United States Government Accountability Office

Report to Congressional Committees

May 2024

CYBER PERSONNEL

Navy Needs to Address Accuracy of Workforce Data

Accessible Version

GAO-24-106879

GAO Highlights

View GAO-24-106879. For more information, contact Joe Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.
Highlights of GAO-24-106879, a report to congressional committees
May 2024

CYBER PERSONNEL

Navy Needs to Address Accuracy of Workforce Data

Why GAO Did This Study

State actors and affiliated hacker groups continue to increase their attacks against U.S. targets. It is vital that DOD's cyber workforce respond to such threats and defeat them. The NDAA for Fiscal Year 2020 required the Navy to study civilian and military cyber career paths. In response, studies were completed in October 2021 and April 2022.

The NDAA for Fiscal Year 2023 required the Navy to report on the extent to which it had implemented study recommendations. It also includes a provision for GAO to assess the extent to which the Navy has implemented the recommendations. GAO's report examines the extent to which the Navy has (1) implemented the recommendations in Navy-sponsored studies, (2) addressed continuing data and training challenges in strengthening its cyber workforce, and (3) established a framework for implementing cyber workforce initiatives.

GAO reviewed Navy reports, interviewed officials, and reviewed relevant documentation such as personnel data, DOD cyber workforce policies and strategies, and a recent Navy instruction.

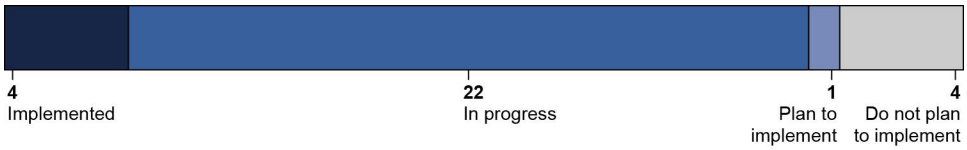
What GAO Recommends

GAO continues to maintain that DOD should fully implement the 2019 priority recommendation to review work roles and position descriptions for accuracy (*see* GAO-23-106305).

What GAO Found

In response to a National Defense Authorization Act (NDAA) mandate, the Center for Naval Analyses issued studies on civilian and military cyber career paths in October 2021 and April 2022, respectively. The two studies made a total of 31 recommendations. GAO determined that 26 of the 31 recommendations have been implemented or are in the process of being implemented.

Implementation Status of Recommendations from Studies on Navy Civilian and Military Service Member Cyber Career Paths as of March 2024



Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

The Navy faces continuing challenges with data as it works to strengthen its cyber workforce. GAO attempted to determine the structure and composition of the Navy's military and civilian workforce but found that the underlying data were unreliable. For example, Navy officials stated that the Navy's civilian cyber workforce data are stored in two different data systems, and the data in both systems differ. This has caused civilian workforce data to show inaccurately high vacancy rates, among other things. Officials said they are in the process of reconciling the data in the systems and addressing accuracy challenges. GAO previously reported in 2019 on similar accuracy issues related to data on Department of Defense (DOD) cyber work roles and position descriptions. GAO recommended that DOD review work roles and position descriptions for accuracy. DOD concurred with this priority recommendation and has taken steps but has not fully implemented it.

The Navy also faces challenges with scheduling cyber training. For example, the National Security Agency and outside vendors administer training for many of the cyber work roles, but accessing this training is dependent on class availability via these external sources, according to Navy documentation and interviews with officials. As a result, the Navy cannot ensure that sailors' training can be scheduled in an appropriate sequential order and without gaps. Navy officials cite this as a primary challenge. In response, U.S. Cyber Command officials stated they are working with the military services to move responsibility for administration of certain cyber training to the services.

The Navy's framework for implementing cyber workforce initiatives includes participating in DOD-wide planning activities, implementing efforts identified in the Navy's cyber strategy, and establishing policy and a governance body. DOD and the Department of the Navy established cyber strategies that outline initiatives intended to improve cyber workforce management. The DOD Cyber Workforce Strategy 2023-2027 and its accompanying implementation plan establish a unified, department-wide direction for managing the cyber workforce. The Department of the Navy issued its own cyber strategy in November 2023, which includes a workforce line of effort aligning with the DOD strategy and plan.

Contents

Abbreviations

CES	Cyber Excepted Service
CIO	Chief Information Officer
CMF	Cyber Mission Force
CNA	Center for Naval Analyses
CWMB	Cyber Workforce Management Board
CYBERCOM	U.S. Cyber Command
DCPDS	Defense Civilian Personnel Data System
DCWF	DOD Cyberspace Workforce Framework
DOD	Department of Defense
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
OCHR	Office of Civilian Human Resources

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 13, 2024

Congressional Committees

State actors and affiliated hacker groups continue to increase their cyberattacks against the federal government and private industry, with new threats and attacks against U.S. infrastructure emerging daily. It is critical that the Navy, like the rest of the Department of Defense (DOD), have a cyber workforce ready to respond to such attacks and be capable of defeating them. In 2019, the Navy completed a comprehensive review following several cyber incidents involving compromises of classified and sensitive information.[1]

The Navy's review, along with other reports, identified several issues related to the Navy's cyber workforce.[2] Subsequently, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 directed the Navy to conduct a study on improving career paths for civilian and military cyber personnel.[3] The Navy asked the Center for Naval Analyses (CNA) to study these issues. CNA issued studies on civilian and military cyber career paths in October 2021 and April 2022, respectively, and made a total of 31 recommendations.[4] In August 2023, the Navy submitted a report to Congress on the implementation status of the civilian recommendations.[5]

Section 1536 of the James M. Inhofe NDAA for Fiscal Year 2023 includes a provision for us to assess the extent to which the Navy has

[1]Secretary of the Navy, *Cybersecurity Readiness Review* (Mar. 4, 2019).

[2]Bedding, Katherine, and Marijke de Jongh. "Federal Workforce: Attracting and Retaining Talent in the Field of Cybersecurity." *Cornell Institute for Public Affairs,* May 2017.

[3]Pub. L. No. 116-92, § 1653 (2019). The National Defense Authorization Act for Fiscal Year 2020 directed the Secretary of the Navy and the Chief of Naval Operations to conduct the study within the Navy. The subsequent studies did not include the Marine Corps.

[4]Center for Naval Analyses, *Navy Civilian Cyber Career Paths: Issues and Recommendations* (October 2021); Center for Naval Analyses, *Navy Military Cyber Career Paths: Issues and Recommendations* (April 2022).

[5]Office of the DCNO for Information Warfare, *Report to Congress, FY23 NDAA Section 1536 Recommendations from Navy Civilian Career Path Study* (Washington, D.C.: June 14, 2023).

implemented recommendations from the studies on civilian and military career paths, and review additional recommended actions to improve the readiness and retention of the cyber workforce of the Navy.[6] This report examines the extent to which the Navy has (1) implemented recommendations in Navy-sponsored studies on improving cyber career paths, (2) addressed continuing data and training challenges in strengthening its cyber workforce, and (3) established a framework for implementing cyber workforce initiatives.

For the first objective, we reviewed documentation and interviewed officials regarding the implementation status of CNA's recommendations. With this information an analyst assessed the status of each recommendation using the following scale: implemented; in progress; not implemented–plans to implement; and not implemented–does not plan to implement.[7] A second analyst reviewed the evidence and the first analyst's determinations and provided comments or concurrence. If the two analysts did not agree, a third analyst adjudicated. For the second objective, we used the information collected on the status of the recommendations to identify areas of challenge and interviewed officials about efforts to address these areas. For the third objective, we reviewed relevant documentation, such as recent DOD and Navy strategies and instructions, and interviewed DOD and Navy officials about their plans, policies, and methods for carrying out their cyber workforce programs and initiatives. For a detailed description of our scope and methodology, see appendix I.

