United States Government Accountability Office

Report to Congressional Committees

December 2022

MILITARY CYBER PERSONNEL

Opportunities Exist to Improve Service Obligation Guidance and Data Tracking

Accessible Version

GAO-23-105423

GAO Highlights

Highlights of GAO-23-105423, a report to congressional committees

December 2022

MILITARY CYBER PERSONNEL

Opportunities Exist to Improve Service Obligation Guidance and Data Tracking

Why GAO Did This Study

To accomplish its national security mission and defend a wide range of critical infrastructure, DOD must recruit, train, and retain a knowledgeable and skilled cyber workforce. However, DOD faces increasing competition from the private sector looking to recruit top cyber talent to protect systems and data from a barrage of foreign attacks.

Senate Report 117-39 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2022 includes a provision for GAO to review retention challenges and service obligations for active-duty cyber personnel. Among other matters, GAO examines the extent to which (1) a service obligation exists for military cyber personnel receiving advanced cyber training and (2) DOD has experienced staffing gaps for active-duty military cyber personnel for fiscal year 2017 through fiscal year 2021 and tracked cyber work roles. GAO reviewed policies and guidance, analyzed staffing data from fiscal years 2017 through 2021, and interviewed DOD and military service officials.

What GAO Recommends

GAO is making six recommendations, including that the Army and Marine Corps clearly define active-duty service obligations for advanced cyber training in guidance, and that the Army, Air Force and Marine Corps track cyber personnel data by work role. DOD concurred with the recommendations.

View GAO-23-105423. For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

What GAO Found

The Navy and the Air Force have guidance requiring a 3-year active-duty service obligation for military personnel who receive lengthy and expensive advanced cyber training. This training prepares personnel to fill the Interactive On-Net Operator (ION) work role, identified as critical by U.S. Cyber Command (USCYBERCOM). In contrast, the Marine Corps does not have such guidance. Additionally, the Army's guidance does not clearly define active duty service obligations. Rather, it sets general service obligations based on the length of training. Using the Army's guidance, GAO estimated that active-duty officers receiving ION training may incur a service obligation of about 1.88 years. However, Army officials stated that they lacked the information needed to calculate and implement service obligations for ION training because it is not specifically listed in Army guidance. Army, Marine Corps, and USCYBERCOM officials acknowledged that guidance with clearly defined service obligations for ION training would create a better return on investment for this critical cyber work role. The Army and the Marine Corps have taken steps to clearly define service obligations for ION training, but officials did not know when or if the guidance would be implemented. Until the revised guidance is implemented, the Army and the Marine Corps are unnecessarily limiting their return on investment in ION training.

Years of Service Obligation Required in Military Service Guidance for Interactive On-Net Operator (ION) Training

	Army[a]	Navy	Marine Corps	Air Force
Officer	1.88	N/A[b]	N/A[b]	3
Enlisted	2.4	3	None	3

Source: GAO analysis of military service information. | GAO-23-105423

[a] GAO estimated these potential obligations, in part based on Army guidance, but ION training is not specifically listed in that guidance making this requirement challenging to implement, according to Army officials

[b] According to Navy documentation and Marine Corps officials, only enlisted personnel in those military services are eligible to train for the ION work role.

Staffing gaps—the difference between the number of personnel authorized and the number of personnel staffed—existed in some active-duty cyber career fields from fiscal years 2017 through 2021. Specifically, most of the Navy, Army, and Air Force cyber career fields were staffed at 80 percent or higher compared with the number of authorized personnel. However, four of the six Marine Corps career fields were below 80 percent of authorized levels in fiscal year 2021.

While the military services track cyber personnel staffing levels by career fields, USCYBERCOM uses work role designations to assign personnel to cyber mission teams. However, the Army, Air Force, and Marine Corps do not track staffing data by work role. As a result, military service officials cannot determine if specific work roles are experiencing staffing gaps. Tracking staffing data at the work role level would enable the military services to identify and address staffing challenges in providing the right personnel to carry out key missions at USCYBERCOM. This information is also essential for increasing personnel assigned to USCYBERCOM as planned by the Department of Defense (DOD).

