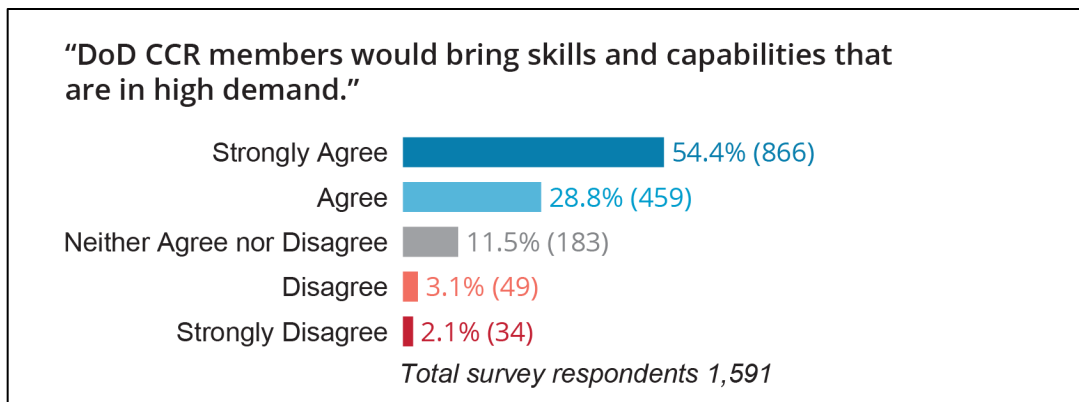


Figure 5: DOD survey results regarding skills and capabilities in high demand

Difficulty retaining top talent was frequently cited, largely caused by the financial and lifestyle opportunities available in the private sector. Significant resources are invested in training and experience building for members during their time of service. The private sector then reaps the benefits of these highly skilled individuals. Also, rotating uniform members every few years, depending on assignment, forces the departure of skilled experts and the need to constantly train and certify new talent.

Training is a major pain point identified by more than half of those interviewed. The insufficient resources budgeted for training as well as the extended time it takes to get new training developed and disseminated are perennial problems. Each service branch has its own workforce priorities, and the cyber workforce mission competes for resources with kinetic domain talent requirements. While some improvements have been made, the services continue to struggle with an inability to establish and maintain a baseline of core skills and cyber readiness requirements, which is a frustration voiced by several interviewees. A career field manager who is experienced with the evolution of the DCWF was one of a few participants who put the pieces together, stating, "If there was an emergency, and everybody was trained to the same standard, against the same matrix, we could put out a call across the Department for specifically coded talent and all come together to help solve a problem of national security for our country."

Critical infrastructure security, specifically those services supporting DOD facilities and the defense industrial base, and the poor collaboration perceived between privately owned organizations and the local and federal

government agencies, was a common concern. The infrastructure underpinning military might was described as a serious concern. It's not just the power plants, but the ports out of which forces deploy, the supply chains, water, hospitals, and all municipal services for bases that also caused concern. The urgency and level of concern for the defense of critical infrastructure was heard in numerous interviews and described in a group interview with senior department leadership as, "the thing that keeps us awake at night."

Challenges

The interviews and survey feedback mentioned challenges to consider with the use of civilians in a DOD environment. The need to obtain and maintain a security clearance to work on a government network or within most physical spaces was the challenge the overwhelming majority agreed would be a hurdle for some civilians. There is a cost, personal background review, and sponsor alignment requirement for obtaining a clearance. Some individuals may not consent to a background investigation, while others may be denied clearance due to their background. A civilian government employee exclaimed, "Some of the smartest people I've ever worked with in industry are ones who may not be able to maintain a security clearance. When it comes to cyber, there's a lot of super smart cyber people who, frankly, got smart by doing illegal things and breaking into things."

The necessity for security clearances is covered further in element 4 of the 1540. Section 4 of this report addresses that element.

Providing training or onboarding processes sufficient for a civilian to understand the operating environment was a challenge captured from input. Even if the civilian expert's role was tightly scoped to an area of expertise, he or she would still need to understand how components work together. Without drill requirements similar to those for traditional reserves, it was difficult to envision the ability for civilians to join a CPT in an emergency, for instance. However, CCR members providing training and mentoring, or serving in an advisory role within their lane of expertise and on emerging trends and techniques, was overwhelmingly seen as a benefit.

Study participants agreed that a clear, well-defined mission and role for a CCR is essential. Specific activities in which a CCR might engage are described later in this report under Section 6. The need for a scoped mission was explained from a few different angles. The primary reason was to aid coordination and limit confusion. During an incident, ambiguity over command authority between civilian reserves and other cyber units may lead to operational disconnects. Related, well-designed coordination will help alleviate resource diversion. Shifting resources and priorities from existing units to bolster new civilian reserves would reduce the readiness and capability of those exiting units. An established mission is vital to help shape the construct and viability of a CCR. A CCR would require detailing variables like skillsets needed, time commitment required, activities to keep members engaged during non-activation, and unique value, to ensure it does not conflict with other recruiting mechanisms.

Interviewees raised workforce disruption as a challenge. They were cautious about assuming civilian talent would be able to respond when summoned, especially for an extended period. While employers typically support reserve activations and abide by mechanisms like the Uniformed Services Employment and Reemployment Rights Act (USERRA), which protects the employment rights of reservists in the civilian sector—and some companies like Cisco offer salary gap pay during activation—the reality of the risk that cybersecurity teams will be diminished during critical business operations cannot be dismissed. Several interviewees remarked that their employer would be agreeable if the need were short term as other team members could effectively cover their duties. This limited absence from one's primary job would also alleviate

the concern described in interviews and reports of creating more competition for limited talent among military reserves, state defense forces, and private industry. Despite this reservation, the prevailing view was that a CCR could enhance overall cyber resilience without undermining existing capabilities.

To realize the vision of enhancing national cybersecurity capabilities by leveraging civilian technical talent in support of national mission objectives, it is imperative that eligibility criteria be defined. Interviews revealed that participants felt strongly about a CCR being limited to individuals who are vetted as subject matter experts. One veteran and a private business owner emphatically declared that “I would happily volunteer to be part of a cyber engineer corps if it were made up of qualified experts to solve problems and didn’t just accept curious or ambitious people who want to learn.”

It would be ideal for eligibility to serve in a CCR to align with the nature of the missions and identified skillset gap area. That nature is primarily intellectual and technical rather than physical. Qualification requirements are also discussed in Section 7 as required by Section 1540. During interviews, the topic of whether the traditional military reserves stringent eligibility requirements such as age and physical fitness benchmarks should be a barrier for otherwise qualified cyber professionals was commonly raised. Some asked, “How would one validate expertise and recertify as appropriate?”

Community feedback was keen to recognize and call out other logistical concerns with implementing a CCR that also appear as itemized elements for analysis in the 1540 requirements. The issues such as compensation, liabilities, authorities, and conflicts of interest are dissected in their respective sections within this report.

Insights and Existing Initiatives

Interviews revealed that a strong motivation to serve and a sense of civic duty outweighed traditional incentives such as rank or other federal benefits. More than a dozen veterans who are working in a private-sector cyber role and were interviewed for this study emphatically expressed their interest, driven by patriotism, to participate in a civilian reserve to strengthen national cybersecurity.

It is also worth mentioning that few participants expressed being incentivized by compensation. When posed with the question of whether payment for their time and effort would be a determining factor for them to participate in a CCR, only reimbursement for expenses was voiced.

Conversations with members of existing initiatives similar to the CCR concept provided insights on potential models. There are close to a dozen states with active civilian cyber corps or that are in the process of exploring their establishment. Multiple state cyber reserve leaders were interviewed for this study. Civilian cyber corps (C3s) organizations facilitate cyber volunteer services at the state level to aid with cyber challenges including response. State programs like the Michigan Cyber Civilian Corps (MiC3), Wisconsin Cyber Response Team, and California and Maryland Defense Force rely heavily on volunteers from the private or governments sectors. The states structure their own frameworks to address issues such as funding, insurance, eligibility, and authorities.⁴⁵ There are multi-layered vetting processes for members.

An active reserve component officer with decades of military and cyber experience advised that additional resources provided to the reserves would go a long way. Successes have already been realized in their ability to establish critical capabilities, effectively retaining highly trained talent, as well as leveraging civilian expertise.

⁴⁵ Civilian Cyber Corps: A Model Law for States: Appendix 3. Model Civilian Cyber Corps (C3) Law, <https://www.newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/appendix-3-model-civilian-cyber-corps-c3-law/>

The officer shared that they “spent millions of dollars to train these folks up and then we have positions for them to roll right into on the reserve side. We get to retain that capability as they continue to refine it in industry.”

Circling back to defending critical infrastructure, most small utility companies don’t have the expertise or finances to prioritize OT security, and they likely do not have a mandate requiring they do so. These are companies in local municipalities. There has been extensive reporting on these utility companies being targets of foreign adversaries.

The call to contribute to the greater good by protecting national security interests might not have a more exemplary model of success than DEF CON Franklin. DEF CON Franklin piloted a program partnering talented hackers with local water companies across several states to offer hands-on technical support. It was touted as cybersecurity as a public service with no mandates or red tape.⁴⁶ Vulnerabilities discovered are published with remediation information to aid national cyber resilience. While DEF CON was overwhelmed by the number of volunteers and had to pause applications, the program is expected to expand to more states and utility companies.

The recommendation to cultivate collaborative efforts and coordination among government agencies, law enforcement, and the private sector was suggested a handful of times. When companies experience a cyber incident, they may choose to call local authorities, the national guard, or the FBI. The authorities and experts who are the closest can be onsite quickest and are likely best suited to know the terrain but may still need access to more experienced talent.

Several industry representatives noted that participation in state cyber reserves enabled cross-sector knowledge sharing, improved readiness, and strengthened relationships between private and government entities. Local programs, if adequately resourced, are well positioned for cultivating a cohesive cybersecurity ecosystem capable of responding to both regional and national threats.

The result of the outreach conducted with industry and state and federal government agencies was enlightening. Participants provided invaluable insights on issues related to cyber gap areas or weaknesses, as well as thoughtful discussions for how a CCR might effectively contribute to collaborative solutions that strengthen the nation’s cybersecurity posture.

⁴⁶ DEF CON Franklin, Hackers and Industry Mobilize to Defend U.S. Water Systems, August 7, 2025, https://defconfranklin.com/water_cybersec.html

4 Necessity and Cost for Security Clearances

Section 1540(c)(4) asks for analysis of the necessity for participants to access classified information and the need to maintain appropriate security clearances as a participant in a CCR program, including while not in Federal service, as well as the cost of sponsoring clearances.

Necessity for Security Clearances and the Cost of Sponsorship in State and CCR Programs

As part of this study, interviewees were asked for their thoughts on the relative importance of obtaining and holding security clearances for CCR members. While discussions of appropriate CCR missions preceded and certainly influenced this feedback, the majority felt that CCR members could offer greater value to the DOD if some members held clearances. However, it was also suggested that clearances should not be made mandatory for all CCR members because that could potentially eliminate highly talented candidates who place a premium on privacy considerations.

DOD civilians and service members who responded to the survey used in this study indicated that security clearances were essential to providing value to DOD missions, as illustrated in Figure 6.

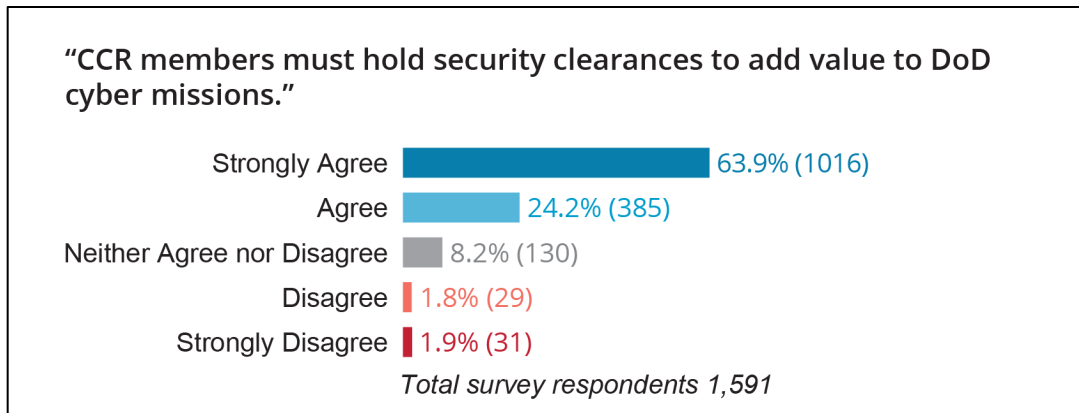


Figure 6: DOD survey results regarding the need for security clearances

The establishment of state and civilian cybersecurity reserve programs has raised complex considerations regarding the necessity for participants to access classified information and maintain appropriate security clearances. These concerns extend to individuals serving outside of federal military service, where maintaining clearances and the associated costs are often not fully supported by federal mechanisms.

The following are example missions requiring different levels of security clearance:

- **High-Sensitivity Incident Response and Collaboration:** Missions involving access to federal or DOD networks, classified intelligence, or participation in joint operations necessitate Top Secret (TC) or Secret-level clearances.
- **State-Level Critical Infrastructure and Incident Support:** Missions focused on state-level incident response and critical infrastructure protection, where the data is sensitive but not federally classified, often only require background checks and non-federal clearances. For example, Michigan’s Cyber

Civilian Corps (MiC3) operates without requiring federal clearances, and they rely instead on state-level vetting and employer validation to ensure that participants are trustworthy and capable.