We conducted this performance audit from June 2023 to May 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]Pub. L. No. 117-263, § 1536 (2022). Section 1536 required the Navy to submit a report on the recommendations, with GAO's review to follow.

[7]The Navy did not prepare a report to Congress on the status of CNA's recommendations to improve military career paths, which it stated it was not required to do. However, we reviewed documentation and interviewed officials to assess the status of these recommendations.

Background

Cyber Workforce and Entities with Key Roles and Responsibilities

DOD defines its cyberspace workforce as those personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. The cyberspace workforce is comprised of five elements: Information Technology (Cyberspace); Cybersecurity; Cyberspace Effects; Intelligence (Cyberspace); and Cyberspace Enablers.[8] Various officials and offices have roles and responsibilities related to DOD and the Navy's cyber workforces, as discussed below.

- The **DOD Chief Information Officer (CIO)** is to oversee the management of the Information Technology (Cyberspace); Cybersecurity; and Cyberspace Enablers workforce elements of the DOD cyberspace workforce. The DOD CIO also provides oversight of the DOD Cyber Workforce Implementation Plan execution and reporting requirements.[9]
- The **Under Secretary of Defense for Personnel and Readiness** is responsible for establishing policy guidance to support military cyberspace training requirements, among other things. Further, the office of the Under Secretary of Defense for Personnel and Readiness is responsible for providing the DOD components with systems to collect required cyberspace workforce personnel data, as well as developing and collecting data elements not currently collected in other authoritative personnel systems.
- The **Principal Cyber Advisor** maintains authority, direction, and control with respect to the administration and support of U.S. Cyber Command, including for readiness and organization of cyber operations forces. The Principal Cyber Advisor also ensures overall integration of cyber operations forces activities relating to cyberspace

[8]Department of Defense Directive 8140.01, *Cyberspace Workforce Management* (Oct. 5, 2020).

[9]In March 2023, DOD published the *2023-2027 Cyber Workforce Strategy*. In July 2023, DOD published the *2023-2027 Cyber Workforce Strategy Implementation Plan,* which serves as DOD's roadmap to achieve the strategy's goals and objectives for cyber workforce management.

operations, including associated policy and operational considerations, resources, personnel, technology development and transition, and acquisition.

- The **Cyber Workforce Management Board (CWMB)** is DOD's principal governance body to manage the health, welfare, and maturity of DOD's military and civilian cyber workforce. The CWMB is responsible for managing the DOD Cyberspace Workforce Framework and, according to officials, is tri-chaired by the DOD CIO, Under Secretary of Defense for Personnel and Readiness, and Principal Cyber Advisor.[10]
- The **Commander, U.S. Cyber Command (CYBERCOM)** is responsible for coordinating across DOD on qualification standards for all cyberspace operational work roles. CYBERCOM also develops and maintains guidance necessary to provide, train, and operate DOD cyber operations forces, among other things.[11]
- DOD component heads, including the **Secretaries of the military departments**, are responsible for implementing cyberspace workforce management programs.[12] These component heads are also responsible for 1) identifying positions and personnel required to perform cyber work roles in authoritative personnel systems and 2) implementing component-specific cyber work role training, qualification, and standards for the component cyber workforce. The DOD components, including the military departments, use the DOD

[10]The DOD Cyberspace Workforce Framework (DCWF) describes the work performed by the full spectrum of the cyber workforce and includes 72 work roles that are based on the work an individual performs, rather than their position title or career field. Each work role includes a representative list of tasks and knowledge, skills, and abilities describing what is needed to execute key functions. The DCWF is intended to facilitate uniform identification, tracking, and reporting; develop qualification requirements for cyber work roles; and support DOD-wide workforce management and planning activities. DOD Instruction 8140.02. According to DOD, the DCWF leverages the National Initiative for Cybersecurity Education (NICE) Cybersecurity Framework and DOD Joint Cyberspace Training and Certification Standards.

[11]DOD cyber operations forces include the Cyber Mission Force, U.S. Cyber Command subordinate command elements, DOD Component Network Operations Centers and Cyber Security Service Providers, special capability providers, and specially designated units. Cyber operations forces do not include business function elements; service-retained forces; Joint Cyber Centers; Intelligence units and personnel; and Commander, U.S. Special Operations Command-assigned forces. *See* DOD Directive 8140.01.

[12]DOD components are organizational entities within the department, including the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the defense agencies, and the DOD field activities.

Cyberspace Workforce Framework as the authoritative reference for identifying, tracking, and reporting on cyberspace positions.

- The **Department of the Navy Principal Cyber Advisor** is responsible for implementing the DOD Cyber Strategy within the Navy and Marine Corps by coordinating and overseeing the execution of the services' policies and programs relevant to the recruitment, resourcing, and training of military cyberspace operations forces; assessment of these forces against standardized readiness metrics; and maintenance of these forces at standardized readiness levels.
- The **Department of the Navy CIO** is to oversee the Navy's cyber workforce program, set related standards and policy, and represent the Navy at the CWMB.
- The Navy and Marine Corps **Cyber Workforce Management Oversight and Compliance Council** is a board co-chaired by representatives from the Navy and Marine Corps providing a collaborative forum for addressing key cyber workforce management, training, and development issues.
- The **Navy Cyber Workforce Program Office**, within the Office of the Deputy Chief of Naval Operations for Information Warfare, is the office of primary responsibility for the Navy cyber workforce program. The office is responsible for developing the Navy's cyber workforce policy and guidance, subject to approval of the Department of the Navy CIO.
- **Navy Cyber Workforce Program Managers** are responsible for the administration and management of the Navy's cyber workforce program at each Department of the Navy organization. Program managers are responsible for reporting, database management, and overall effectiveness of the cyber workforce program at commands and/or subordinate units. The functions of the Cyber Workforce Program Manager may be performed by more than one individual, and individuals must be military or government civilian personnel.

DOD Cyber Workforce Policies and Strategy

Since 2020, DOD has issued several policies and a strategy aimed at improving the identification, recruitment, development, retention, and management of the cyber workforce (see table 1).

Table 1: Department of Defense Cyber Workforce-Related Policies and Strategies Issued Since 2020

Document name	Date	Description
DOD Directive 8140.01, Cyberspace Workforce Management	10/5/2020	Establishes a definition for the cyber workforce, introduces the DOD Cyberspace Workforce Framework (DCWF) as an authoritative reference, and outlines component roles and responsibilities for the management of the DOD cyber workforce.[a]
DOD Instruction 8140.02, Identification, Tracking, and Reporting of Cyberspace Workforce Requirements	12/21/2021	Outlines the identification, tracking, and reporting of the cyber workforce in accordance with the DCWF, enabling enterprise strategic workforce planning efforts.
DOD Manual 8140.03, Cyberspace Workforce Qualification and Management Program	2/15/2023	Establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements.
DOD Cyber Workforce Strategy 2023-2027	3/9/2023	Establishes a unified direction for DOD cyber workforce management using four human capital pillars: Identification, Recruitment, Development, and Retention.
DOD Cyber Workforce Strategy Implementation Plan 2023-2027	8/3/2023	Supplements the Cyber Workforce Strategy to serve as a roadmap for the department to achieve its higher-level goals.