Contents

Tables

Figures

Abbreviations

DCWF	DOD Cyberspace Workforce Framework
DOD	Department of Defense
ION	Interactive On-Net Operator
MARFORCYBER	Marine Corps Forces Cyberspace Command
NICE	National Initiative for Cybersecurity Education
USCYBERCOM	U.S. Cyber Command

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

December 21, 2022

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate
The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

With the advent of cyberspace warfare, the Department of Defense (DOD) must ensure its ability to offensively target adversaries and defensively protect its networks, information systems, and data. DOD's 2018 Cyber Strategy, among other things, identifies a ready cyber workforce as critical to executing these tasks. The strategy states that in order to accomplish DOD's mission and defend a wide range of critical infrastructure, DOD must recruit, train, and retain a knowledgeable and skilled cyber workforce.[1] As the world becomes more dependent on cyber capabilities, DOD faces increasing competition from the private sector looking to recruit top cyber talent to protect the department's systems and data from a barrage of foreign attacks.

In April 2022, the Commander, U.S. Cyber Command (USCYBERCOM), testified before the Senate Armed Services Committee noting that the command was experiencing a high level of operations and planned to increase its cyber workforce over the next 5 years.[2] In addition, Army officials stated in June 2022 that the Army was planning to approximately double the size of its cyber forces over the next 5 years, but the officials

[1] Department of Defense*, 2018 Department of Defense Cyber Strategy Summary.*

[2] *Hearing to Receive Testimony on the Posture of the United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2023 and the Future Years Defense Program Before the S. Comm. on Armed Services,* 117th Cong. 2-3 (2022) (prepared statement of Paul Nakasone, Commander/Chief, United States Cyber Command/ National Security Agency).

later noted the Army would miss its recruitment goals for fiscal year 2022. In June 2022, DOD stated that the broader recruiting market continues to present significant challenges to the military services. Similarly, we reported in August 2022 that the military services have acknowledged recent challenges in recruiting for military service.[3] DOD and the military services have attributed these challenges to a number of social and economic factors, such as low unemployment rates, competitive labor markets, limited eligibility among the youth population, and the COVID-19 pandemic.

Senate Report 117-39 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2022 included a provision that we review recruiting and retention challenges as well as “service obligations”—minimum terms of military service—for active-duty military cyber personnel.[4] Our report examines the extent to which (1) a service obligation exists for military cyber personnel receiving advanced cyber training, (2) DOD has experienced staffing gaps for active-duty military cyber personnel for fiscal year 2017 through fiscal year 2021 and tracked cyber work roles, and (3) the military services have used special and incentive pays since fiscal year 2017 to address any recruiting and retention challenges.[5]

For our first objective, we reviewed federal law and DOD and military service guidance related to service obligations for military cyber personnel, and interviewed military service officials about how they implement such policies. USCYBERCOM officials identified three critical work roles: Capabilities Developer, Interactive On-Net Operator (ION),

[3] GAO, *Military Personnel: Armed Forces Should Clarify Tattoo Policies’ Waiver Guidance,* GAO-22-105676 (Washington, D.C.: Aug. 17, 2022).

[4] S. Rep. No. 117-39, at 163 (2021).

[5] DOD Instruction 1304.29 states that it is DOD policy that the military services use enlistment, accession, reenlistment, and retention bonuses (what we refer to as “special pays” in this report) as monetary incentives to influence personnel levels. Each military service sets its own policies for when to award special pays and for how much to award. See Department of Defense Instruction 1304.29, *Administration of Enlistment Accession Bonuses, for New Officers in Critical Skills, Selective Reenlistment Bonuses, and Critical Skills Retention Bonuses for Active Members* (Dec. 15, 2013) (incorporating change 1, effective July 11, 2016).