- **Training, Exercises, and Public Education:** Cyber reserve missions focused on public cybersecurity awareness, training exercises, and simulations may not require any clearances. These activities prioritize knowledge sharing and preparedness without accessing sensitive systems, thereby reducing the need for costly clearance processes.

Necessity for Classified Access and Clearances

Many state and civilian cybersecurity programs involve incident response roles that may necessitate access to sensitive or classified information. For instance, Maryland's cyber units have personnel supporting classified processing, analysis, and dissemination within joint operations spaces involving both Army and Air components. Access to DOD information systems for these personnel often requires the issuance of a Volunteer Access Card (VoLAC), which serves as a proxy for the standard Common Access Card (CAC) used by federal personnel.

Furthermore, state defense forces, such as those in California and Wisconsin, face barriers when members are required to maintain clearances for their roles. These barriers arise from the inability to carry over federal clearances into state roles, necessitating the establishment of new clearance processes under the DHS or state security regimes. Notably, approximately 50 percent of personnel in these organizations are expected to possess clearances, reflecting the operational need for classified access.

However, in other states, such as Michigan, participation in incident response programs typically does not require federal security clearances. Instead, background checks and credentials appropriate for state and local networks suffice.

Clearance Maintenance Outside Federal Service

A significant challenge in sustaining a capable cyber reserve lies in maintaining security clearances for participants who are not in federal service. A leader in a state cyber force highlighted that individuals in Title 32 (state active duty) without federal clearances are restricted from accessing federal systems. In contrast, those with preexisting federal clearances can operate across state and federal boundaries. This divergence creates potential operational gaps, especially for states that rely heavily on volunteers whose clearances may lapse or lack support.

Managing security clearances, particularly in situations without federal sponsorship, is a complex and resource-intensive process. The process often requires repeated background investigations and clearances through state or DHS channels, resulting in inefficiencies and delays.

Costs of Sponsoring Security Clearances

Sponsoring clearances for civilian or state reserve personnel entails significant costs. A second state cyber force leader notes that costs for background checks alone (a prerequisite for clearance) can amount to \$72 per person, and additional expenses are incurred for security training and certifications such as SANS exams. The lack of federal funding to offset these costs imposes a burden on state programs, which may deter participation or limit the scalability of such initiatives.

The cost of a security clearance largely depends on the level of access required. A **Secret** clearance, corresponding to a Tier 3 background investigation, generally costs around \$500. A **TC** clearance, which

involves a Tier 5 investigation and may include enhanced screening or polygraph examinations, can range from \$5,000 to \$15,000 or more depending on complexity, agency-specific requirements, and investigative depth.

These costs are incurred by the government and contracting organizations, not the individuals undergoing investigation. Individuals are not permitted to apply or pay for a clearance on their own; they must be sponsored by a government agency or a cleared contractor with a validated need-to-know.

Payment Responsibility and Sponsorship Structures

The financial responsibility for obtaining a security clearance is determined by the type of sponsoring organization, with distinct funding mechanisms in place for federal agencies, Federally Funded Research Organizations (FFROs), and private defense contractors.

DOD Agencies

For active-duty personnel, federal civilian employees, and uniformed services within the DOD, the government directly funds the costs of security clearance investigations. Payments are typically managed through intra-governmental funding transfers to the Defense Counterintelligence and Security Agency (DCSA), which oversees the majority of federal background checks. These costs are absorbed as part of the agency's operating budget and are not visible to applicants externally.

Federally Funded Research and Development Centers (FFRDCs)

FFRDCs operate in close coordination with government sponsors but are technically non-governmental entities. In these cases, the **sponsoring federal agency** bears the financial responsibility for clearance costs. The process mirrors those used for internal federal employees, and clearances are managed through similar channels, typically using the same investigation tiers and agencies.

Defense Contractors

Contractor organizations also sponsor employees for security clearances. However, in these cases, the **contractor pays for the clearance**—either as a direct cost or by including it in indirect overhead rates billed to the government. While this shifts the administrative burden to the contractor, the costs are generally passed through in the pricing of deliverables or services under the terms of federal contracts. Clearance costs, therefore, form part of the negotiated contract price and are ultimately reimbursed by the government through labor or program costs.

Variations and Additional Factors

Several additional variables influence the overall cost of maintaining a cleared workforce. For example, polygraph requirements used by intelligence agencies such as the National Security Agency (NSA) or the Central Intelligence Agency (CIA) add significantly to clearance costs, as does the necessity of periodic reinvestigations (although many agencies are transitioning to a continuous vetting model that reduces the frequency of large-scale reinvestigations).

Furthermore, timelines and administrative overhead can vary across organizations. Some agencies may require more frequent updates or conduct more intensive background checks, depending on the sensitivity of the mission and its access requirements.

Moreover, administrative processes for clearances and credentials often involve prolonged timelines, with background checks potentially taking weeks to complete and clearances taking months to years to process. The cumulative effect of these costs and delays underscores the need for streamlined clearance processes and funding support if cyber reserve programs are to fulfill their critical missions effectively.

The evolving landscape of state and civilian cybersecurity reserves necessitates careful consideration of access to classified information and the management of security clearances. As these programs increasingly supplement federal and state cyber incident response capabilities, the challenges of maintaining clearances for non-federal participants, along with the associated financial burdens, must be addressed. Policy interventions to harmonize clearance requirements and provide funding support are essential to ensure the viability and readiness of these emerging cybersecurity forces.

5 Appropriate Member Compensation and Benefits

Section 1540(c)(5) asks to consider appropriate compensation and benefits for members of a CCR program.

As cyber threats intensify globally, the establishment of a CCR emerges as a critical complement to existing defense and response infrastructures. Designing appropriate compensation and benefits for these members requires examining established frameworks in both traditional military reserves and emerging state cyber reserve programs.

Compensation and Benefits

Traditional Military Reserves

Traditional military reserves, including the U.S. Army Reserve (USAR) and the National Guard, offer a structured system of compensation and benefits designed to attract and retain skilled personnel. Key elements include:

- **Pay:** Reservists receive drill pay based on rank and years of service, aligned with active-duty pay rates, for training activities and active deployments. Annual training (AT) and inactive duty training (IDT) are compensated under established military pay scales.
- **Bonuses and Incentives:** Enlistment and re-enlistment bonuses, often targeting critical skills such as cybersecurity, serve as financial incentives for recruitment and retention.
- **Benefits:** Comprehensive benefits include access to health insurance, retirement benefits accruing through a points system, tuition assistance, and the Montgomery GI Bill Selected Reserve (MGIB-SR).
- **Legal Protections:** Protections under the Uniformed Services Employment and Reemployment Rights Act (USERRA) ensure that the civilian employment rights of reservists are maintained during and after their service.

State Cyber Reserves

Interviews with representatives from various state cyber reserve programs reveal significant variations in compensation and benefits structures:

- **Michigan Cyber Civilian Corps (MiC3):** MiC3 operates voluntarily, with no direct financial compensation. Members benefit from professional development opportunities, access to training, and recognition for public service but do not receive salaries, stipends, or structured benefits.
- **Wisconsin Cyber Response Team:** Similarly, Wisconsin's approach emphasizes voluntary participation without direct financial compensation. Members may receive professional development, credentials, and access to training, but they often lack standardized benefits.
- **California and Maryland Cyber Reserve:** This organization provides a more structured framework, offering activation pay, access to state-sponsored insurance during missions, and

stipends tied to Title 32 status. These benefits align with state active-duty provisions and include base pay, legal protections, and operational support.

- **Texas Cyber Command:** On June 2, 2025, Texas enacted House Bill 150⁴⁷, which established the Texas Cyber Command, a component institution of the University of Texas System. The command's authorities only apply to public and governmental bodies in the state, but its mission is quite broad, as outlined in the following section of the Texas Cyber Command bill:

The Command is established to prevent and respond to cybersecurity incidents that affect governmental entities and critical infrastructure in this state, and among other responsibilities, is responsible for providing leadership, guidance, and tools to enhance cybersecurity defenses, facilitating education and training of a cybersecurity workforce, monitoring and coordinating cyber threat intelligence and information systems, creating partnerships needed to carry out the Command's functions, and receiving all cybersecurity incident reports from state agencies and covered entities.

The Texas Cyber Command bill includes funding for 65 STE in FY2026 and 130 FTE in FY2027. Standard state and University of Texas system employee compensation and benefits are accounted for as part of appropriations.

Notional Model for CCR Compensation and Benefits

To estimate costs for compensation and benefits, a notional CCR organizational model was conceptualized for this study and is presented below. While this model could serve as a reference to USG policy makers, it is not intended as a comprehensive or vetted solution and does not include details on mission parameters, command and control, structure, and so on.

This notional CCR is envisioned as a voluntary national service organization designed to strengthen the nation's cybersecurity resilience by leveraging the skills and expertise of civilian professionals. Modeled in part on the DOD reserve structure and informed by successful state cyber initiatives, this theoretical CCR organizational model provides a framework for pay, benefits, service commitments, healthcare protections, professional development stipends, and retirement incentives. Key differences with existing uniformed reserve components are as follows:

- no requirement for basic military training or initial technical training
- no medical examination requirement or physical conditioning and appearance standards
- relaxed uniform standards (custom CCR polo shirt, slacks)
- one day per month virtual assembly plus one week per year in-person assembly

Cyber Specialist (CS) CCR Member

Members are compensated according to a specialized pay scale aligned with DOD warrant officer grades, supported by stipends for professional development, specialized education, and industry certifications. Legal protections are provided under the USERRA. Federal healthcare benefits are available during extended activations and retirement savings are enhanced through matching contributions. To recruit and retain

⁴⁷ HB150 by Capriglione (Relating to the establishment of the Texas Cyber Command and the transfer to it of certain powers and duties of the Department of Information Resources.), <https://capitol.texas.gov/tlodocs/89R/fiscalnotes/html/HB00150F.htm>

individuals with critical skills, signing and retention bonuses may be authorized, ensuring the reserve attracts and sustains the talent essential for national cybersecurity readiness.

Service Commitment

While the CCR is a voluntary organization, members would enter into service agreements to serve for a minimum term of two years and renew at two-year intervals. All new CCR members will first complete a one-year probationary period, during which their performance, participation, and suitability for continued service will be evaluated. At the end of this probationary period, members deemed a good fit will continue under the standard two-year renewable commitment.

CCR members are required to complete an annual service of nineteen days. This period includes one day of virtual participation each month and seven days of in-person duties each year dedicated to professional development, exercises, or operational deployments. It may also be useful to allow CCR candidates to select from a small range of service commitment options. For example, DOD retirees may desire to commit to more duty days than the standard baseline of 19. Regardless, it is important to note that this proposed two-year service commitment is binding only for the specified number of duty days in the contract. Any additional days of service or activation periods above the baseline are considered voluntary. The CCR administrative office or command may request volunteers for extra days of service as needed.

Several former DOD CMF service members were interviewed (not serving in the RC), and their feedback indicated that contractually mandated extended (non-voluntary) activation periods could hinder CCR recruitment and retention. Figure 7 shows survey results on the topic of gathering virtually.

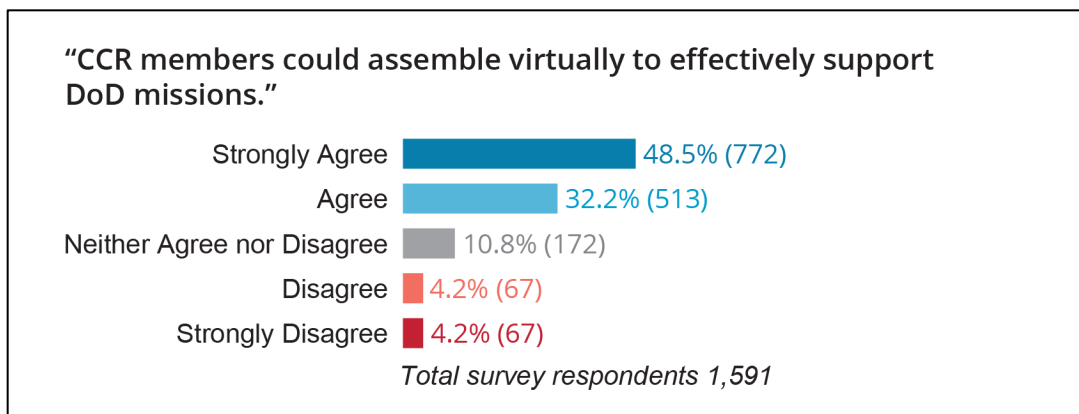


Figure 7: DOD survey results regarding monthly virtual assemblies

In-person duty includes authorized travel to and from the duty site, lodging, meals, and incidental expenses in accordance with applicable federal per diem regulations.

Pay, Benefits, and Advancement

Before being appointed as a CCR member, applicants' résumés, education, professional experience, and specialized skills shall be formally assessed to determine their eligibility and initial pay grade within the cyber reserve.

All members who successfully complete the probationary period shall also be evaluated to ensure that their assigned grade is properly aligned with their demonstrated qualifications, with subsequent reevaluation taking place after two years of continued service. Pay grades will be based on the DOD warrant officer scale (W1

through W5), with relevant experience influencing grade assignment. Pay grades shall be reviewed at least every two years to assess whether members qualify for promotion and advancement based on established criteria, ensuring a transparent, fair, and merit-based progression system. When performing official duties, including training, professional development, exercises, or operational deployments, members shall receive pay and benefits appropriate to their designated pay grade.

Signing and Retention Incentives

To ensure the recruitment and ongoing service of personnel with critical skills, the CCR may authorize signing bonuses upon appointment and retention bonuses at specified intervals. These incentives will be targeted toward occupations or specialties considered essential for mission success and national cybersecurity readiness and will be administered in accordance with relevant federal compensation policies and oversight requirements.