Source: Department of Defense (DOD). | GAO-24-106879

[a]The DOD Cyberspace Workforce Framework describes the work performed by the full spectrum of the cyber workforce using work roles based on the work an individual performs, as opposed to the individual's position title or career field. Each work role includes a representative list of tasks and knowledge, skills, and abilities describing what is needed to execute key functions.

GAO Related Work on DOD's Cyber Workforce

In 1997 we designated information security as a government-wide high-risk area. Subsequently, in 2003 we expanded this high-risk area to include protecting cyber critical infrastructure. Cybersecurity remained a designated government-wide high-risk area in our 2023 biennial report.[13] In the 2023 report, we found that federal agencies continued to face challenges addressing needs related to their cyber workforce and reiterated the need to address such challenges.

We have also identified challenges specific to DOD's cyber workforce. In 2019, we reported on DOD's use of work role codes found in the National Initiative for Cybersecurity Education (NICE) framework to categorize

[13]GAO's High-Risk Series identifies and recommends actions to help resolve serious weaknesses in areas that involve substantial resources and provide critical services to the public. GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

cybersecurity positions.[14] We recommended, among other things, that DOD review and assess the NICE framework work role codes and position descriptions for accuracy. DOD concurred with the recommendation and in September 2020, stated that it had taken steps to decrease the number of positions that were assigned inappropriate codes. DOD further stated that it would continue to monitor and track coding with the aim of addressing the recommendation by September 2022. As of March 2024, according to the DOD CIO, the department had a coding remediation initiative underway. The CIO added that coding of cyber positions would evolve over time to keep pace with changes to mission, the addition or deletion of positions, and advances in cyber technology. We are continuing to monitor DOD's efforts to address this recommendation and have designated it as a priority recommendation.[15]

In 2019, we also reported on DOD's current and planned state of cyber training for its Cyber Mission Force (CMF).[16] We examined the extent to which DOD had developed a trained CMF, made plans to maintain a trained CMF, and leveraged other cyber experience to meet training requirements for CMF personnel. In total, we made eight recommendations, including that the military services develop CMF training plans with specific personnel requirements and that CYBERCOM establish the training tasks covered by foundational training courses and convey them to the services. DOD concurred with these recommendations and implemented all of them.

[14]GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

[15]Priority open recommendations are the GAO recommendations that warrant priority attention from heads of key departments or agencies because their implementation could save large amounts of money; improve congressional and/or executive branch decision-making on major issues; eliminate mismanagement, fraud, and abuse; or ensure that programs comply with laws and funds are legally spent, among other benefits. For our latest priority recommendation report sent to DOD, see: GAO, *Priority Open Recommendations: Department of Defense*, GAO-23-106305 (Washington, D.C.: May 16, 2023, reissued with revisions on June 8, 2023).

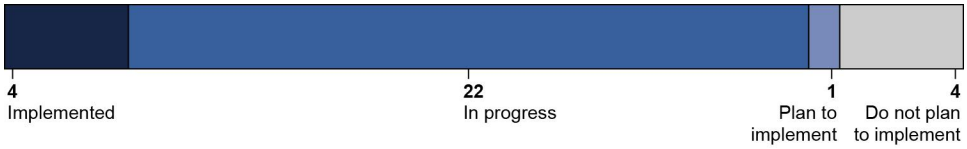
[16]GAO, *DOD Training, U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, D.C.: Mar. 6, 2019). The Cyber Mission Force comprises cyber mission teams made up of service members with advanced cyber training who play a critical role in executing cyber missions.

In 2022, we reported on retention challenges and service obligations for active-duty cyber personnel.[17] We made six recommendations, including that the Army and Marine Corps update or develop guidance to clearly define active-duty service obligations for advanced cyber training. We also recommended that the Army, Marine Corps, and Air Force track cyber personnel data by work role. DOD concurred with these recommendations. Three of these recommendations have been implemented, and we continue to monitor the status of the remaining three related to tracking data by work role.

The Navy Has Taken Steps to Implement Most Recommendations to Improve Cyber Career Paths

The Navy has implemented or is in the process of implementing 26 of the 31 recommendations from the Center for Naval Analyses (CNA) studies to improve civilian and military cyber career paths (see fig. 1).[18]

Figure 1: Implementation Status of Recommendations from Studies on Navy Civilian and Military Service Member Cyber Career Paths as of March 2024



Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

Recommendations implemented. We determined that the Navy has implemented four recommendations related to developing a strategy, career paths, and retention (see table 2).

[17]GAO, *Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking*, GAO-23-105423 (Washington, D.C.: Dec. 21, 2022).

[18]In the Navy's Report to Congress, it stated that out of the 19 civilian recommendations, the Navy had implemented one, begun to implement 13, had not implemented but planned to implement one, and did not plan to implement four. CNA's civilian study identified Congress as being responsible for implementing three recommendations, DOD responsible for four, and the Navy responsible for 12. The Navy did not report on the status of the military recommendations, which it stated it was not required to do, and CNA did not designate entities other than the Navy as responsible.

Table 2: GAO's Assessment of the CNA Recommendations to Improve Cyber Career Paths the Navy Has Implemented

	Recommendation (civilian or military)	Navy action(s) to implement recommendation
Strategy	Develop a comprehensive Navy cyber strategy with sufficient detail to create a subsequent Navy cyber workforce strategy (military)	The Department of the Navy issued the Navy Cyber Strategy in November 2023, which includes a line of effort to improve and support the cyber workforce. This line of effort includes goals to improve recruitment and retention, workforce management, talent development, and cybersecurity awareness. According to a senior Navy official, the Navy does not plan to produce a cyber workforce strategy and instead plans to align itself with the goals and objectives outlined in the Department of Defense's Cyber Workforce Strategy Implementation Plan 2023-2027—a department-wide plan for managing and advancing the cyber workforce.[a]
Career paths	Consider developing a specialist cyber career path for officers (military)	The Navy established the Maritime Cyber Warfare Officer designator in June 2023. According to Navy officials, there will be around 100 transfers from other designators throughout fiscal year 2024. New accessions will also begin in fiscal year 2024.
Retention	Identify critical civilian cyber positions (civilian)	The Navy identified seven critical cyber work roles in the mission areas of cyber operations forces, acquisitions, and information technology networks. According to Navy officials, the Navy faces the greatest skill shortages in these work roles in terms of staffing and competency levels. The Navy plans to focus its recruiting, rewarding, and retention efforts on these work roles.
	Consider conducting an in-depth retention study for the Cryptologic Technician – Networks rating (military)[b]	The Navy analyzes retention and how it applies incentives quarterly, by rating and skillset. According to Navy officials, the last review increased all Cyber Warfare Technician reenlistment bonuses (the Navy renamed the Cryptologic Technician-Networks rating as the Cyber Warfare Technician rating). These actions address the sub-element of the CNA recommendation to target incentives to the Navy Enlisted Classification.

Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

[a]Department of Defense, *Cyber Workforce Strategy Implementation Plan 2023-2027* (August 3, 2023).

[b]Navy ratings are enlisted occupations that consist of specific skills and abilities. The Cryptologic Technician–Networks rating (now renamed the Cyber Warfare Technician rating) is one of the primary ratings used for sailors performing cyber-related work.

Recommendations in progress. We determined that the Navy has taken some actions to begin implementing 22 of the civilian and military recommendations. Many of these recommendations, and the actions to address them, are related to the DOD Cyber Workforce Strategy Implementation Plan—a department-wide plan for managing and advancing the cyber workforce.[19] The plan involves developing action plans for each initiative to achieve targets by fiscal year 2027.