We did not include the Space Force or the Coast Guard in this review because they do not currently provide cyber personnel to U.S. Cyber Command to fill cyber mission team positions.

and Exploitation Analyst. Further, DOD and military service officials identified the advanced cyber training to fill the ION work role as resource-intensive and lengthy. Accordingly, this report focuses on service obligations related to ION training. We determined that principles for internal control—specifically, that management should complete and document corrective actions to remediate internal control deficiencies, and should implement control activities through policies—were relevant to this objective.[6] We assessed military service guidance related to service obligations to determine the extent to which the guidance aligned with these principles, as well as the extent to which they aligned with key principles of human capital management identified in our prior work.[7]

For our second objective, we evaluated the extent to which DOD has experienced staffing gaps for active-duty military cyber personnel. We worked with the military services, their personnel offices, and with career field managers to identify career fields that are primarily cyber in their function.[8] We collected and analyzed data on staffing and authorizations for those career fields for fiscal years 2017 through 2021—the most recent years for which complete data were available across the military services. We compared the information with our review of military service data, DOD guidance, and interviews with DOD to determine if the military services were collecting and tracking data on cyber work roles.[9]

For our third objective, we identified which special pays the military used to help recruit and retain cyber personnel for fiscal years 2017 through 2021— the most recent years for which data were available We also

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

[7] GAO, *A Model of Strategic Human Capital Management,* GAO-02-373SP (Washington, D.C.: Mar. 15, 2002). Specifically, we identified the key principles that agencies should make targeted investments in employees, and that decisions about such investments should be based largely on expected improvement in agency results as relevant to this objective.

[8] Military “career fields” are referred to differently by each military service. Within the Army, career fields are referred to as Military Occupational Specialties; in the Air Force, as Air Force Specialty Codes; within the Navy, as Navy Ratings (enlisted) or Designator (officer); and within the Marine Corps, as Primary Military Occupational Specialties. For the purposes of this report, we use the term “career field” to refer to these positions. See the background section of this report for a full list of career fields selected from each military service.

[9] Department of Defense Instruction 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements* (Dec. 21, 2021).

reviewed the extent to which DOD had taken steps to implement our prior recommendations related to special and incentive pays directed at military cyber personnel.[10]

We assessed the reliability of the data we collected on staffing, authorizations, and special and incentive pay options by reviewing the data for completeness and interviewing officials knowledgeable about the implementation of the data systems. We found these data to be sufficiently reliable for comparing staffing levels for cyber personnel against military service retention goals, and for understanding the extent to which cyber personnel had accepted special pay retention incentives.

For more information on our scope and methodology, see appendix I.

We conducted this performance audit from September 2021 to December 2022 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.

Background

Military Cyber Work Force and Entities with Key Roles and Responsibilities

DOD defines its “cyberspace workforce” as personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources, among other things. The cyberspace workforce comprises several workforce elements, including IT, cybersecurity, and portions of the intelligence workforce.[11] Various officials and offices have roles and responsibilities related to DOD’s cyber workforce, as discussed below.

- The **DOD Chief Information Officer** oversees and is responsible for the management of DOD IT, cybersecurity, and cyberspace enabler

[10] GAO, *Military Compensation: Additional Actions Are Needed to Better Manage Special and Incentive Pay Programs,* GAO-17-39 (Washington, D.C.: Feb. 3, 2017).

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

workforce elements of the DOD cyberspace workforce, among other things.

- 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, and developing and collecting data elements not currently collected in authoritative manpower and personnel systems.
- The **Principal Cyber Advisor** advises the Secretary of Defense on cyber-related activities that support or enable DOD's missions in, through, and from cyberspace, and coordinates and oversees the implementation of the DOD Cyber Strategy.
- The **Commander, U.S. Cyber Command (USCYBERCOM)** is responsible for coordinating across DOD on qualification standards for all cyberspace operational work roles to ensure enterprise baseline standards support mission force qualifications, and developing and maintaining guidance necessary to provision, train, and operate DOD cyber operations forces, among other things.[12]
- DOD component heads, including the **Secretaries of the military departments**, are responsible for implementing cyberspace workforce management programs. Further, among other things, the component heads are responsible for identifying personnel required to perform cyberspace work roles in authoritative manpower and personnel systems, and establishing and implementing component-specific cyberspace work role training, qualification, and standards for the component cyberspace workforce. The DOD components, including the military departments, are to use the DOD Cyberspace Workforce Framework (DCWF) as the authoritative reference for identifying, tracking, and reporting on cyberspace positions.[13]

[12] DOD cyber operations forces include cyber mission forces, 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.