Duty Pay and Travel Reimbursements

CRR members are entitled to duty pay based on a specific cyber reserve service pay scale during duty, training, exercises, or operational incident response. Besides duty pay, travel reimbursements may be approved to compensate members for ongoing participation in annual duty, cyber exercises, operational assignments, or other approved activities.

Compensation should be structured to fairly acknowledge the time invested, dedication, and professional expertise of members, while aligning with federal compensation and benefits practices.

Healthcare and Legal Protections

Members of the CRR must maintain primary healthcare coverage through their civilian employers or the healthcare marketplace.⁴⁸ Federal health insurance benefits will only be provided during activation periods exceeding thirty consecutive days.

Furthermore, members are entitled to legal protections equal to those provided under the Uniformed Services Employment and Reemployment Rights Act, ensuring continuity of civilian employment and protection against adverse employment actions related to reserve duty.

Retirement and Recognition Incentives

A 401(k) retirement savings plan with employer matching contributions of up to five percent could be established for members of the CRR.

Additionally, an awards program may be established to honor exceptional performance based on established DOD practices. These initiatives could offer both long-term financial security and formal recognition of outstanding service, thereby strengthening member retention, professional pride, and mission effectiveness.

As a CCR operating at the intersection of public service and national cyber resilience, the organization needs a compensation and benefits system that combines the strong incentives of traditional military reserve models with the flexibility of state-level cyber programs. By including activation pay, professional development

⁴⁸ The location of the marketplace can be accessed through the following URL: <https://www.healthcare.gov/>

opportunities, legal protections, and targeted retention incentives, this system aims to attract, acknowledge, and maintain the highly skilled talent vital to enhancing national cybersecurity preparedness.

Table 2 shows the estimated compensation and benefits costs for a CCR member.

Table 2: Cost estimation

Pay Grade	Annual Pay (19 days) (\$)	Travel Lodging M&IE Air/Car	Education Stipend	Overhead (training, admin, equipping, uniforms)	Total Government Baseline Cost per Person
CS-1 (4+ yrs)	\$3,420	~\$1,846 /yearly	\$2,500 /yearly	~\$5,000 /yearly	~\$12,766 /yearly
CS-2 (8+ yrs)	\$4,180	~\$1,846 /yearly	\$2,500 /yearly	~\$5,000 /yearly	~\$13,526 /yearly
CS-3 (12+ yrs)	\$4,940	~\$1,846 /yearly	\$2,500 /yearly	~\$5,000 /yearly	~\$14,286 /yearly
CS-4 (16+ yrs)	\$5,890	~\$1,846 /yearly	\$2,500 /yearly	~\$5,000 /yearly	~\$15,266 /yearly
CS-5 (20+ yrs)	\$6,840	~\$1,846 /yearly	\$2,500 /yearly	~\$5,000 /yearly	~\$16,186 /yearly

Travel Expenses

For planning and reimbursement, travel expenses for CCR members include transportation, lodging, meals, and incidental expenses according to federal travel regulations. When travel occurs by privately owned vehicle, mileage is reimbursed at the General Services Administration (GSA) standard rate of (\$0.70) per mile. When travel occurs by commercial air, reimbursement is based on coach class airfare, which generally ranges from (\$600) to (\$1,200) for cross-country trips, and from (\$200) to (\$600) for regional flights. Lodging expenses are reimbursed at the applicable GSA per diem rate, which for Fiscal Year 2025 is (\$110) per night in standard areas, with higher limits in designated non-standard areas. Meals and incidental expenses (M&IE) are reimbursed at the standard GSA rate of (\$68) per day unless a higher local rate applies.⁴⁹ These rates serve as the baseline for estimating and authorizing travel expenses related to duty, training, exercises, or operational deployments.⁵⁰

Legal Feedback on Notional CCR Model

The notional model outlined above in Section 5 of this report was shared with a senior USCC staff judge advocate (lawyer) during an interview. This was done to illicit professional and legal feedback on the hybrid service commitment proposed in this report. In this concept, CCR members sign binding contracts that commit them to serving a fixed amount of duty days per year, but any additional days of service above this baseline are considered voluntary, wherein members can respond to mission support announcements posted by the CCR’s administrative/owning organization. These support requests would describe the mission and skillsets needed, the location if physical presence is required, expected activation duration, and other details that would ensure respondents “fit the bill.” The consulting SJA concurred that this approach was viable and further stated that CCR members must be covered by USERRA protections. This officer reflected that precedence exists due to the passing of the Civilian Reservist Emergency Workforce (CREW) act of 2022.⁵¹

⁴⁹ U.S. General Services Administration, “M&IE Breakdowns,” GSA Per Diem Rate Resources.

⁵⁰ U.S. General Services Administration, “FY 2025 CONUS Per Diem Rates,” August 16, 2024.

⁵¹ S.2293 - CREW Act, 117th Congress (2021-2022), <https://www.congress.gov/bill/117th-congress/senate-bill/2293>

6 Activities CCR Members May Undertake

Section 1540(c)(6) asks to consider activities that members may undertake as part of their duties.

To understand the feasibility of establishing a DOD CCR, it is important to first consider what mission sets a CCR could and should support. The range of missions could be exhaustive to include direct support of both offensive and defensive cyber operations or non-operational support missions like providing training and assessments for active and reserve component personnel. Each mission set comes with potential benefits, risks, and constraints. Consequently, Section 1540 of the FY23 NDAA narrows these expectations somewhat by specifying that the intent of a CCR is “to provide qualified civilian staffing to the Department of Defense to effectively respond to significant cyber incidents or to assist in solving other exceptionally difficult cyber workforce-related challenges.”

CCR Mission Scenarios

These extraordinary employment expectations can assist in shaping the potential makeup and mission sets of a DOD CCR. To further elucidate this makeup, it is helpful to identify plausible scenarios for each circumstance.

A. Response to significant cyber incidents

Response scenarios are, by their nature, defensive missions. As noted above, the majority of personnel in the DOD COF work in IT, and IT security roles and the majority of teams in the CMF are CPTs in both the active and reserve components. Since there is considerable defensive capacity already, a CCR could feasibly provide surge support when full-time government civilian and uniformed personnel and activated reserve components are incapable of meeting staffing requirements during an emergency. An example scenario might involve a massive disruption or destruction of enterprise IT or mission systems due to a pervasive supply-chain compromise, zero-day ransomware, crisis-inducing software vulnerability, or other advanced cyber attack that overwhelms containment and recovery efforts of DOD cyberspace security and personnel protection.

Cyber-physical equipment or adjacent technology is compromised causing direct and collateral impact on DOD operations or personnel safety. This event could be realized through multiple scenarios to include cyber-induced disruptions of upstream utilities and other critical services to military installations, cyber attacks impacting specialized healthcare and life-support systems in military hospitals, or catastrophic damage from natural disasters that require significant IT and cybersecurity recovery efforts. These scenarios can impact continuity of military operations and may require the backfill of reprioritized DOD cyber defenders and responders via a CCR.

A significant adversary attack on U.S. critical infrastructure during a declared national emergency or state of war. The U.S. national command authority may prioritize the Defend the Nation or Defense Support of Civil Authorities⁵² (DSCA) missions when the health and safety of the U.S. civilian population are at risk. Under these authorities, a DOD CCR could feasibly be used for direct support to these homeland security emergencies.

⁵² Congressional Research Service, Defense Primer: Defense Support of Civil Authorities, Updated April 9, 2025, https://www.congress.gov/crs_external_products/IF/PDF/IF11324/IF11324.16.pdf

B. Solving exceptionally difficult cyber workforce challenges

- A CCR could potentially include experts with advanced cybersecurity skillsets such as securing and performing response and forensics in cloud computing, advanced malware reverse engineering, high-volume data engineering and analytics, advanced software engineering, and AI.
- A CCR may also provide expertise in OT systems and mission-critical legacy OT systems, possibly written in legacy programming languages.
- A CCR could provide cyber threat intelligence experts with specific foreign language abilities (Chinese, Russian, Persian, Korean, Arabic, etc.).
- A CCR may include retired or separated former members of CMF teams that were cleared and fully qualified to perform missions where current CMF staffing levels are insufficient or lack the degree of mastery or expertise required for highly specialized mission sets (e.g., support for offensive cyber operations). These CCR members may work in private industry and wish to continue to perform DOD missions but do not wish to join the uniformed RC.
- A CCR could provide vulnerability discovery (red teaming) capabilities for weapons systems security or for assessing the internal or external security of the DODIN enterprise. This mission could be extended to mitigating these discovered vulnerabilities and perhaps developing capabilities (effects) for weaponizing novel vulnerabilities.

CCR Sustainment Missions

Using the notional CCR model described in Section 5 of this report, a hybrid approach can be envisioned whereby a CCR performs both sustaining and response missions as part of its charter. Sustaining missions provide value to the DOD and the nation in a proactive sense and are not subject to the urgent timelines and less predictable nature of response missions. In the context of the notional CCR model, sustainment missions can usually be conducted virtually, primarily utilizing baseline duty days built-in to members' service commitment contracts.

The following are examples of sustainment mission sets:

- advanced training development and delivery
- software tools and capabilities development
- red teaming and security assessments
- applied research and TTP development
- exercise planning, development, administration, and participation
- AI LLM engineering or agentic model development

CCR Response Missions

Response missions typically require more precise matching of CCR member expertise and skillsets to the specific technical details of the cybersecurity incident. These missions will likely be driven by DOD workforce capacity and capability gaps. For example, a CCR could be assigned to a CI response mission that requires specific expertise with a particular ICS or OT technology. Another CCR response mission may involve post-incident recovery actions that involve restoring and testing compromised systems.

The following are examples of response mission sets:

- investigative analysis of large datasets
- authorship of custom code/scripts to support investigations
- advanced malware analysis and reverse engineering
- analysis of niche systems not used by the DOD (ICS and OT, mainframes, etc.)
- surge analysis and recovery support of compromised networks and systems

Interview Perspectives on CCR Missions

As mentioned previously, approximately 50 interviews were conducted with cyber professionals from private industry, U.S. congressional staff, USG interagency, and across the spectrum of DOD civilians and active, reserve, and former or retired uniformed service members. All the interviews included discussions on potential CCR missions. The following are excerpted or paraphrased summaries on this topic.

The most suggested CCR mission across all interviewees was the protection of U.S. critical infrastructure (CI). These discussions included concerns about the DOD's authorities to pursue this mission. However, the majority refrain was that the country is most vulnerable to devastating, asymmetric attack due to systemic security weakness in CI and a lack of protective and response resources available during a significant nation-state attack or national emergency. Currently, CISA leads the U.S. CI protection mission, and the FBI leads the U.S. CI incident response mission. Current U.S. CI law limits what CISA and FBI can do, since there are no legislative mandates on the private sector to report to or engage with USG agencies on CI protection matters.⁵³ Conversely, this does mean that CI operators in the private sector (and state and local governments) can voluntarily report issues and request assistance from the federal government.⁵⁴ A CI protection resource gap is illustrated by the utilization and popularity of the DEF CON Franklin program, mentioned in Section 3 of this report. This program demonstrates that civilians have a strong propensity to serve the country by protecting U.S. CI for the benefit of national security.

However, if a widespread and highly disruptive attack on U.S. CI occurs, interview feedback suggests that a scalable and coordinated USG response would likely rely on or be led by the DOD as part of its Defend the Nation mission. This feedback is buttressed and built upon in a 2019 Cyber Defense Review (CDR) report.⁵⁵ That report describes current uncertainty surrounding authorities and responsibilities of the DOD's Defend the Nation mission. The paper an important thought piece that should be considered carefully as it focuses on "the role of the DOD in the conceptual clarity of a black-and-white scenario of a true cyber war targeting the [U.S.] private sector." In this scenario, the paper "suggests four additional pillars of support: private-sector call for fire support, coordination of multi-stakeholder defensive actions, response-support forces, and private-sector access to the entire intelligence cycle. Together, these can be a new approach: "Defense Support to the Private Sector" (DSPS)." Preparing for war with a pacing adversary who would target U.S. CI is prudent and deserves special consideration.

⁵³ H.R.5005 - Homeland Security Act of 2002, 107th Congress (2001-2002), <https://www.congress.gov/bill/107th-congress/house-bill/5005/text/pl>

⁵⁴ Protected Critical Infrastructure Information (PCII) Program, *An information-protection program to enhance information sharing between the private sector and the government.*, <https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program>

⁵⁵ Healey, Jason and Korn, Erik B., Defense Support to the Private Sector, *New Concepts for the DoD's National Cyber Defense Mission*, <https://cyberdefensereview.army.mil/Portals/6/Session%205%20Number%201%20CDR-Special%20Edition-2019.pdf>

During interviews with several leaders from another USCC service component command, the concept of a CCR made up of elite cybersecurity experts from industry and academia to provide advisory and instructive support to CMF teams was viewed favorably. However, it was called out that members of the uniformed reserve components already provide this capability to a degree, intimating that the impact of this existing program is helpful but also limited by skillset matching and availability of annual individual mobilization augmentee (IMA) duty days. Other obstacles were noted during interviews, particularly the stated requirement that CCR members would need to hold TS or Sensitive Compartmented Information (SCI) security clearances to participate in most CMF missions.

In another interview, a former White House staff cyber policy advisor stated that a CCR may provide benefit if used for “clean-up” and recovery efforts following a significant cyber attack. This individual referenced an incident where law enforcement and technical incident responders reported that detection, response, and eradication efforts were concluded within a week. However, large-scale recovery efforts (restoring backups, re-imaging compromised computers, etc.) would take weeks or months to complete. While the referenced cyber incident occurred on private sector healthcare networks (not DODIN), the interviewee believed capacity issues may exist in DOD recovery efforts and a CCR made up largely of IT security professionals could fill gaps while lessening expertise and clearance requirements.