Table 3 shows the 14 civilian career path-, retention-, training and education-, and data collection-related recommendations that we

[19]Department of Defense, *Cyber Workforce Strategy Implementation Plan 2023-2027* (August 3, 2023).

determined are in progress based on our assessment and information that the Navy provided in its report to Congress.

Table 3: GAO's Assessment of CNA Recommendations to Improve Civilian Cyber Career Paths that the Navy Has in Progress

	Recommendation	Description of Navy actions and related DOD initiatives
Career path	Expand scholarship program use	According to the Navy's report to Congress on the status of civilian recommendations (the Navy report), the Navy does not have service-specific scholarships and instead participates in federal or Department of Defense (DOD) scholarship programs. The DOD Cyber Workforce Strategy Implementation Plan (DOD Plan) has an initiative related to this recommendation for which Navy is an office of coordinating responsibility: increase return on investment of scholarship programs. Through this initiative, DOD plans to identify metrics, track them, then use the findings to guide enhancements to scholarship programs by fiscal year 2027.
	Establish candidate inventories for positions likely to come open	In January 2024, the Office of Personnel Management launched a feature referred to as "Candidate Inventory" that allows hiring managers direct access to search for candidates who have already applied to jobs within their agency without the need to undergo a new recruitment. According to Navy officials, the feature is currently limited to use within a single organization. For example, the officials said Navy can use the feature within Navy but cannot use DOD-wide inventories. However, officials stated DOD's Defense Civilian Personnel Advisory Service is coordinating with DOD components, including the Navy, and the Office of Personnel Management to allow for cross-component inventories. Furthermore, the Navy Cyber Workforce Program Office is working with Navy offices that participated in pilots of the feature to receive demonstrations and learn how to effectively employ it, according to officials from that office.
	Expand the Cyber Excepted Service (CES)[a]	The Navy is a stakeholder in DOD's Cyber Workforce Management Board, the decision-making body for expanding the CES. During the board's September 2023 meeting, the board added three new work roles that qualify for the CES, according to DOD officials. The DOD Plan has an objective related to this recommendation: expand CES authorities to optimize program capabilities and increase attractiveness for talent. Through this objective, DOD plans to enhance CES flexibilities and incentives beyond existing levels and develop shared products and tools to standardize CES processes by fiscal year 2027.
	Review DOD Cyberspace Workforce Framework (DCWF) work role codes periodically	The Navy is a stakeholder in DOD's Cyber Workforce Management Board, the decision-making body for reviewing and approving proposed DCWF work roles. The board added new and modified existing work roles during one of its quarterly meetings in September 2023. In addition, the DOD Plan has an initiative related to this recommendation for which the Navy is an office of coordinating responsibility. Specifically, the DOD plan is to use standardized processes to identify workforce requirements based on the DCWF work roles by fiscal year 2027.
Retention	Increase use of pay flexibilities	Navy commands have access to pay flexibilities and recruitment, relocation, retention, and student loan repayment incentives, according to the Navy's report. However, exercising these flexibilities depends on a command's priorities and available funding. According to the report, the Navy plans to add more work roles to the CES. The report stated that additional work roles will address this recommendation by providing greater flexibilities and options for recruiting and retaining cyber professionals. As described above, DOD's Cyber Workforce Management Board is the decision-making body for adding more work roles to the CES. Further, the DOD Plan has an objective related to this recommendation, which is to expand CES authorities to optimize program capabilities and increase attractiveness for talent. Through this objective, DOD plans to enhance CES flexibilities and incentives beyond existing levels and develop shared products and tools to standardize CES processes by fiscal year 2027.

	Recommendation	Description of Navy actions and related DOD initiatives
	Ensure full use of CES flexibilities	The Navy established a CES Program Office under Fleet Forces Command responsible for implementing the CES personnel system in the Navy. According to officials, Fleet Forces Command holds biweekly meetings with commands to ensure human resources professionals have access to information, resources, and incentives. The Navy has also partnered with the Office of Civilian Human Resources to create a CES incentive fact sheet, which is available online. The DOD Plan has an initiative related to this recommendation: standardize CES core processes across the department to optimize delivery of human resources services. Through this initiative, DOD plans to develop shared products and standardized tools, such as training for human resources professionals, to simplify CES processes by fiscal year 2027.
	Collect data on incentive pay	According to the Navy's report, the Navy and the Office of Civilian Human Resources currently track incentive payments but do not analyze those payments against decisions of cyber workforce personnel who have left the Navy. However, Navy officials told us that the Navy's standardized civilian exit survey, created in October 2023, provides departing civilians the option to say whether a monetary incentive would have encouraged them to stay. The Navy's report stated that the DOD Plan contains several initiatives related to data analytics that will support Navy's implementation of this recommendation. For example, one such initiative in the DOD Plan is to integrate cyber workforce data into enterprise-wide systems by fiscal year 2027.
	Offer a broader range of nontraditional benefits	According to the Navy's report, the Navy offers a broad range of non-monetary or non-traditional benefits, such as access to health and fitness facilities (where available), transportation subsidies, alternative work schedules, telework options, and paid parental leave, among others. However, if an individual qualifies for any of these benefits, exercising them depends on command priorities and funding (when funding is involved). The DOD Plan has two initiatives related to this recommendation for which the Navy is an office of coordinating responsibility: (1) identify unique telework challenges to the cyber workforce and identify mitigation strategies by fiscal year 2027, and (2) establish supplemental training for supervisors to effectively manage the cyber workforce and periodically evaluate remote and telework delivery performance. The DOD Plan has a target to increase the percentage of the cyber workforce that is remote work eligible by 1 percent beginning in fiscal year 2026.
	Increase formal training opportunities	According to CNA's study, gaps remain in training for cyber civilians. Nevertheless, the Navy has made some progress on improving training opportunities, such as developing a plan with the Marine Corps to provide civilians access to online training, according to Navy officials. Additionally, according to officials from the Navy's Cyber Workforce Program Office, they coordinated with Defense Acquisition University to grant the cyber workforce access to the university's learning platforms. Navy officials stated that the Navy is reestablishing the cyber workforce management, oversight, and compliance council in the third quarter of fiscal year 2024 to manage cyber workforce training and advocate for more training options.
Training and education	Provide personnel management training to cyber managers	According to the Navy's report, the Navy uses the CES DOD Leaders Orientation Course to provide training to cyber managers on the CES personnel system. In addition, the DOD Plan has an initiative related to this recommendation for which the Navy is an office of coordinating responsibility: develop specialized training for hiring managers to better understand available hiring authorities and know how to appropriately apply authorities by fiscal year 2027.