An interview was conducted with an active-duty officer assigned to a CMF team responsible for offensive cyber operations. This officer related that significant staffing (capacity) and talent (capability) gaps exist in the DOD’s offensive cyber workforce and that these gaps “negatively impact cyber operations every day.” Moreover, this officer stated that the DOD is not keeping pace with foreign adversaries and explained that part of the reason for this is that the individual military services prioritize their native warfighting domains over cyberspace. This reality takes the DOD’s top cyber talent off mission routinely, and the high operations tempo leads to burnout and retention problems. Furthermore, the officer stated that the two-year FORGE training pipeline to certify offensive operators is saturated and opined that it could be shortened, streamlined, or broadened to increase capacity. When asked how a CCR might address these issues, the officer said that a CCR could offer separating or former cyber operators a way to continue serving the country without the potential of long mobilization periods of traditional uniformed RC service.

A follow-on question was posed in the interviews concerning practical challenges that could impede CCR participation in certain missions. In answering this question, an offensive cyber operations (OCO) officer acknowledged that security clearance level (TS and SCI plus polygraph) and interactive on-net (ION) operator crew certification maintenance would likely preclude CCR members from participating in direct OCO missions. However, this officer stated that a CCR could indirectly support OCO missions by conducting targeted vulnerability research and by developing capabilities (exploits) for discovered vulnerabilities. It should be noted that a high-ranking retired officer concurred with this proposed CCR mission and stated that a top USAF software factory conducted similar unclassified research and development, and that a CCR could augment and scale these efforts.

Several interviewees suggested that a CCR could provide value to the DOD by taking on a training and education mission with emphasis on emerging and specialized technologies or cutting-edge cybersecurity practices. The DOD’s cyber training schools were described as effective but perpetually behind due to the rapid pace of change in cyber and the significant burden of updating training content and materials on a timely basis. As a prime example, AI training from industry experts (members of a CCR) could bridge the gap in helping the DOD leverage AI to enhance and modernize DOD cybersecurity and cyber operations missions. Other potential CCR training mission topics mentioned by interviewees included development security

operations (DevSecOps), cloud security and forensics, data engineering and analysis, industrial control systems and OT, and advanced or niche software engineering practices.

An interview was also conducted with a retired flag officer who commanded one of USCC's service components. This retired officer was concerned about mission readiness and capacity issues within the CMF. He estimated that "out of the approximately 6,2000 authorized CMF billets, I suspect with some confidence that they are about 80 percent filled. So that means the Department's paying for 6,200, but they only have about 5,000 in the formation. Of those 5,000, I suspect that they're about 50 percent fully qualified. Okay, so that means 2,500." He acknowledged that his estimates were dated but felt that the DOD should be open with Congress concerning staffing and readiness issues.

Additionally, this interviewee stated "I've heard a couple of previous commanders of U.S. Cyber Command talk about the strategic environment in terms of the competitive landscape or the threat or the adversaries or capabilities or just what the real world in cyberspace looks like. I've consolidated their words into what I call the four (4) no's of cyberspace: 1. There is no rear area. 2. There is no safe bastion. 3. There is no operational pause. 4. There is no strategic reserve." This retired officer emphasized the serious risk to national security that comes with a lack of a strategic U.S. cybersecurity reserve and indicated that the USG's cyber workforce (to include the Department of Justice (DOJ), DHS, and the DOD) is insufficient to successfully respond to a catastrophic cyber attack on the nation from pacing adversaries. He went on to suggest that a strategic CCR "is vital and necessary" and that the DOD "can mine the depth of a wide range of expertise and experience to bring emerging practices [to the DOD] for rapid adoption and to [increase] scalability [in times of crisis]."

7 Methods for Identifying and Recruiting

Section 1540(c)(7) asks for analysis of methods for identifying and recruiting members, including alternative methods to traditional qualifications requirements.

The crux of a functional CCR is having qualified individuals at the ready when a need arises to call upon them for support. Surveying approaches for recruitment were explored and considered for alignment with the concept of a CCR. That is, recruiting strategies that could target and net qualified civilian cyber professionals to assist the government for a short period of time with an urgent or difficult issue.

As previously highlighted, clearly defining the mission that CCR members would participate in could help to scope the desired talent pool. In reviewing mechanisms for identifying and attracting cyber professionals, the exploration and results apply to a gamut of cyber-related work roles.

Strategic CCR Recruitment

Military reserve programs have modernized or augmented their models to better align with mission goals as well as appeal to recruitable talent. It is important to note the careful balance required to incentivize civilian talent to join a CCR so that it is not a detriment to other personnel staffing and recruiting efforts. The value of obtaining talent from civilians working in the private sector is recognized and appreciated— “they’re worth their weight in gold,” as described in a USAF reserve leadership interview. Services have reservists whose civilian occupation involves the same discipline as the service branch mission. However, with cyber there are complexities and a wide diversity of skillsets as opposed to, for instance, a professional commercial airline pilot who flies planes for reserve duty. In the example of the pilot, there is less risk of proprietary mission detail being leaked and less training cycles to stay abreast of the operating environment. There is a much different cadence and evolution in the cyber domain. The civilian cyber reservist needs meaningful time drilling and being embedded with the tools, environment, and interoperability of services and data to keep pace with evolving technology. However, for CCR purposes and what might compel specialized and elite-level talent to assist for an urgent event or difficult problem, some compromise may be prudent.

A recent article from the Virginia National Guard described the success of a direct commission program with the Army National Guard where civilian expertise is leveraged by appointing them to an officer rank, thereby enabling them to apply their skillsets in a leadership position. The arrangement, through an RC, provides the balance to maintain a full-time job and fulfill their desire to participate in protecting national security. For specialized elite-level cyber expertise, mutually beneficial relationships similar to this example could entice civilian talent to serve.⁵⁶

The significant advantages CCR members would have if they earned a higher salary from a private sector full-time job, a role serving their country, and having access to insider intel and cutting-edge technology is substantial but difficult to quantify. It is not only a key concern itemized in related literature, but it was raised during the interview with USAF reserve wing’s leadership. They were concerned that recruiting for a CCR could be detrimental to the reserve’s ability to fill the significant amount of unfilled civilian positions. Further,

⁵⁶ Keller, Meghan, *91st Cyber Brigade direct commissions veteran as LTC*, March 2025, <https://va.ng.mil/News/Article/4113732/91st-cyber-brigade-direct-commissions-veteran-as-ltc/>

the group hypothesized that those currently working in full-time civilian positions at the DOD may want to transition to the CCR instead if they saw it as a more flexible and profitable arrangement.

Designing a CCR strategically to target a subset of the recruitable cyber workforce and limiting the impact on other recruiting efforts was suggested in interviews. Details such as selective qualifying criteria and incentives based on work performed were described. Additionally, tagging the CCR with an elite name, logo, mission description, casual uniform, and skill or achievement badges were other ideas captured in discussions for enticing participation.

Retention of highly trained and experienced talent may also improve with an attractive CCR model. For example, the National Guard reserves reported successes in attracting talent to continue their service in a reserve capacity. An interviewee in a leadership role within a National Guard unit explained how they invest “millions of dollars [...] to train and provide experience for members; when they come off active duty, positions are ready for them in reserve capacity. They’re taking experience from the military into the private sector, where they continue to refine it in industry and bring it back.” These service members would be ideal recruiters for a CCR. They know the skillsets required for DOD cyber operations and would recognize those abilities in their civilian-sector network of colleagues.

Qualification Identification

This comprehension of skills and abilities required for CCR missions is a fundamental piece of the recruiting strategy. To address a difficult problem—whether it involves response or recovery, or capability or capacity—it’s crucial to know what the most effective resources are for the solution, to understand how to locate them, and to have confidence in the resources’ abilities. Once the talent or skillsets required for CCR missions are determined, recruiting efforts can be better scoped. There are mechanisms to validate an individual’s professional experience and capabilities that could be leveraged to identify talent for a CCR and recruit for it.

To determine the qualifications or expertise criteria for a CCR, and to locate where to recruit that talent, existing methods for workforce management, sector professional organizations, and similar cyber reserves could be leveraged. This is where describing crucial skillsets, relevant experiences, and capability indicators for cyber roles is essential.

Job position screening and aptitude tests to assess candidate qualifications are common for high-tech job roles. The NSA uses testing for a variety of job roles tailored to the needs of the role. These assessments are aptitude and performance based and provide data-driven insights on a person’s alignment to duty requirements rather than solely relying on a resume. Hands-on simulated virtual environments are heavily utilized for training and team exercising as well as in cybersecurity competitions. These competition-style events—which attract top cyber talent to use their sharpened skillsets to achieve a difficult end goal—could aid in identifying, assessing, and recruiting CCR members. The annual President’s Cup Cybersecurity Competition (PCCC) and Hack The Pentagon are examples of performance-based events. These government-sponsored cyber competitions were designed to attract top experts in the cyber field and give them an opportunity to demonstrate their technical prowess. The PCCC gathers over a thousand competitors annually from federal agencies and the DOD to engage in scenario-driven, capture-the-flag type cyber challenges to earn their way up the leaderboard and advance to more difficult rounds. The users demonstrate troubleshooting, problem-solving, teamwork, and

technical proficiency by completing tasks aligned with the NICE Framework. It's an initiative that identifies and rewards individuals who possess specific skillsets.⁵⁷

A similar program that awarded individuals for proving their cyber talent was Hack The Pentagon, which was organized through the Defense Digital Service. It is described as a bug bounty program where ethical hackers were used to find and report vulnerabilities on government systems, and they received monetary rewards for their work.⁵⁸ These examples demonstrate a willingness of top cyber talent to engage and contribute their expertise in pursuit of recognition or to fulfill their desire to be part of a greater good. These programs provide a mechanism for cyber experts to prove their skills and capabilities, making them a potential source for CCR recruitment.

Professional membership organizations and trade associations are other avenues for locating specific talent. For instance, industry certification agencies maintain records of professionals who have earned and maintained criteria for certification. Earning a certification typically includes passing an assessment that demonstrates concept comprehension and continued accumulation of professional development credits. Acronyms, such as CISSP (which stands for the Certified Information Systems Security Professional credential), are commonly included in position description requirements. The credential itself doesn't validate the technical capabilities of an individual; however, the concentration of each certification is scoped to a community of professionals with varying levels of expertise within that specialty lane.

Professional membership organizations are established to collaborate and contribute to the betterment of their industry. Information Sharing and Analysis Centers (ISACs) are collaborative bodies designed to enhance information flow between private-sector critical infrastructure and government. ISACs for industries such as finance, healthcare, aviation, and energy share cyber threat intel and defensive best practices to help mitigate risks and enhance resiliency.⁵⁹ Similarly, CISA sponsors the Protected Critical Infrastructure Information (PCII) Program⁶⁰ to encourage information sharing between the private-sector infrastructure owners and the government. CISA also sponsors the Joint Cyber Defense Collaborative⁶¹ with the goal to unify cyber defense capabilities. These participative associations on the leading edge of the state of practice are made up of seasoned experts. The value they could add to CCR recruitment, outreach, and coordination is immeasurable.

Colleges, universities, and other educational institutions that offer cyber-related programs are optimum sources for CCR recruitment efforts. Partnerships with higher education institutions to cultivate cyber workforces of the future are common. Government-academia coordination such as Centers of Academic Excellence (CAE) and Scholarship for Service (SFS) build a pipeline of trained individuals aligned with industry priorities and

⁵⁷ Casey, Denise, *NCIS Cyber Analyst Competes in President's Cup Cybersecurity Competition*, NEWS | May 8, 2025, <https://www.ncis.navy.mil/Media/News/Article/4177813/ncis-cyber-analyst-competes-in-presidents-cup-cybersecurity-competition/>

⁵⁸ Defense Digital Service (DDS), HACK THE PENTAGON, <https://www.ai.mil/about/organization/dds/hack-the-pentagon/>

⁵⁹ National Council of ISACs, ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators. <https://www.nationalisacs.org/>

⁶⁰ Protected Critical Infrastructure Information (PCII) Program, *An information-protection program to enhance information sharing between the private sector and the government*. <https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program>

⁶¹ Joint Cyber Defense Collaborative, *No one entity can secure cyberspace alone*. <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>

provide opportunities for scholarships and guidance for careers within government agencies. These audiences are a natural fit for recruitment into a CCR.

In summary, there are a multitude of sources to locate cyber professionals that provide the potential to scope talent according to specific specialties via degree, credentials, or other achievements. The ideal scenario for a CCR is the ability to precisely and rapidly locate a person or group of people with a specific skill or competency to respond to an urgent issue. Maintaining a data management strategy that stores skills, credentials, achievements, and variables such as security clearance status of cyber professionals would aid in achieving that scenario. There are workforce management systems that inventory human capital using job codes and framework attributes, and they track professional development and other achievements. The Joint Cyber Command and Control Readiness (JCC2-R) is the reporting system for the joint cyber workforce, per TASKORD 23-0029. It tracks personnel training, mission qualifications, and other readiness data. The U.S. Coast Guard cyber training and qualification directive, Commandant Instruction 1500.2A, outlines training and other requirements for cyber-coded roles based on mission-essential task lists (METLs) to be recorded within JCC2-R.⁶²

A CCR talent management system could link information in these systems and bridge the lexicons of private-sector and government cyber roles, skill details, and qualification criteria, not only for resource identification in time of crisis, but also for broader skill gap analysis and career progression insights. A talent pipeline could be modeled by extracting and enumerating specific skillsets necessary for roles and for CCR candidates.

Existing recruitment initiatives and qualification vetting mechanisms can be tuned for CCR-specific goals. Drawing on lessons learned from traditional reserve structures and emerging state-level programs demonstrate that skilled talent is obtainable. A recruitment model informed by mission requirements that employs objective technical validation practices and strategies that target capable civilian participants is a good start. A pilot program would provide insight into interest and viability, as well as relative impact on other recruitment initiatives.

⁶² CYBER TRAINING AND QUALIFICATION, COMDTINST 1500.2A, July 2025, https://media.defense.gov/2025/Jul/07/2003748942/-1/-1/0/CI_1500_2A.PDF

8 Preventing Conflicts of Interest or Ethical Concerns

Section 1540(c)(8) asks for an analysis of methods for preventing conflicts of interest or other ethical concerns as a result of participation in a CCR program.

Reserve Component Mechanisms for Handling Conflicts of Interest

A CCR should adopt existing preventative methods from the uniformed reserve components. There is a robust set of laws, regulations, and guidelines for preventing conflicts of interest within the DOD RCs that could also be used for a CCR. The DOD Standards of Conduct Office (SOCO) has published guidelines for handling conflicts of interest within the RC in accordance with the DOD Joint Ethics Regulation (5500.07-R), Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635), and the Federal Acquisition Regulation (FAR).⁶³ These guidelines address a comprehensive set of topics including conflicts of financial interests, financial disclosure reports, outside (off-duty) employment and off-duty business enterprises, holding civil office while on reserve duty, supplementation of salary, post-government employment, and gifts.

According to DOD SOCO guidelines, commanders are prohibited from assigning reserve component service members to duties that could enable them to obtain non-public information, gain unfair advantages over competitors, or present an actual or apparent conflict of interest. To prevent conflicts of interest, commanders must screen service members to ensure that no real or apparent conflicts exist between service members' private interests and their assigned duties. Screening should include information about reservists' civilian jobs such as their employer, job title, and duties and responsibilities. It should also include information about any current or pending government contracts held by reservists' employers. Furthermore, the screening information should include whether reservists will be performing duties related to contractual actions.

In addition, the FAR prohibits contracting officers from knowingly awarding a government contract to a government employee or to a business concern or other organization owned or substantially owned or controlled by one or more government employees. The FAR exempts special government employees from this provision unless their duties directly affect the procurement. Many reserve component service members are considered special government employees, and therefore their civilian businesses could still be awarded government contracts so long as the service member was not in a position to influence the procurement.⁶⁴

DOD SOCO guidelines also deal with organizational conflict of interest and are in accordance with FAR subpart 9.5, *Organizational and Consultant Conflicts of Interest*. The guidelines state that reservists and contracting officials must be aware of potential organizational conflicts of interest that could exist due to reservists' civilian employment and that an organizational conflict of interest could disqualify reservists' employers from participating in procurement actions when reservists return to their civilian jobs after serving on active duty⁶⁵.

⁶³ CHAPTER K RESERVE COMPONENT ETHICS ISSUES, 14th Ethics Counselor Course Deskbook, October 2016, https://dodsoco.ogc.osd.mil/Portals/102/reserve_ethics.pdf

⁶⁴ Federal Acquisition Regulation 3.601(a) & (b), <https://www.acquisition.gov/far/3.601>

⁶⁵ Federal Acquisition Regulation 9.504(e), <https://www.acquisition.gov/far/9.504>

Finally, laws and regulations prohibit federal employees, including reserve component service members, from using nonpublic information to further their own private interests or those of another.⁶⁶ This includes information not releasable under the Freedom of Information Act (FOIA), information that is protected by the Privacy Act of 1974, classified information (18 U.S.C. § 798, 50 U.S.C. Code § 783(b)), and information protected by procurement integrity law (41 U.S.C. § 423), or the Trade Secrets Act (18 U.S.C. § 1905).

Financial Disclosure Requirements

The purpose of financial disclosure is to identify and mitigate potential financial conflicts of interest. The Reserve Component has two types of financial disclosure: the Public Financial Disclosure Report (OGE Form 278e) and the Confidential Financial Disclosure Report (OGE Form 450).

The Public Financial Disclosure Report is a detailed financial disclosure that includes information about assets held, income sources, and so on. This type of financial disclosure is reserved for senior government officials such as certain Senior Executive Service (SES) members and general officers in the military (O-7 and above). In addition, these financial disclosures are available to the public upon request. The Confidential Financial Disclosure Report (OGE Form 450) is a financial disclosure for federal employees in positions below the public disclosure level. DOD Joint Ethics Regulations (JER) 6-300 defines “covered positions” that subject to filing an OGE Form 450, which includes reserve officers. Reserve component services members on active duty for less than thirty consecutive days during a calendar year are exempted unless they are performing duties that impact the financial interests of non-federal entities (NFEs).

JER 6-300 defines various circumstances where reserve component service members could be subject to filing an OGE Form 450 including when their responsibilities require them to make decisions or judgements, without substantial supervision and review, that affect (1) contracting or procurement, (2) administering or monitoring of grants, subsidies, licenses, or other federally conferred financial or operational benefits, (3) regulating or auditing any non-federal entity, or (4) other activities in which the final decision or action will have a direct and substantial economic effect on the interests of any non-federal entity. While this requirement is specified in the Joint Ethics Regulations, it is applicable to all executive branch employees whose position is classified at GS-15 or below.⁶⁷ Additionally, DOD personnel—including reserve component service members—are subject to filing an OGE Form 450 if their supervisor determines that their duties and responsibilities require the form to avoid an actual or apparent conflict of interest (JER 6-300(a)(3)(b)). It is worth noting that the example used in the JER under this provision specifically calls out the RC, as follows:

A member of the Reserve Component who is expected to work less than 60 days during the year drills as a contract specialist for two weeks. Although they are not required to file a financial disclosure form as an SGE, they may be required to file because of their assigned duties.⁶⁸

⁶⁶ Code of Federal Regulations, 5 CFR § 2635.703(a), <https://www.ecfr.gov/current/title-5/chapter-XVI/subchapter-B/part-2635>

⁶⁷ Code of Federal Regulation, 2634.904 Confidential filer defined (a)(1)(i), Last amended 7/25/2025, <https://www.ecfr.gov/current/title-5/section-2634.904>

⁶⁸ DOD Joint Ethics Regulations, May 15, 2024, <https://dodsoco.ogc.osd.mil/Portals/102/Documents/Issuances/JER%20and%20Directives/JER%20May%2015%202024.pdf>

9 Resources Necessary for a CCR

Section 1540(c)(9) asks for resources, including funding levels, necessary to carry out a CCR program.

Full-Time Support Staff Models

This section provides a detailed analysis of the full-time support staff required for the CCR. The method relies on established models from the U.S. Army Reserve (AGR), the National Guard's Title 32 structure, and State Defense Force cybersecurity units. Calculations for a 200-member CCR using different staffing ratios, along with cost estimates and job descriptions, are included.

Army Reserve AGR Model

The U.S. Army Reserve relies on a group of Active Guard and Reserve (AGR) personnel who serve full time to oversee and train the predominantly part-time reserve force. AGR roles typically represent about 8 to 12 percent of the total reserve unit's staffing. This arrangement ensures continuous administrative oversight, training coordination, and readiness for mobilization while maintaining manageable costs.

National Guard Title 32 Model

The National Guard maintains a group of full-time personnel under Title 32 status to oversee training, readiness, and daily activities for the larger part-time force. These personnel include AGR soldiers, military technicians, and dual-status employees. Typically, full-time support staff make up about 12 to 15 percent of the overall National Guard force. For example, a state with 10,000 Guardsmen might employ between 1,200 and 1,500 full-time staff to support daily operations and training needs.

State Defense Force Model

Several states have established cyber units within their defense forces. These units typically have fewer than five full-time personnel who handle administrative tasks, manage training pipelines, protect state networks, coordinate with state and federal partners, and ensure operational continuity. This streamlined approach demonstrates that scaling administrative work based on the size of the force is achievable, but it also highlights the challenges of limited growth when relying on minimal full-time staff.

Coast Guard Auxiliary Model

The United States Coast Guard Auxiliary is a fully volunteer, uniformed division of the Coast Guard established in 1939 to support non-combat missions such as recreational boating safety, public education, and operational assistance. It has around 21,000 members nationwide, funded by an annual federal budget of approximately \$15 to 20 million, which accounts for a small part of the overall Coast Guard budget. Daily management and oversight are provided by fewer than 300 full-time, active-duty personnel and civilian staff, primarily through Directors of Auxiliary (DIRAUX) teams in each district. This structure demonstrates how modest federal funding can organize and maintain a large volunteer force. However, its dependence on personal motivation and donated time poses challenges in recruiting, retaining members, and providing specialized training.

Civil Air Patrol Model

The Civil Air Patrol (CAP) is the official civilian auxiliary of the U.S. Air Force and acts as both a federally chartered nonprofit organization and an Air Force auxiliary during missions. CAP has approximately 66,000

members, including adults and cadets, and operates more than 560 aircraft. It receives about \$250 to \$270 million annually in federal funding, which supports its various missions such as search and rescue, disaster relief, homeland security, aerospace education, and youth development. CAP depends on roughly 250 full-time staff members at its national headquarters and the Air Force liaison unit (CAP-USAF) to oversee programs and coordinate operations. This structure highlights the scalability and costs involved in maintaining a large national auxiliary and provides insight into how volunteer forces are sustained through strong federal support, dedicated infrastructure, and extensive training resources.

Comparison of Models

Three models are presented: Army Reserve AGR, National Guard Title 32, and State Defense Force. These serve as reference structures for determining the appropriate balance of full-time support staff for a CCR. The AGR model emphasizes efficiency with about 8–12 percent staffing, the Title 32 model highlights strong support at 12 to 15 percent, and the State Defense Force model demonstrates a minimal staff approach, with 3 to 5 percent staffing, often involving fewer than 5 full-time personnel. The Coast Guard Auxiliary and Civil Air Patrol are not included in this comparison because they mainly operate as volunteer organizations with minimal paid full-time support, which does not directly align with the administrative and staffing needs envisioned for a CCR. Additionally, auxiliary models are effective and appropriate when large numbers of civilians are available to complete relatively straightforward and well-defined missions. The cybersecurity workforce pipeline is already failing to meet growing demand, and missions in the cyber domain are complex and constantly changing. An auxiliary model could be considered in the future if these conditions change over time.

AGR Model: 200 Members (FTEs 8-12 Percent)

Applying the Army Reserve AGR model ratio of roughly 8 to 12 percent, a 200-member CCR would need about 16 to 24 full-time staff. This streamlined structure focuses on efficiency and cost control.

- full-time support staff required: approximately 16 full-time equivalents (FTEs)
- estimated annual rate per FTE: \$130,000–\$200,000
- total annual cost (16 FTEs): \$2.08M–\$3.2M

Title 32 Model: 200 Members (FTEs 12–15 Percent)

Applying the National Guard Title 32 ratio of 12 to 15 percent, a 200-member CCR would require 24 to 30 full-time staff. This more robust structure provides greater redundancy and oversight but at a higher cost.

- full-time support staff required: approximately 24 FTEs
- estimated annual rate per FTE: \$130,000 to \$200,000
- total annual cost (24 FTEs): \$3.12M to \$4.8M

State Defense Force Model: 200 Members (FTEs 3–5 Percent)

Applying the State Defense Force ratio of 3 to 5 percent, a 200-member CCR would require 6 to 10 full-time staff.

- full-time support staff required: approximately 6 FTEs
- estimated annual rate per FTE: \$125,000 to \$175,000
- total annual cost (6 FTEs): \$.75M to \$1.05M

Comparison of Support Staff Ratios

For convenience, Table 3 offers an overview of the comparisons outlined above.

Table 3: Comparison of support

Model	% Full-Time Staff	Full-Time Staff (200 Members)	Estimated Annual Cost
Army Reserve AGR	8 -12%	16 - 24 FTEs	\$2.08M - \$4.8M
National Guard Title 32	12 -15%	24 - 30 FTEs	\$3.12M - \$6.0M
State Defense Force Contractors	3 - 5%	6 - 10 FTEs	\$0.75M - \$1.75M

A CCR of 200 members can be managed effectively using either an AGR-style model with 16 full-time staff or a Title 32-style model. The AGR model prioritizes efficiency and lower costs, while the Title 32 model provides greater oversight and redundancy. The state defense force model indicates that a smaller, leaner staff is possible, though it might limit scalability. A hybrid approach could offer the optimal balance of cost, readiness, and administrative efficiency.

Staffing Breakdown and Functions

Effective management requires a balanced allocation of full-time staff across key functional areas. The staffing structure is designed to ensure that all critical activities, from administrative oversight to operational planning, are properly supported. Full-time staff handle managing personnel records, pay, and clearances; overseeing training and professional growth; coordinating cyber operations and incident response planning; managing logistics and resources; and ensuring compliance with legal, policy, and reporting standards. This organization provides the administrative foundation needed to support a part-time reserve force, maintain readiness, and enable quick mobilization when necessary.

Based on the Army Reserve AGR-style model, a CCR staffed with 16 FTEs can be effectively organized into five core functional areas.

- Administration and Personnel Records (4 FTEs): Responsible for personnel management, pay processing, records maintenance, and security clearance tracking to ensure members remain in good standing.
- Training and Professional Development Oversight (3 FTEs): Develops training schedules, coordinates virtual and in-person events, manages professional certification programs, and tracks member readiness.
- Operations and Incident Response Planning (4 FTEs): Provides operational planning, scenario development, and coordination for cyber incident response exercises and mobilizations.
- Logistics and Resource Management (3 FTEs): Manages travel coordination, equipment distribution, IT systems, and sustainment of facilities and infrastructure.
- Policy, Legal, and Compliance (2 FTEs): Ensures alignment with federal and state policies, enforces legal protections such as USERRA, prepares compliance reports, and supports program audits.