	Recommendation	Description of Navy actions and related DOD initiatives
	Make cyber career information more accessible	The Navy's Cyber Workforce Program Office continues to develop a partnership with the Office of Civilian Human Resources (OCHR), according to Navy officials. The offices meet monthly to develop and distribute hiring information to aid human resources professionals, according to the officials. Further, these officials said they have provided hiring and incentive fact sheets. For example, the Navy released a cyber human resources guide in February 2024. Officials stated they will continue partnering with OCHR to determine how best to ensure commands have the information they need on hiring authorities.
	Establish system-wide skill requirement monitoring and planning	According to the Navy's report, the Navy is in the process of implementing this recommendation by updating the workforce management database that tracks training and proficiency levels. The updates help the Navy comply with DOD policy requirements related to tracking proficiency levels of the cyber workforce. The report states that the Navy also purchased a cloud-based learning management system that it is evaluating for Navy-wide adoption. The learning management system would document, track, and report learner progress. The Navy's goal is to include all Department of the Navy civilians in this system by the end of fiscal year 2025.
	Develop external training partnerships	The Navy's report states that civilians are eligible to attend National Defense University's cyber courses. Officials from the Cyber Workforce Program Office stated they worked with the Defense Acquisition University to give the civilian cyber workforce access to the university's learning platforms. In addition, the DOD Plan has three initiatives related to this recommendation. The Navy is an office of coordinating responsibility for two of these initiatives: (1) ensure National Centers for Academic Excellence in Cybersecurity curriculum aligns with department-wide cyber standards; and (2) increase return on investment of scholarship programs and effectively track participation to customize recruitment and outreach efforts by fiscal year 2027.[b]
Data collection	Develop enhanced data gathering capabilities	According to the Navy's report, the Navy is improving data gathering capabilities by coding all cyber positions and configuring their data systems to meet the requirements specified in the DOD Cyberspace Workforce Framework. Further, meeting these requirements enables tracking of the workforce, force quality, proficiency, and experience. The Navy faces challenges with some cyber workforce data and is taking action to correct and validate them. In addition, the DOD Plan has an initiative related to this recommendation for which the Navy is an office of coordinating responsibility: implement a data maturity plan by fiscal year 2027 to drive the DOD toward department-wide cyber workforce analytics. According to the DOD Plan, this is intended to enable data-driven talent management of critical skillsets.

Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

[a]The Cyber Excepted Service is a mission-focused personnel system for Department of Defense civilian cyber employees who support the U.S. Cyber Command to facilitate the recruitment, retention, and development of highly skilled personnel.

[b]The third initiative in the DOD Plan related to this recommendation, for which the Navy is not an office of coordinating responsibility, is to establish a centralized program office to manage cyber-focused student and employee developmental programs across the department.

Table 4 shows the eight military career path-, training and education, and data collection-related recommendations that we determined are in progress.

Table 4: GAO's Assessment of CNA Recommendations to Improve Military Service Members Cyber Career Paths That the Navy Has in Progress

	Recommendation	Description of Navy Actions
Career path	Establish cyber proficiency levels and assessments	U.S. Cyber Command (CYBERCOM) officials stated that the Department of Defense (DOD) Joint Cyberspace Training and Certification Standards define proficiency levels for service members, including sailors, in the Cyber Mission Force. Additionally, DOD Manual 8140.03 defines proficiency levels for all DOD Cyberspace Workforce Framework work roles. Though these proficiency levels are defined, the Navy has not yet completed coding them. The Navy expects to complete coding proficiency levels by May 2024.
	Consider developing technical career tracks	The Navy developed a "Career-Long Learning Continuum" for the new cyber enlisted rating, according to Navy officials, which is an effort to capture technical, professional, and leadership training; and applicable qualifications, certifications, and skillsets for each rating. The Navy expects to complete this effort by the end of fiscal year 2024, according to the officials. This will meet the aspect of this Center for Naval Analyses recommendation that "at a minimum, the Navy should clearly define standards of continuing training and education."
	Consider expanding the Cyber Warrant Officer field	The Navy considered expanding the Cyber Warrant Officer field when creating the new cyber officer designator and plans to evaluate it again in fiscal year 2025, according to Navy officials.
Training and education	Increase training opportunities for cyber sailors, such as training in the flow of work/microlearning, off-the-shelf training, and refresher training	The Navy has several initiatives under development to improve training and address training gaps, such as the Career Long Learning Continuum, which is intended to develop courses of action by the end of fiscal year 2024 according to Navy officials.
	Increase currency and relevance of Navy cyber training	Navy officials stated they are working to improve the relevance of training content, including to improve unit level training through the assessment of training gaps by the end of fiscal year 2024.
	Improve officer training for cyber	According to cyber community managers, the Navy is currently piloting two different training tracks with specialized cyber training to determine the best training route for cyber officers. The community managers stated they will make a final decision based on student performance after new accessions complete these training tracks in fiscal year 2024.
	Address issues with training not controlled by the Navy	The Navy continues to advocate for more control over cyber training and recently has taken over foundational training for some work roles, according to Navy officials. DOD is conducting a study to evaluate service responsibilities for organizing, training, and assigning personnel to the Cyber Mission Force, in response to a requirement in section 1533 of the National Defense Authorization Act for Fiscal Year 2023. DOD is required to complete this study no later than June 1, 2024, and is also required to establish a revised total force generation model for the Cyberspace Operations Forces by December 31, 2024.
Data collection	Improve collection of cyber training data	CYBERCOM officials stated they have an action plan to support the services' migration to the Joint Cyber Command and Control Readiness system. This system, operational since July 2023, captures training data, including National Security Agency courses, according to Navy and CYBERCOM officials. CYBERCOM officials stated they are working to connect external vendor training records to the system, and they expect to complete changes to the system by November 2024.

Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

Recommendations not implemented. The Navy has not implemented five CNA recommendations related to career paths, retention, and data issues (see table 5). The Navy concurred with one of these recommendations and plans to implement it over the next year as it accumulates additional data. The Navy did not concur with the other four recommendations and does not plan to implement them. The Navy's position on these recommendations is that the current conditions or processes are sufficient for addressing the underlying issues, as explained in the table.

Table 5: GAO's Assessment of CNA Recommendations to Improve Cyber Career Paths the Navy Has Not Implemented

	Recommendation (civilian or military)	Navy's rationale for not implementing or implementing later
Career paths	Analyze career paths in 2-3 years with better data (military)	The Navy concurred with this recommendation and plans to implement it when more data are available. Specifically, the recommendation requires time to accumulate data and evaluate trends with respect to newly created Navy Enlisted Classifications that identify skills and qualifications. Navy officials stated they continue to adjust Navy Enlisted Classifications for the new enlisted cyber rating to reflect U.S. Cyber Command training standards, and they will continue to evaluate data throughout 2024 to inform the maturation of the new cyber rating. In addition to Navy Enlisted Classifications, Navy continues coding for the Department of Defense (DOD) Cyberspace Workforce Framework, its authoritative reference for identifying and managing the cyber workforce, which also includes skill and qualification information and could be another analysis tool.
	Increase junior-level hiring (civilian)	The Navy did not concur with this recommendation and does not plan to implement it. According to the Navy's report to Congress, commands tend to hire mid-level rather than junior-level civilian employees, because they already have the skills the command requires. Furthermore, officials stated that hiring managers are averse to hiring civilian employees at the junior-level because (1) such hires require clearance adjudication, (2) the Navy struggles to compete with private sector entry-level salaries, and (3) junior employees, once trained, tend to leave for higher paying jobs in industry. CNA officials stated that other recommendations the Navy is in the process of implementing, such as expanding the Cyber Excepted Service, may in part address the intent of this recommendation.[a]
	Create more senior-level positions, including technical positions (civilian)	The Navy did not concur with this recommendation and does not plan to implement it. The Navy's report stated that the Navy's civilian cyber workforce is concentrated at the mid-level based on technical skill requirements. According to Navy officials, the creation of more senior-level positions must be made at the command-level based on the commander's needs and mission requirements. Navy officials at headquarters levels stated that they were not aware of any demand for more senior positions from commanders. CNA officials stated that other recommendations the Navy is in the process of implementing, such as expanding the Cyber Excepted Service, may in part address the intent of this recommendation.
Retention	Study effects of pay caps on retention, and if warranted, petition for raising pay caps for senior-level employees (civilian)	The Navy did not concur with this recommendation and does not plan to implement it. The Navy's report stated that current pay flexibilities are sufficient for retaining senior talent; therefore, studying, and potentially raising pay caps, is not necessary. Officials from the office of the DOD Chief Information Officer concurred with Navy's position, noting that they are not aware of any issues with the current pay cap for senior-level employees and stated that DOD Chief Information Officer is prepared to petition to raise the pay caps if necessary.