This staffing structure guarantees that the CCR has administrative support, training oversight, operational planning, logistical capacity, and policy compliance systems needed to maintain a 200-member reserve under the AGR model.

Additional Resource Requirements

Establishing and maintaining a CCR will require both physical and virtual infrastructure. Facilities should include office space for full-time personnel, meeting rooms for training and planning, and dedicated server rooms or access to secure cloud environments. Equipment will include secure laptops, mobile hotspots, software, and secure storage. Depending on the mission scope, members may need access to both unclassified and classified networks. Cyber ranges will be essential to support individual training, team exercises, and large-scale simulated incident response activities. These ranges could be hosted by the DOD, the DHS, or contracted providers.

Facilities

Estimated yearly costs for office space range from \$30 to \$50 per square foot, depending on the location. For an office supporting 16 full-time employees, around 10,000 square feet might be needed, leading to an annual facility expense of \$300,000 to \$500,000. Additional charges for security upgrades, utilities, and maintenance could add about \$100,000 per year.

- Basis: GSA Federal Real Property Council data and average office lease rates used for federal agencies
- Assumption: approximately 10,000 sq ft for 16 FTE full-time staff, including a mix of offices, secure meeting rooms, IT and server rooms, and classroom training space
- Cost range: \$30–\$50 per square foot annually → \$300K–\$500K
- Add-ons: \$100K for security retrofits (SCIF or controlled facilities), utilities, and ongoing maintenance

Equipment

Estimated equipment costs include the technology and tools needed for members to perform their duties securely and effectively. This covers laptops or other secure computing devices configured with the right software, virtual private network access, and cybersecurity tools. Members might also need mobile hotspots, secure storage, accessories, and licenses for collaboration software to support both virtual and in-person participation. Additionally, equipment costs include system upgrades, replacements on a regular cycle to maintain technical readiness, and ongoing IT support to ensure devices stay compliant with federal cybersecurity standards.

Equipment costs should cover start-up expenses and ongoing replacement costs. The following sections offer an updated breakdown for CCR equipment costs based on a four-year laptop replacement schedule.

Equipment Expenses (200 members + 16 FTE staff)

- Start-up costs (year 1)
 - Full-time staff (16 FTEs)
 - Secure laptops, mobile hotspots, software licenses, accessories.
 - Estimate: \$5,000 each × 16 = \$80,000.
 - Part-time members (200)
 - Secure laptop, VPN/token, baseline software, headset.
 - Estimate: \$2,500 each × 200 = \$500,000.
- Total start-up equipment cost (Year 1): = \$580,000

- Recurring costs (Years 2–4)
 - software licensing, VPN tokens, secure collaboration platforms, help desk ticketing, and skills database.
 - Estimate: $\$500 \text{ per member per year} \times 216 = \$108,000$ annually.
 - replacement and refresh reserve fund
 - Laptops are replaced every 4 years.
 - Annualized replacement cost = $(\text{Total laptop pool} \div 4 \text{ years})$.
 - Pool value = $\$580,000 \rightarrow \text{Annualized} = \$145,000$ per year.
- total recurring annual cost (Years 2–4): approximately \$253,000 annually
- Cost Profile Over 4 Years
 - year 1 (start-up): \$580,000
 - year 2: \$253,000
 - year 3: \$253,000
 - year 4: \$253,000
 - total (4 years): approximately \$1.34M
 - average annualized cost: approximately \$335,000 per year

Cyber Ranges and Training Platforms

Access to cyber ranges and training platforms is crucial for operational readiness. Contracted access may cost between \$2,000 and \$5,000 per participant annually. For 200 part-time members and 16 full-time staff, the yearly costs for range and training are estimated at \$400,000 to \$1.0M. Costs can be reduced by using existing DOD or DHS/CISA cyber range agreements.

Overhead

Overhead expenses include administrative, logistical, and support functions needed to keep members prepared and run the program smoothly. This covers costs related to managing personnel records, processing pay, and obtaining security clearances (if required). It also involves providing secure virtual collaboration tools and IT help desk support. Overhead also includes distributing basic apparel and identification items, such as polo shirts and ID cards. It involves supplying training materials, creating scenarios, and organizing events for the annual in-person training exercise. Additionally, overhead accounts for ongoing program management activities like scheduling, communication, and reporting, which help maintain continuity and accountability within the reserve.

Overhead expenses include the following:

- Uniform and apparel—polo shirts (2 per year), ID badge, lanyard
 - Estimate: approximately \$150 per member annually
- Administrative systems, including pay processing, personnel records, and security clearance renewals.
 - estimate: approximately \$750 per member annually.
- Virtual platform licensing and IT support – secure teleconferencing, collaboration tools, cyber range connectivity.
 - estimate: approximately \$1,000 per member annually.

- Annual training event logistics (non-travel)—event administration, printed materials, scenario preparation.
 - estimate: approximately \$300 per member annually.

Total overhead cost per member is approximately \$2,200 annually.

The annual overhead cost for 200 members is approximately \$440,000.

Organizational Options

Several organizational options are available for managing and supporting the CCR. Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) offer technical expertise, policy analysis, and independence in research, development, and training. National laboratories, such as those operated by the Department of Energy, along with intramural federal research institutes like the Naval Research Laboratory and Army Research Laboratory, also serve as models of government-supported technical capacity. Additionally, agency-sponsored Centers of Excellence can function as focal points for specialized research and education partnerships.

General Schedule (GS) civilians provide long-term federal employment stability and institutional knowledge within the CCR. At the same time, government contractors offer flexibility and surge capacity, allowing the CCR to quickly increase resources when needed.

Using a combination of federally funded research organizations for program design and implementation, GS civilians for ongoing support, and contractors for specialized or temporary assistance may be the most effective approach to setting up and maintaining the CCR.

Full-time support can be organized using three main workforce models, each providing unique benefits.

Personnel support costs are estimated through three primary models:

- Federally Funded Research Organizations (FFRO) include FFRDCs, National Labs, UARCs, Centers of Excellence (COE). FFROs provide specialized research, technical expertise, and training capacity under government-supported structures.
- GS civilians: Offer continuity, stability, and institutional knowledge through long-term federal employment.
- Government contractors: Deliver surge capacity, specialized skills, and flexible staffing that can be scaled rapidly to meet mission requirements.

Table 4 offers an overview of the costs for each of these models.

Table 4: Estimated personnel support cost

Workforce Type	Salary/ Direct Compensation	Overhead/ Benefits Factor	Total Cost to Gov (Annual)
Federally Funded Research Organizations (FFRDCs, National Labs, UARCs, COEs)	\$175K – \$225K	×1.6 – 1.8	\$280K – \$405K ⁶⁹

⁶⁹ GAO, *Oversight of Federally Funded Research Organizations* (GAO-21-510, 2021); DOE and DHS reports on National Labs and Centers of Excellence (contract structures generally billed at 1.6–1.8× direct compensation).

GS Civilians (GS-13 to GS-15)	\$113K – \$158K	+30 – 36%	\$150K – \$215K ⁷⁰
Government Contractors	\$125K – \$190K	×1.5 – 2.0	\$190K – \$380K ⁷¹

Summary of High-Level Costs

The CCR requires a mix of full-time staff and a larger part-time membership, with costs driven by the staffing model selected.

- AGR-style model (8 to 12 percent full-time): approximately 16 FTEs with estimated annual costs of \$2.4M on the low end of scaling to 6.48M.
- Title 32-style model (12 to 15 percent full-time): approximately 24 FTEs with estimated annual costs \$3.6M on the low end of scaling to \$9.72M.
- The State Defense Force model is too fragmented, under-resourced, and state-limited to serve as the foundation for a CCR. The CCR must be structured as a federally resourced, standardized, and scalable program to meet national cyber defense needs.

Table 5 provides an overview of the total annual costs for a 200-member CCR including personnel, facilities, equipment, training ranges, and overhead.

Table 5: Estimated annual cost for 200 members

Category	Low Estimate	High Estimate
Personnel (16 FTEs)	\$2,080,000	\$3,200,000
Personnel (200 Part-Time)	\$3,000,000	\$4,000,000
Facilities	\$300,000	\$600,000
Equipment (4 yr average)	\$335,000	\$600,000
Cyber Ranges/Training	\$400,000	\$1,000,000
Overhead	\$440,000	\$1,000,000
Cost Estimates	\$6,555,000	\$10,400,000

Establishing and Administering a CCR

A potential path to establishing a CCR is through a phased approach that leverages the strengths of different organizational models over time. It may be prudent to appoint an FFRO to support the standup of a CCR or assist with a pilot project. FFROs offer advanced technical expertise, policy knowledge, and program design skills, which are vital during the reserve's early development. FFRO's non-profit charters, independence, and ability to adopt best practices from government, academia, and industry make them well-suited to develop the governance structures, recruiting and assessment programs, and operational practices and standards necessary for success.

⁷⁰ U.S. Office of Personnel Management (OPM), *2025 GS Pay Tables*; Congressional Budget Office (CBO), *Federal vs. Private Sector Compensation* (benefits load ~30–36%).

⁷¹ U.S. Government Accountability Office (GAO), *Contractor Costs and Oversight* (GAO-21-236, 2021); RAND Corporation, *Contractor Support in the U.S. Department of Defense* (RR-870, 2015).

Once the CCR is established and operational procedures are in place, responsibility could shift GS civilian employees, who can provide continuity, institutional knowledge, and long-term program stability. GS personnel (with oversight from the uniformed chain of command) offer a sustainable and accountable federal workforce foundation, ensuring that the program remains aligned with federal standards and objectives.

By working with GS staff during the steady-state phase, contractors can provide flexibility, surge capacity, and specialized technical support. They offer scalability and can be quickly added to respond to emerging cyber threats, surge demands, or specialized training needs.

By adopting this notional phased model, FFROs can engage in design and launch, GS employees in institutionalization, and contractors in scaling. This method could enable quick implementation, cost-efficient operations, and long-term sustainability for the CCR.

10 Penalties for Non-Activation Response

Section 1540(c)(10) asks for an analysis of potential penalties or other adverse actions that might be taken against individuals who do not respond to activation when called.

CCR Disciplinary Measures

Because the CCR is designed to enhance national cyber defense on a voluntary and part-time basis, its enforcement mechanisms for non-response differ from those used in the DOD's traditional RCs. While military reservists may face administrative, financial, or even judicial consequences for failing to report, CCR members would be subject to a less severe set of accountability measures suitable for a civilian program.

Civil Air Patrol and Coast Guard Auxiliary members who fail to perform duties face the following administrative discipline: verbal or written reprimands, suspension from duties, removal of qualifications, and ultimately termination of membership. Neither organization has UCMJ authority; discipline is administrative and focused on maintaining mission readiness and professionalism.

The consequences for failing to respond to duty or activation for a CCR would highlight corrective measures, professional responsibility, and maintaining program continuity rather than punishment. Escalation would depend on the frequency of non-responses, the member's intent, and the effect on mission readiness.

Progressive Response Framework

The following list provides several options for corrective measures that could be taken by a CCR against its members if they fail to report for duty or activation. The measures are listed from least to most severe, and they could be applied in order depending on repeat offenses.

- Informal counseling and clarification—Initial outreach to identify reasons for non-response and reaffirm expectations.
- Formal written counseling—Issued as a documented notice if a pattern of unresponsiveness continues.
- Temporary suspension from activation pool—Members may be placed on hold from future taskings until their availability is clarified.
- Loss of priority consideration—Members who repeatedly fail to respond could lose eligibility for higher-visibility assignments, training opportunities, or leadership development within the CCR.
- Administrative removal from roster—Continued non-response may lead to removal from the CCR activation roster, with the option to reapply upon demonstrating renewed commitment.
- Referral to employer engagement office (if applicable)—If civilian job conflicts cause repeated non-responses, the program may collaborate with employer support resources to address barriers before considering separation.

Comparison to Traditional Reserve Components

Unlike traditional reservists in the Army, Navy, Air Force, Marine Corps, Coast Guard Reserve, or National Guard, CCR members would not face loss of military pay or retirement points, involuntary activation, nonjudicial punishment, or court-martial under the Uniform Code of Military Justice. The CCR discipline

framework is intentionally less restrictive, focusing on accountability through administrative and professional consequences rather than punitive actions.

Summary of Findings

The main question this study explores is whether it is feasible and advisable to establish a CCR for the DOD. Answering this question is complex due to competing stakeholder opinions and the large number of variables that must be understood and carefully weighed. The legislation directing this study includes a specific requirement that states, “The entity or center shall take into consideration the results of the evaluation of nontraditional cyber support to the Department of Defense required by section 1730 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).” In compliance with this requirement, the 1730 Report was carefully analyzed and compared with new data collected as part of this study. As such, that report’s “keep the status quo” conclusion is still a viable course of action for policy makers. However, research activities conducted to inform this study indicate that **establishing a CCR within DOD is feasible and advisable.**

A CCR within the DOD Is Feasible

- **There is a need:** As discussed in Section 1, there is a general shortage in the cybersecurity workforce at large and an acknowledged gap within the DOD cyber workforce. For example, in his May 2025 testimony before the House Armed Services Subcommittee on Cyber, Information Technologies, and Innovation, William Hartman, the Acting Commander of U.S. Cyber Command, stated that the United States cannot unilaterally match the quantity of resources that China can devote to cyber operations. Furthermore, he stated that “CISA, NSA, and FBI assess that PRC actors are positioning themselves within information technology networks, enabling lateral movement to OT systems—the hardware and software that control critical infrastructure.”⁷² A civilian cybersecurity reserve, along with other efforts underway such as CYBERCOM 2.0, and the Commission on U.S. Cyber Force Generation⁷³ could strengthen and bolster the DOD cyberspace workforce.
- **Distinct mission:** For a CCR to be viable, it needs to have a mission that distinguishes it from the RCs. Section 6 identifies two types of missions that would be well-suited for a CCR: sustainment missions and response missions. Sustainment missions provide value to the DOD and the nation through various support functions such as training, security assessments, and exercises. Response missions involve support for responding to cyber incidents and can leverage the expertise and specialized knowledge that exists outside of the DOD to enhance response outcomes.
- **Interest in serving:** The research into voluntary state-level cybersecurity response organizations and teams demonstrates that under the right conditions, a desire and propensity to serve the country exists. At the federal level, a propensity to serve is further illustrated by cyber auxiliary programs sponsored by the U.S. Marine Corps and the U.S. Coast Guard. More broadly, voluntary participation in non-cyber civilian auxiliaries such as the Civil Air Patrol and Coast Guard Auxiliary have been sufficiently

⁷² Cybersecurity and Infrastructure Security Agency (CISA), People's Republic of China Threat Overview and Advisories, <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

⁷³ CSIS, Commission on U.S. Cyber Force Generation, September 2025 <https://www.csis.org/programs/strategic-technologies-program/projects/commission-us-cyber-force-generation>

staffed with volunteers for decades. Furthermore, numerous former CMF members interviewed for this report expressed an interest in serving in a CCR.

A CCR in DOD is Advisable

- **New supply of talent:** The primary motivation for creating a CCR is to recruit and retain talented cyber professionals who would never choose to serve in uniform or work as a DOD civilian employee. This talent pool requires no costly initial training investment or lengthy military indoctrination. Qualitative evidence suggests that a properly designed CCR could offer civilians a way to serve the country in a manner that is mutually acceptable and beneficial. Additionally, direct interview feedback suggests that a CCR would attract former or retired DOD cyber operators who hung up their uniforms but still wish to serve under certain conditions.
- **Strategic reserve:** U.S. CI is highly vulnerable. If a war breaks out with China, disruptions to utilities and services will impact the DOD's ability to prosecute its mission. Interviewed senior USG and DOD leaders assert that the lack of a strategic cyber reserve presents unacceptable risk to the country, and they feel this should be remedied. A CCR could benefit the DOD in peacetime, but more importantly, it would provide a well-organized and prepared homeland defense capability if war comes.
- **Perceived value:** 82 percent of DOD personnel surveyed for this report agree that there is value in establishing a CCR. Additionally, 83 percent agree that a CCR would "bring skills and capabilities that are in high demand in the DOD."

Findings and Suggestions

Address Cyber Workforce Gaps

The preponderance of evidence from data collected during this study suggests that considerable capacity and capability gaps exist in the DOD's cyber workforce. Some of these gaps can be addressed with new or streamlined force generation approaches or organizational models. A September 2025 GAO report supports this finding and recommends consolidation of DOD cyberspace training courses and cybersecurity service providers.⁷⁴ However, even if efficiencies are found in current force generation methods, the report also notes that a 16 percent job vacancy rate exists for USCC-aligned DOD organizations. Moreover, the rapid pace of change in cyber and expected disruptive influence of AI leaves the DOD and the USG at a strategic disadvantage. As mentioned previously, the PLA outnumbers the DOD by a factor of 10 in cyber and its support of many affiliated APTs (e.g., Volt Typhoon) present significant risk to U.S. national security. A properly designed and implemented CCR could address staffing gaps and reduce risk.

Unlike USG auxiliaries like CAP and CGA, a CCR must prioritize recruiting expert cyber talent over amassing thousands of members. Setting a high bar for CCR member selection and acceptance criteria is essential. A CCR made up of elite cyber professionals can build credibility and trust in USG and DOD stakeholders. As mentioned in Section 7 of this report, a CCR personnel database is critical for surgically matching talent with specific mission requirements. Hence, this system should store granular skills data for all CCR members, thereby creating an easily searchable rolodex for mission owners. These skills should be confirmed using rigorous hands-on assessments as part of the recruiting and selection process. Finally, ensuring that a CCR is

⁷⁴ GAO DOD CYBERSPACE OPERATIONS, <https://files.gao.gov/reports/GAO-25-107121/index.html>

organized and equipped to fill USG capability gaps and take on advanced or emerging DOD cyber challenges will enhance its value to the nation.

Challenge the Status Quo

As stated above, CCR membership should prioritize top-tier cyberspace expertise. Obviously, former CMF team members who are not willing to join the RC are ideal candidates. While pursuing patriots with PhDs in AI and data science is advisable, such pedigree should not preclude the potential acceptance of accomplished black hat and Def Con researchers with high school diplomas. Also, recruiting CCR members with expertise in adjacent fields could have a force multiplying effect. For example, it may be invaluable to retain master software engineers, mathematicians, and tech savvy CI engineers and operators. Furthermore, the CCR culture should be merit based and accepting of 65-year-old NSA retirees and 20-something-year-old, capture-the-flag competition finalists. Lastly, to garner and retain top-talent, CCR leadership should seek flexibility regarding virtual assemblies and voluntary, short duration activations.

Collaborate with the USG Interagency

As noted earlier, the U.S. homeland is vulnerable to potentially devastating cyber attacks from nation-state adversaries and well-organized criminal elements. Combating this strategic risk requires a proactive, whole-of-government approach. On Aug 2, 2025, Sean Cairncross (the U.S. National Cyber Director) stated in his confirmation hearing that “The United States must dominate the cyber domain through strong collaboration across departments and agencies, as well as private industry.” Accordingly, a CCR should play a part in this national effort. CCR members can bring unique skills and insights to the DOD and the interagency and provide forums, training, red teaming, exercise support, and specialized incident-response capabilities where they are needed. A CCR, like any elite organization, must rehearse and perform its missions regularly to maintain its edge. Therefore, CCR participation in exercises like Cyber Shield⁷⁵ are recommended.

Conduct a CCR Pilot Project

It is recommended that the DOD plan and execute a small-scale pilot to further evaluate the CCR concept. This pilot could follow a phased approach and start with the creation of a detailed written plan for the pilot project itself and the development of a CCR concept of operations. Key elements of the pilot include determining the necessary legal and contractual requirements; developing recruitment, assessment, and selection criteria and methodologies; designing and developing talent management processes and system prototypes; defining the CCR’s initial mission set and organization structure; and so on. Once all the design and planning phases are completed, the pilot project would proceed into the execution and evaluation phase. This phase could include the trial recruitment and processing of a small cohort of 15 to 20 candidates. The pilot should also include the collection and analysis of relevant, evaluative cost and benefit metrics for each phase of the project. Oversight and management of the pilot would be most efficient if maintained at a relatively high level in the DOD hierarchy rather than assigning it to operational units in the services or at USCC.

Conclusion

This report concludes that it is feasible and advisable to establish a CCR within the DOD under certain conditions. It is important to stipulate that this conclusion is primarily derived using qualitative analysis techniques. The statistical results of survey data stem from amalgamated feedback of individuals responding to

⁷⁵ Hircock, Samantha, Staff Sgt., Cyber Shield June 2025, https://www.army.mil/article/286378/cyber_shield_2025

statements presented using a five-point Likert scale. These data are useful for assessing subjective characteristics, such as feelings, attitudes, or perceptions, and while statistically relevant, they can be distorted by various biases.

Furthermore, the scope of this study was limited in large part to the 10 elements defined in Section 1540(c). As such, a minimum of time was invested in the creation and comparison of specific CCR implementation scenarios. The notional CCR model described in Section 5 of this report was conceived mainly for the purpose of estimating financial costs of member compensation and benefits and other administrative matters. It is recommended that further analysis be conducted to determine optimum CCR implementation courses of action. This could be incorporated into a follow-on pilot project as desired.

List of Acronyms

Acronym	Description
1540	Section 1540 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263)
1730 Report	<i>Evaluation of Reserve Models Tailored to the Support of Cyberspace Operations</i>
AC	active component
ACI	Army Cyber Institute
ACI Report	<i>Practical Challenges in Implementing a Civilian Cyber Reserve by the Army Cyber Institute</i>
AF	Air Force
AGR	Active Guard and Reserve
AI	Artificial intelligence
AT	annual training
CAC	Common Access Card
CAE	Centers of Academic Excellence
CAP	Civil Air Patrol
CCR	Civilian Cybersecurity Reserve
CEH	Certified Ethical Hacker
CGA	Coast Guard Auxiliary
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CISSP	Certified Information Systems Security Professional
CITEP	Cyber Information Technology Exchange Program
CMF	Cyber Mission Force
CMT	Combat Mission Teams
COF	Cyberspace Operations Forces
CPB	Cyber Protection Brigade
CPT	Cyber Protection Teams
CST	Combat Support Teams

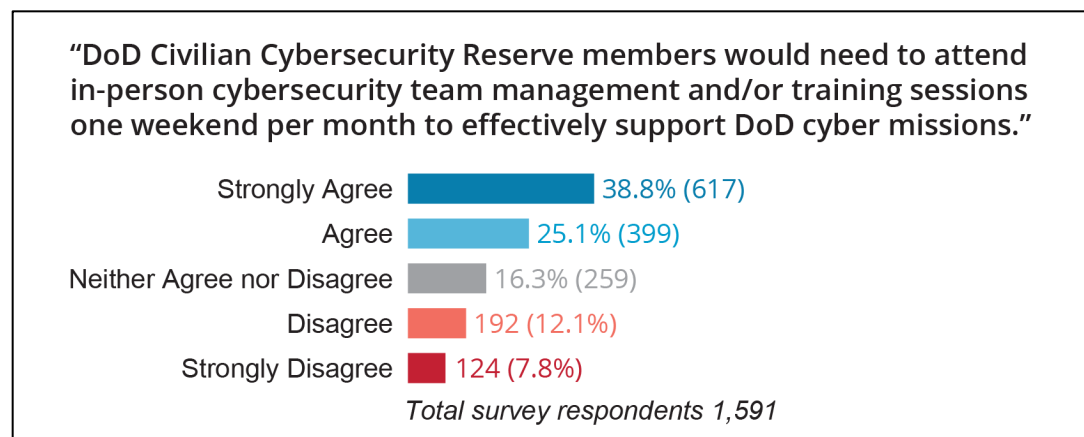
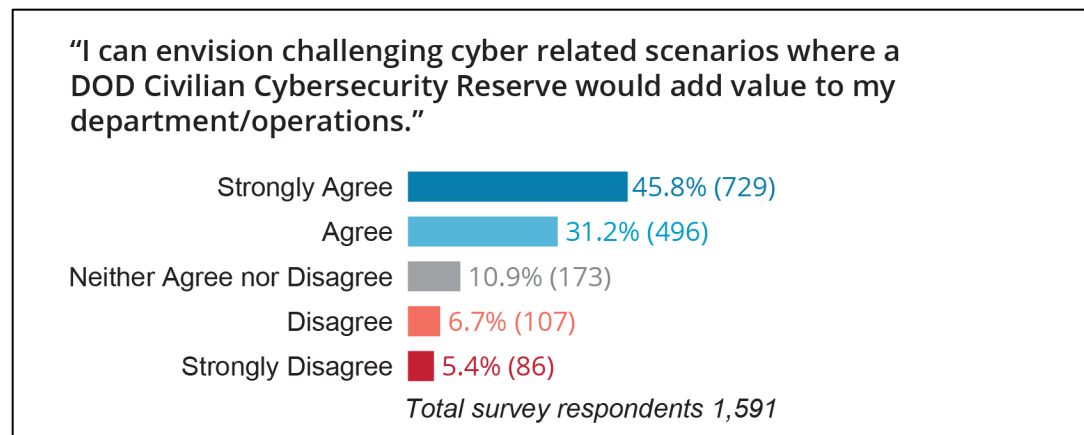
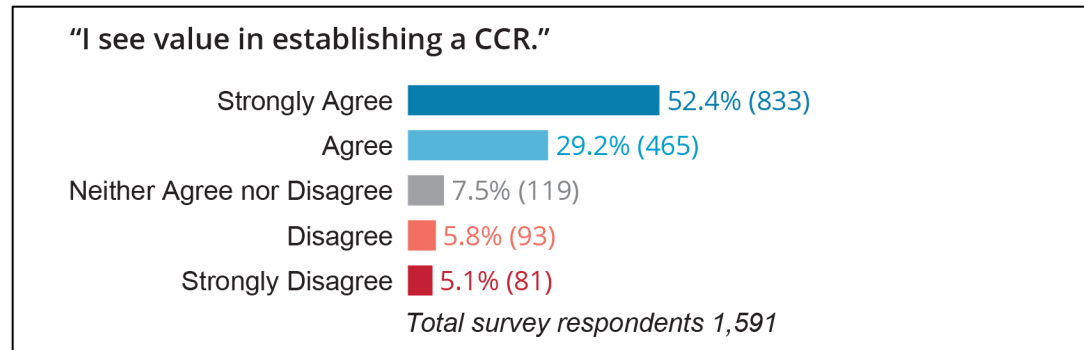
CWMB	Defense Cyber Workforce Management Board
DAF	Department of the Air Force
DCSA	Defense Counterintelligence and Security Agency
DCWF	Defense Cyber Workforce Framework
DevSecOps	development security operations
DHS	Department of Homeland Security
DIRAUX	Directors of Auxiliary
DOD	U. S. Department of Defense
DOJ	U.S. Department of Justice
DSCA	Defense Security Cooperation Agency
DSPS	Defense Support to the Private Sector
ESAD	Emergency State Active Duty
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FFRO	Federally Funded Research Organization
FTEs	full-time equivalents
GS	General Schedule
GSA	General Services Administration
IDT	inactive duty training
IMA	individual mobilization augmentee
ION	interactive on-net
ISACs	Information Sharing and Analysis Centers
ISC2	International Information System Security Certification Consortium
IT	Information Technology
JCC2-R	Joint Cyber Command and Control – Readiness
JCT&CS	DOD’s Joint Cyber Training and Certification Standards
JER	Joint Ethics Regulations
KSAT	Knowledge, Skills, Abilities, Tasks from DCWF
MGIB-SR	Montgomery GI Bill Selected Reserve
MiC3	Michigan Cyber Civilian Corps