	Recommendation (civilian or military)	Navy's rationale for not implementing or implementing later
Data issues	Increase use of the Intergovernmental Personnel Act[b] for database support (civilian)	The Navy did not concur with this recommendation and does not plan to implement it. According to Navy officials, personnel serving under Intergovernmental Personnel Act authorities serve on 2-year assignments (with the possibility of extending assignments for another 2 years). Officials stated this assignment length is not ideal for the creation and long-term maintenance of data management systems. Instead, the Navy plans to continue using contractors for database support.

Source: GAO analysis of U.S. Navy and Center for Naval Analyses (CNA) information. | GAO-24-106879

[a]Cyber Excepted Service is a mission-focused personnel system for DOD civilian cyber employees who support the U.S. Cyber Command to facilitate the recruitment, retention, and development of highly skilled personnel.

[b]The Intergovernmental Personnel Act Mobility Program regulations provide for the temporary assignment of personnel between the federal government and state, local, and Indian tribal governments; institutions of higher education; and other eligible organizations.

The Navy Is Working to Address Continuing Challenges with Data and Training to Help Strengthen Its Cyber Workforce

The Navy Faces Challenges with the Reliability of Its Cyber Workforce Data

The Navy faces challenges with the reliability of its cyber workforce data, which it is working to address. These challenges include mismatches between data systems, data inaccurately showing multiple personnel assigned to the same billet, and ongoing revisions to DCWF work roles.

CNA Recommendations Related to Data

The CNA studies on civilian and military cyber personnel career paths made multiple recommendations related to cyber workforce data issues. For example, the studies recommended the Navy

- identify critical civilian cyber positions,
- review DOD Cyberspace Workforce Framework work role codes periodically,
- collect data on incentive pay,
- establish system-wide skill requirement monitoring and planning,
- develop enhanced data gathering capabilities, and
- improve collection of cyber training data.

Source: GAO analysis of Center for Naval Analyses (CNA) information (text); littlewolf1989/stock.adobe.com (image). | GAO-24-106879

The Navy faces challenges with mismatches between data systems and data inaccurately showing assignment of multiple personnel assigned to the same billet. These two issues cause data to show inaccurately high vacancy rates. Navy officials stated that civilian data that describe positions are stored in a different data system than civilian data describing the individuals filling those positions, and the two systems currently do not correspond.[20] Specifically, the DCWF work role codes and proficiency levels in the Total Force Manpower Management System, the Navy's database that describes positions, do not match the personnel assigned to them in the Defense Civilian Personnel Data System (DCPDS). Officials also reported instances of multiple personnel assigned to a single position in the database, which the Navy is working to correct.

The Navy has developed two different ways to update the civilian data in DCPDS, according to Navy officials. First, the Cyber Workforce Program Office and the Office of Civilian Human Resources have developed a form for cyber program managers and human resources officers to use to

[20]For personnel management purposes, the Navy uses the term "manpower" to denote requirements, billets, or spaces and "personnel" to denote people or individuals staffed to positions. The Navy's manpower database is the Total Force Manpower Management System. The Navy's civilian personnel database is the Defense Civilian Personnel Data System.

update DCPDS, according to these officials. Second, the Navy developed a reconciliation dashboard, which is intended to help users identify where the Total Force Manpower Management System does not match DCPDS. According to the officials, the Office of the Assistant Secretary of the Navy for Manpower and Reserve Affairs is offering training to help users understand how to use the dashboard.

In December 2022, the DOD CIO directed the military services to remediate all civilian cyber workforce data by March 2023.[21] The Navy requested three extensions—to March 2024—to complete remediation, which they did not meet, according to Navy officials. Officials stated the office of the DOD CIO approved another extension to April 2024. Further, individual Navy offices with cyber personnel are currently reconciling the mismatches in the data systems for their personnel.

Navy officials stated that they do not have the same challenges matching different databases for military cyber workforce data because there is a single database for positions and the personnel filling them. However, these officials stated that they also plan to conduct a validation of the military data even though they do not have obvious errors.

According to officials in the Navy's Cyber Workforce Program Office, correcting and validating data is their number one priority. According to officials from the office of the DOD CIO, the Navy has been actively partnering with them to address DCWF data issues. Further, DOD CIO officials noted that these data issues are not unique to the Navy; each military service is validating and correcting its cyber workforce data.

In addition to the issues above, DOD continues to revise and validate DCWF work roles, which will require the services to consistently update coding for both civilian and military personnel. The Cyber Workforce Management Board, DOD's decision-making body for the cyber workforce, regularly adds and modifies existing cyber work roles during its DCWF refresh process. In its September 2023 quarterly meeting, the board added four new work roles to the DCWF's Cyber Effects category and modified six work roles in the same category. These changes better align the work roles CYBERCOM uses with the DCWF work roles.

[21]Department of Defense Chief Information Officer Memorandum, *Remediation of Cyber Workforce Civilian Manpower and Personnel Data* (Dec. 21, 2022).

In addition to continuing updates to the DCWF, both we and the DOD Inspector General have found issues with the completeness of DCWF coding for civilians across the department. As previously mentioned, in 2019, we recommended that DOD take steps to review the assignment of certain work role codes to any positions in the department within the 2210 Information Technology Management civilian occupational series and assign the appropriate work role codes as well as assess the accuracy of position descriptions.[22] DOD concurred with this recommendation. As of March 2024, according to the DOD CIO, the department had a coding remediation initiative underway and the coding of cyber positions would evolve over time to keep pace with changes to mission, the addition or deletion of positions, and advances in cyber technology. We are continuing to monitor DOD's efforts to address this recommendation and have designated it as a priority recommendation.[23]

Furthermore, in 2021 the DOD Inspector General recommended that the DOD CIO require DOD components to code filled and unfilled positions to meet federal cyber workforce coding requirements and comply with the DOD Coding Guide.[24] The Inspector General also recommended that the DOD CIO and other stakeholders conduct a study on the feasibility of including quality assurance checks in systems used for coding civilian cyber workforce positions. Both recommendations are still open as of March 2024, according to the DOD Inspector General.

To begin addressing these recommendations, DOD CIO has issued coding requirements for civilian and military cyber positions and personnel, issued data quality assurance taskers, and developed

[22]GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: March 12, 2019). According to the Office of Personnel Management, an occupational series is a grouping of positions with a similar line of work and qualification requirements. For example, the 2210 Information Technology Management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services.

[23]Priority open recommendations are the GAO recommendations that warrant priority attention from heads of key departments or agencies because their implementation could save large amounts of money; improve congressional and/or executive branch decision-making on major issues; eliminate mismanagement, fraud, and abuse; or ensure that programs comply with laws and funds are legally spent, among other benefits. For our latest priority recommendation report sent to DOD, see: GAO, *Priority Open Recommendations: Department of Defense*, GAO-23-106305 (Washington, D.C.: May 16, 2023, reissued with revisions on June 8, 2023).

[24]Department of Defense Inspector General, *Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce* (July 29, 2021).

automated mechanisms to report on coding quality and completeness. According to officials, Services and Components must code their workforce and sustain coding accuracy through annual reviews of position duties and requirements.