METLs	mission essential task lists
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Science and Technology
NMT	National Mission Teams
NSA	National Security Agency
OGE	Office of Government Ethics
OT	Operational technology
OUSDP	Office of the Under Secretary of Defense for Policy
PLA	China's Peoples Liberation Army
RC	reserve component
SEI	Software Engineering Institute
SES	Senior Executive Service
SFS	Scholarship for Service
SJA	staff judge advocate
SOCO	Standards of Conduct Office
TS/SCI security clearances	Top Security / Sensitive Compartmented Information security clearances
U.S.	United States
USAF	U.S. Air Force
USAR	U.S. Army Reserve
USBLS	U.S. Bureau of Labor of Statistics
USCC	U.S. Cyber Command
USERRA	Uniformed Services Employment and Reemployment Rights Act
USG	United States Government
VoLAC	Volunteer Access Card

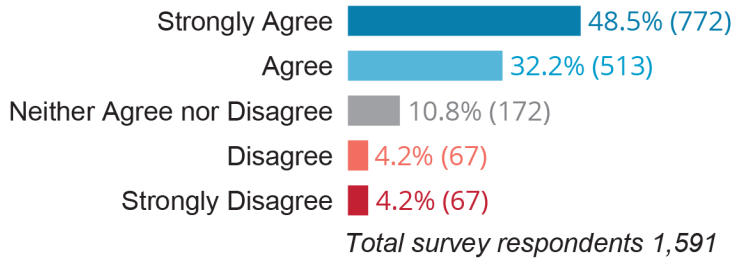
Appendix A: Compiled Survey Results

SURVEY QUESTION	STRONGLY DISAGREE	SOMEWHAT DISAGREE	NEITHER AGREE NOR DISAGREE	SOMEWHAT AGREE	STRONGLY AGREE
Given intent, I see value in establishing a CCR.	81 (5.1%)	93 (5.8%)	119 (7.5%)	465 (29.2%)	833 (52.4%)
I can envision challenging cyber related scenarios where DOD Civilian Cybersecurity Reserve would add value to my department/operations.	86 (5.4%)	107 (6.7%)	173 (10.9%)	496 (31.2%)	729 (45.8%)
DoD Civilian Cybersecurity Reserve members would need to attend <u>in-person</u> cybersecurity team management and/or training sessions one weekend per month to effectively support DoD cyber missions.	124 (7.8%)	192 (12.1%)	259 (16.3%)	399 (25.1%)	617 (38.8%)
DoD Civilian Cybersecurity Reserve members could participate in monthly <u>virtual</u> cybersecurity team management and training sessions to successfully integrate DoD cyber operations/missions.	67 (4.2%)	67 (4.2%)	172 (10.8%)	513 (32.2%)	772 (48.5%)
The DOD is the right US department to put a Civilian Cybersecurity Reserve corps.	104 (6.5%)	130 (8.2%)	239 (15.0%)	386 (24.3%)	732 (46.0%)
A Civilian Cybersecurity Reserve would be more effective within a federal agency like CISA.	112 (7.0%)	211 (13.3%)	578 (36.3%)	421 (26.5%)	269 (16.9%)
Logistical issues like maintaining access to DoD facilities and networks would inhibit CCR operations.	64 (4.0%)	185 (11.6%)	306 (19.2%)	638 (40.1%)	398 (25.0%)
It would be feasible to integrate members of a DoD Civilian Cybersecurity Reserve into military cyber operations on a temporary basis.	92 (5.8%)	161 (10.1%)	247 (15.5%)	649 (40.8%)	442 (27.8%)
Existing uniformed reserve and national guard cyber talent/manpower precludes the necessity for a DoD Civilian Cybersecurity Reserve.	260 (16.3%)	526 (33.1%)	440 (27.7%)	234 (14.7%)	131 (8.2%)
A college degree in a STEM field is necessary to qualify for a Civilian Cybersecurity Reserve.	357 (22.4%)	433 (27.2%)	276 (17.3%)	306 (19.2%)	219 (13.8%)
A DoD Civilian Cybersecurity Reserve would impede other DoD recruitment and retention efforts.	299 (18.8%)	492 (30.9%)	520 (32.7%)	188 (11.8%)	92 (5.8%)
A DoD Civilian Cybersecurity Reserve will cause conflict and/or morale problems within the existing DoD civilian workforce.	342 (21.5%)	442 (27.8%)	468 (29.4%)	242 (15.2%)	97 (6.1%)
A DoD Civilian Cybersecurity Reserve will cause conflict and/or morale problems within the existing DoD uniformed reserves and national guard.	310 (19.5%)	427 (26.8%)	519 (32.6%)	238 (15.0%)	97 (6.1%)
DoD Civilian Cybersecurity Reserve members must hold security clearances to add value to DoD's cyber mission.	31 (1.9%)	29 (1.8%)	130 (8.2%)	385 (24.2%)	1016 (63.9%)
DoD Civilian Cybersecurity Reserve members would bring skills and capabilities that are in high demand in DoD.	34 (2.1%)	49 (3.1%)	183 (11.5%)	459 (28.8%)	866 (54.4%)

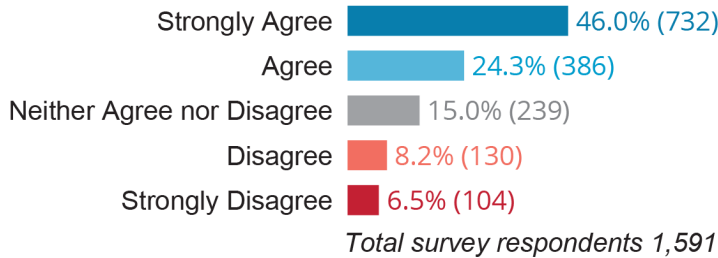
Each chart represents the proportional distribution of responses to the 15 survey questions listed in the table above. Charts are displayed according to the question sequence in the survey.



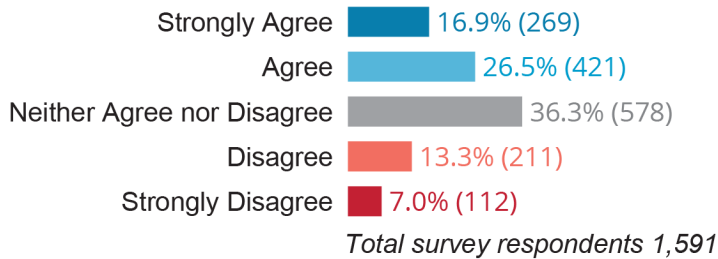
“CCR members could assemble virtually to effectively support DoD missions.”



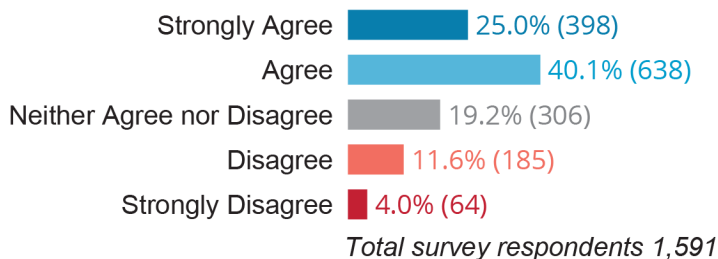
“DOD is the right department for a CCR.”



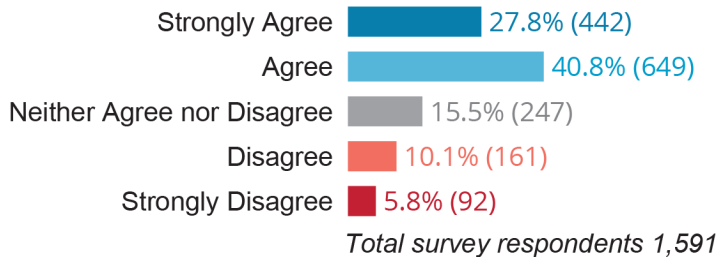
“A Civilian Cybersecurity Reserve would be more effective within a federal agency like CISA.”



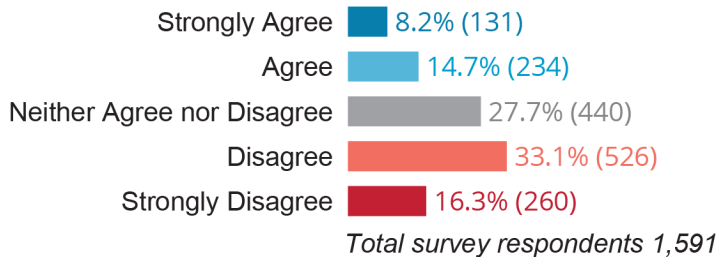
“Logistical issues like maintaining access to DoD facilities and networks would inhibit CCR operations.”



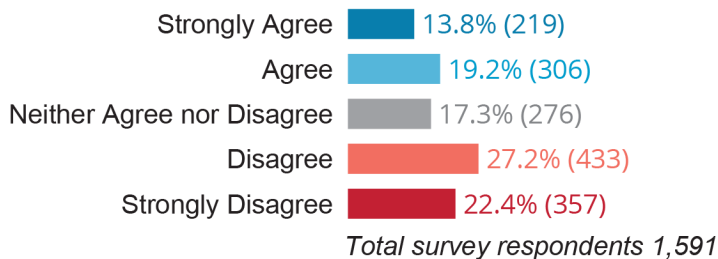
“It would be feasible to integrate members of a DoD Civilian Cybersecurity Reserve into military cyber operations on a temporary basis.”



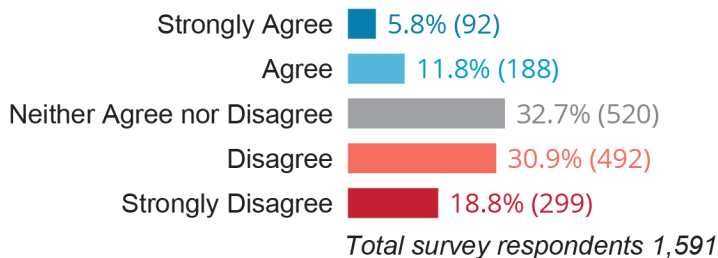
“Existing uniformed reserve and national guard cyber talent/manpower precludes the necessity for a DoD Civilian Cybersecurity Reserve.”



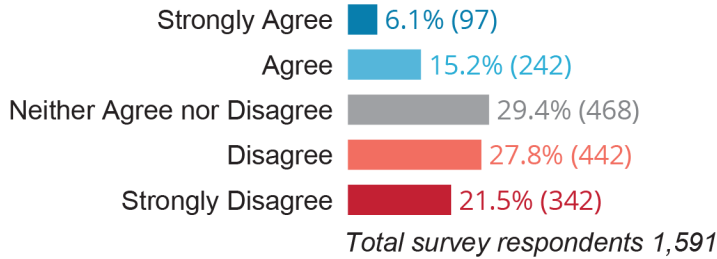
“A college degree in a STEM field is necessary to qualify for a Civilian Cybersecurity Reserve.”



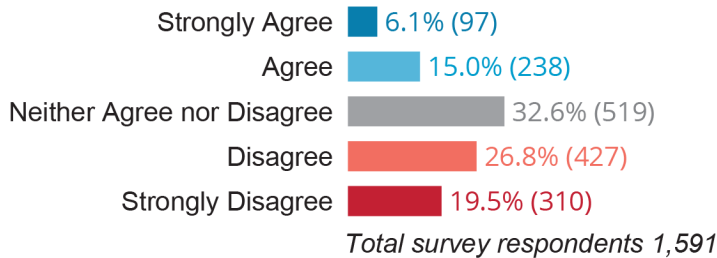
“DoD CCR would impede other recruitment and retention efforts.”



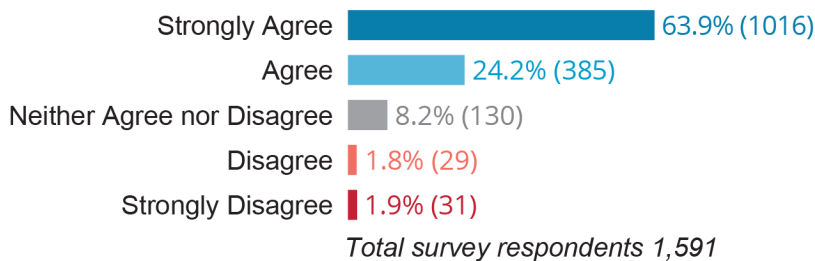
“A DoD Civilian Cybersecurity Reserve will cause conflict and/or morale problems within the existing DoD civilian workforce.”



“A DoD Civilian Cybersecurity Reserve will cause conflict and/or morale problems within the existing DoD uniformed reserves and national guard.”



“CCR members must hold security clearances to add value to DoD cyber missions.”



“DoD CCR members would bring skills and capabilities that are in high demand.”