The Navy Faces Challenges with Cyber Training

The Navy faces challenges with scheduling cyber workforce training for sailors preparing for the Cyber Mission Force and improving low pass rates for certain advanced cyber training and is working to address both challenges.[25]

CNA Recommendations Related to Training

The CNA study on military career paths made multiple recommendations related to military cyber training issues. For example, the study recommended the Navy

- increase training opportunities for cyber sailors, such as training in the flow of work/microlearning, off-the-shelf training, and refresher training;
- increase currency and relevance of Navy cyber training;
- improve officer training for cyber; and
- address issues with training not controlled by the Navy.

Source: GAO analysis of Center for Naval Analyses (CNA) information (text); U.S. Navy/Petty Officer 1st Class S. Souvannason (image). | GAO-24-106879

A primary challenge to the Navy's cyber readiness is scheduling sailors for certain work role training. According to Navy documentation and interviews with officials, while the services provide entry-level training for cyber personnel and selected work role training, the National Security Agency and outside vendors deliver training for other work roles. Further, accessing this work role training is heavily dependent on National Security Agency or outside vendor course scheduling and class

[25]The Cyber Mission Force comprises cyber mission teams made up of service members with advanced cyber training who play a critical role in executing cyber missions. In 2019 we reported on DOD's efforts to develop and maintain a trained Cyber Mission Force, among other things. For more information on training for CYBERCOM personnel, see GAO, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, D.C.: Mar. 6, 2019).

availability, rather than on the Navy's training timeline. This disconnect can have the effect that certain courses cannot be taken sequentially without gaps.

Another challenge is that training for some work roles is only available after sailors arrive at the Cyber Mission Force, which reduces the amount of time sailors are available to perform their job. Navy officials said that once sailors arrive at their units on the Cyber Mission Force, training completion is often not the highest priority. As a result, there can be a tension between completing training and meeting the operational needs of the commander.

In addition to scheduling challenges, Navy officials stated that the Navy has limited tools for addressing low pass rates for the training they do not administer. For example, the entry-level exploitation analyst training has a 64 percent pass rate. However, officials said the Navy does not manage or oversee any portion of exploitation analyst training. In contrast, Navy officials stated that the Joint Cyber Analysis Course, an entry-level training course for personnel designated for Cyber Mission Force roles, is administered by the Navy. Therefore, the Navy has more options for working to improve pass rates for that course and can determine whether to require sailors to retake parts of it to retain them, according to these officials.

The combination of scheduling challenges and limited control to address pass rates for advanced cyber training has led to low fill rates for certain Cyber Mission Force work roles. For example, according to data provided by Navy officials, while the Cyber Warfare Technician rating (formerly the Cryptologic Technician-Networks rating), which primarily fills Cyber Mission Force positions, had a 92 percent fill rate overall as of December 2023, certain work roles within the rating have lower fill rates.[26] For instance, according to data provided by Navy officials, the Interactive On-Net Operator position within the Cyber Warfare Technician rating had a 44 percent fill rate, which Navy officials attributed primarily to issues with training the sailors.

[26]Navy ratings are enlisted occupations that consist of specific skills and abilities. The Cryptologic Technician –Networks rating (now renamed the Cyber Warfare Technician rating) is one of the primary ratings used for sailors performing cyber-related work. Interactive On-Net Operator is a position or work role within the Cyber Warfare Technician rating.

According to CYBERCOM officials, despite its challenges, the current training model is designed to mitigate risk, including those involved in controlling sensitive techniques, tactics, and procedures. Further, CYBERCOM is working with the military services to analyze which courses can be moved to the services and has already moved some of them. Furthermore, DOD is conducting a study to evaluate service responsibilities for organizing, training, and assigning personnel to the Cyber Mission Force in response to a requirement in section 1533 of the National Defense Authorization Act for Fiscal Year 2023.[27] DOD is required to complete this study no later than June 1, 2024 and to establish a revised total force generation model for the Cyber Operations Forces by December 31, 2024. The DOD Inspector General is also conducting an audit to determine whether the military services are meeting readiness requirements for staffing, training, and equipping the Cyber Mission Force in accordance with DOD guidance. A DOD Inspector General official stated they plan to issue a report in fall 2024.

According to Navy documentation and interviews with officials, in response to low Cyber Mission Force readiness and these training challenges, the Navy has reviewed training models and made changes and additional investments. For example, according to Navy officials, the Navy is working on the following initiatives:

- **The Career Long Learning Continuum.** The continuum is an effort to capture all technical, professional, and leadership training; and applicable qualifications, certifications, and skillsets for each rating. By the end of fiscal year 2024, the Navy plans to develop courses of action to address training gaps identified and intends to be able to provide comprehensive roadmaps for the sailor, which will outline individual training by rating throughout the sailor's career.
- **The Cyber Qualification Training Teams.** These teams are intended to improve unit training, support certification events, monitor Cyber Mission Force team readiness, tailor advanced training, and manage continuous execution of unit level training. The Navy expects these teams to be initially operational in fiscal year 2026 and fully operational in fiscal year 2028.

According to CYBERCOM officials, it is difficult to gauge the effects of the Navy's changes to career paths and training given they are so recent. However, Navy officials stated that these initiatives, if fully implemented,

[27]Pub. L. No. 117-263, § 1533 (2022).

would address challenges in several areas of cyber training, including work role training, unit training, and certification. Further, according to CYBERCOM and Navy officials, the new cyber-specific rating allows the Navy to assign sailors in this rating to more tours in the Cyber Mission Force, thus increasing the return on investment of cyber training.

DOD and the Navy Established a Framework for Implementing DOD Cyber Workforce Initiatives

The Navy's framework for implementing cyber workforce initiatives includes participating in DOD-wide planning activities, implementing efforts identified in the Navy's cyber strategy, and establishing policy and a governance body.

DOD's 2023-2027 Cyber Workforce Strategy and the accompanying implementation plan establish a unified direction for managing the department's cyber workforce.[28] Specifically, the strategy and implementation plan describe a series of goals, objectives, initiatives, key performance indicators, and timelines to enable DOD to identify, recruit, develop, and retain a more agile and effective cyber workforce.

In addition, the DOD Cyber Workforce Strategy Implementation Plan (DOD Plan) identifies the military services as having coordinating responsibility for certain initiatives. For the Navy, it is an office of coordinating responsibility for 31 of 38 initiatives, according to DOD officials. In these roles, the Navy is participating in action planning groups to achieve the initiatives. For example, the Navy participated in action planning groups for initiatives related to developing a mentoring program, increasing utilization of talent exchanges with the private sector, and increasing the return on investment of scholarship programs, according to Navy officials.[29]

[28]Department of Defense, *Cyber Workforce Strategy 2023-2027* (Mar. 9, 2023); Department of Defense, *Cyber Workforce Strategy Implementation Plan 2023-2027* (Aug. 3, 2023).

[29]Officials from the Office of the DOD CIO, the lead for the DOD Plan, said that as of mid-February 2024, offices of primary responsibility had submitted action plans for most of the 38 initiatives in the DOD Plan.

The Department of the Navy issued its own Cyber Strategy in November 2023.[30] The strategy includes a workforce line of effort with five sub-lines of effort related to improving recruitment, workforce management, talent development, retention, and cybersecurity awareness. The workforce line of effort seeks to align with the DOD Cyber Workforce Strategy. For example, to improve workforce management, the Navy strategy states the Navy will implement the DOD Cyberspace Workforce Qualification and Management Program, in alignment with the DOD cyber strategy.

The Navy currently does not have plans to develop a Navy-specific cyber workforce strategy, a step suggested in the CNA report on military cyber career paths to ensure completion of initiatives. According to a senior Navy official, there is currently no plan to develop another strategy document within the Navy. Rather, the Department of the Navy is focused on aligning its cyber strategy and lines of effort with the DOD Plan and related directives coming from the Office of the Secretary of Defense level. According to officials from the office of the DOD CIO, the DOD *Cyber Workforce Strategy* and accompanying implementation plan provide a robust framework for implementing initiatives through collaboration and development of action plans to achieve the initiatives by 2027.

In addition to its new cyber strategy, the Navy issued an instruction in October 2023 that establishes policy and assigns responsibility for qualification and management of the Navy's cyber workforce.[31] The instruction authorizes the re-establishment of a cyber workforce management, oversight, and compliance council and requires each Navy organization to designate, in writing, Cyber Workforce Program Managers responsible for administering each Navy organization's cyber workforce program.[32] Additionally, the Cyber Workforce Program Office is currently working on an update to the policy manual that builds upon the instruction, providing a greater level of detail on responsibilities and

[30]Department of the Navy, *Cyber Strategy* (Nov. 21, 2023).

[31]Secretary of the Navy Instruction 5239.25*, Department of the Navy Cyberspace Workforce Qualification and Management Program* (Oct. 10, 2023).

[32]The Navy and Marine Corps Cyberspace Workforce Management, Oversight, and Compliance Council is described in Secretary of the Navy Instruction 5239.25. Department of the Navy policy and this oversight council apply to the Department of the Navy overall; whereas the scope of the CNA studies and our review was limited to the Navy and excluded the Marine Corps.

processes, according to Navy officials. The Navy plans to release this manual in the third quarter of fiscal year 2024.

The Navy's cyber workforce management, oversight, and compliance council, originally established in 2019, is intended to provide a forum for addressing key cyber workforce management, training, and development issues. According to Navy officials, the council put its meetings on hold pending updates to DOD and Navy policy. Specifically, the policies to be updated include DOD issuances describing the Cyber Workforce Qualification and Management Program, and the corresponding Navy instruction and manual.[33] In the meantime, the Navy has been conducting a senior-level biweekly meeting to discuss cyber workforce issues, according to Navy officials, and expects to complete the council's charter and resume meetings in the third quarter of fiscal year 2024.

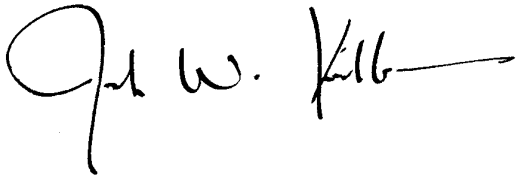
Agency Comments

We provided a draft of this report to DOD for review and comment. DOD provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Secretary of the Navy, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

[33]According to officials, the relevant issuances are DOD Directive 8140.01, DOD Instruction 8140.02, DOD Manual 8140.03, and Secretary of the Navy Instruction 5239.25, respectively. The Navy manual is still in development.

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.



Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable Jack Reed
Chairman
The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chair
The Honorable Susan Collins
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chair
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Section 1536 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 included a provision for us to assess the extent to which the Navy implemented recommendations from studies on career paths and to make additional recommended actions for improving readiness and retention of the Navy's cyber workforce.[1]

In this report we examine the extent to which the Navy has

- implemented the recommendations in the Navy-sponsored studies on improving cyber career paths,
- addressed continuing data and training challenges in strengthening its cyber workforce, and
- established a framework for implementing cyber workforce initiatives.

For objective one, we reviewed the Center for Naval Analyses (CNA) studies on civilian and military career paths and the 31 recommendations described in those studies.[2] We determined that the CNA studies focused on the Navy as a service specifically and did not include analysis of Marine Corps cyber career paths. We therefore limited our analysis to the Navy as a service.

Next, we collected information on the status of these recommendations from (1) the Navy's Report to Congress regarding the implementation status of the civilian recommendations,[3] (2) additional documentation we requested from the Navy regarding the civilian and miliary recommendations, and (3) interviews with Navy officials responsible for or knowledgeable of actions taken to implement the recommendations. With

[1]Pub. L. No. 117-263, § 1536 (2022).

[2]Center for Naval Analyses, *Navy Civilian Cyber Career Paths: Issues and Recommendations* (October 2021); Center for Naval Analyses, *Navy Military Cyber Career Paths: Issues and Recommendations* (April 2022).

[3]Office of the DCNO for Information Warfare, *Report to Congress, FY23 NDAA Section 1536 Recommendations from Navy Civilian Career Path Study* (Washington, D.C.: June 14, 2023).

this information, an analyst assessed the status of each recommendation using the following scale:

- **Implemented.** The Navy has taken actions to fully implement the recommendation.
- **In progress.** The Navy has taken steps towards implementing the recommendation or has partially implemented the recommendation with plans to take further actions.
- **Not implemented – plans to implement.** The Navy has not taken actions to implement the recommendation but plans to implement it in the future.
- **Not implemented – does not plan to implement.** The Navy has not taken actions to implement the recommendation and does not plan to implement it.

A second analyst reviewed the evidence and the first analyst's determinations and provided comments or concurrence. If the two analysts did not agree, a third analyst adjudicated.

CNA officials stated it typically does not conduct follow-up on study recommendations unless contracted to conduct a formal study that is sponsored and approved, which has not happened for these studies. However, CNA officials provided us with their perspectives on various recommendations and Navy actions to address them.

For the four recommendations that the Navy does not plan to implement, we gathered outside perspectives from the Center for Naval Analyses and the office of the Department of Defense (DOD) Chief Information Officer.

For objective two, to assess the extent to which Navy faces continuing challenges related to its cyber workforce, we interviewed DOD and Navy officials. Based on interviews and our follow up on the status of recommendations, we identified the common themes of data challenges and training challenges. Regarding data challenges, we reviewed personnel data for military and civilian cyber career fields and interviewed officials about their ongoing efforts to correct data reliability issues. We attempted to use this data to determine the structure and composition of the Navy's military and civilian workforce but found that the underlying data were unreliable. Regarding training challenges, we interviewed officials from Navy organizations involved in training cyber personnel and reviewed documentation.

For objective three, to assess the extent to which the Navy had a framework for implementing cyber workforce initiatives, we reviewed relevant documents, such as the DOD and Navy cyber strategies, the DOD Cyber Workforce Strategy Implementation Plan, and DOD and Navy policy to understand management of their cyber workforce programs and ongoing and planned cyber workforce initiatives. In addition, we discussed with DOD and Navy officials their plans, policies, and methods for carrying out their cyber workforce programs and initiatives.

As part of this work, we determined that internal controls were significant to our objectives.[4] Specifically, we determined that the control environment component of internal control, along with the underlying principles that (1) the oversight body should oversee the entity's internal control system and (2) management should establish organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives, were significant to our objectives. Additionally, we determined that the control activities component of internal control, along with the underlying principle that management should design control activities to achieve its objectives and respond to risks, were significant to our objectives. Also significant to our objectives were the information and communication component and the principles that management should (1) use quality information to achieve the entity's objectives and (2) communicate the necessary quality information to achieve the entity's objectives.

We conducted this performance audit from June 2023 to May 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[4]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or KirschbaumJ@gao.gov

Staff Acknowledgments

In addition to the contact named above, Lori Atkinson (Assistant Director), William Tedrick (Analyst in Charge), Vincent Buquicchio, Brenda S. Farrell, Christopher Gezon, Jacob Harwas, Katie Hickman, Michael Silver, Theologos Voudouris, and Lillian Moyano Yob made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548