[13] DOD Directive 8140.01.

The DCWF describes the work performed by the full spectrum of the cyber workforce, and includes 54 work roles based on the work an individual performs, as opposed to 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.[14] According to officials with the office of the Chief Information Officer, they have developed an IT system and dashboard that allows them to code and track civilian cyber positions by both occupation and DCWF work role. However, these DCWF work roles are different from the work roles used by USCYBERCOM for its cyber mission forces, according to DOD CIO officials. Further, these officials also stated they are collaborating with USCYBERCOM to align these work roles in fiscal year 2023.

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. DOD defines the “cyber operations force” as units organized, trained, and equipped to conduct offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.[15] To achieve its mission, the USCYBERCOM is supported by the military service cyber components—U.S. Army Cyber Command, Fleet Cyber Command, Marine Corps Forces Cyberspace Command, and Air Forces Cyber. As previously discussed, multiple military career fields within each military service are primarily cyber in their function (see table 1 for a list of relevant career fields, identified by DOD officials, that we included in our review).

[14] DOD Instruction 8140.02.

[15] DOD Directive 8140.01.

Table 1: Military Cyber Career Fields Reviewed by GAO

Military service	Career field designation	Career field title
Army	17A	Cyber Warfare Officer (officer)
	17C	Cyber Operations Specialist (enlisted)
	170A	Cyber Warfare Technician (warrant officer)
	255S	Information Protection Technician (warrant officer)
	25D	Cyber Network Defender (enlisted)
Navy	1810	Cryptologic Warfare (officer)
	1820	Cyberspace Information/Information Professional (officer)
	1840	Cyber Warfare Engineer (officer)
	7820	Information Systems Technical (warrant officer)
	7840	Cyber Warrant Officer (warrant officer)
	CTN	Cryptologic Technician-Networks (enlisted)
	IT	Information Systems Technician (enlisted)
Marine Corps	1702	Cyberspace Officer (officer)
	1705	Cyberspace Warfare Development Officer (officer)
	1710	Offensive Cyberspace Warfare Officer (warrant officer)
	1711	Offensive Cyberspace Exploitation Operator (enlisted)
	1720	Defensive Cyberspace Warfare Officer (warrant officer)
	1721	Cyber Defensive Operator (enlisted)
	1799	Cyberspace Operations Chief (enlisted)
Air Force	17D	Warfighter Communications Operations Officer (officer)
	17S	Cyberspace Effects Operations Officer (officer)
	1B4X1	Cyber Warfare Operations (enlisted)
	1N4X1A	Cyber Intelligence Analyst (enlisted)
	3D0X2	Cyber Systems Operations (enlisted)
	3D0X4	Computer Systems Programming (enlisted)

Source: GAO analysis of Department of Defense and military service information. | GAO-23-105423

Note: Effective in fiscal year 2022, the Army established the career field 17D, Cyber Capabilities Development Officer. Some cyber personnel previously in the 17A, Cyber Warfare Officer career field were recoded to this new career field. The Army also established the career field 170D, Cyber Capabilities Developer Technician, which included some cyber personnel previously in the 170A, Cyber Warfare Technician career field. Air Force officials stated that the 3D0X2 and 3D0X4 have been updated to 1D7X1B, Cyber Systems Operations and 1D7X1Z, Software Development Operation respectively.

The military services support USCYBERCOM by providing personnel to fill work role billets, such as Capabilities Developer, Operator, and

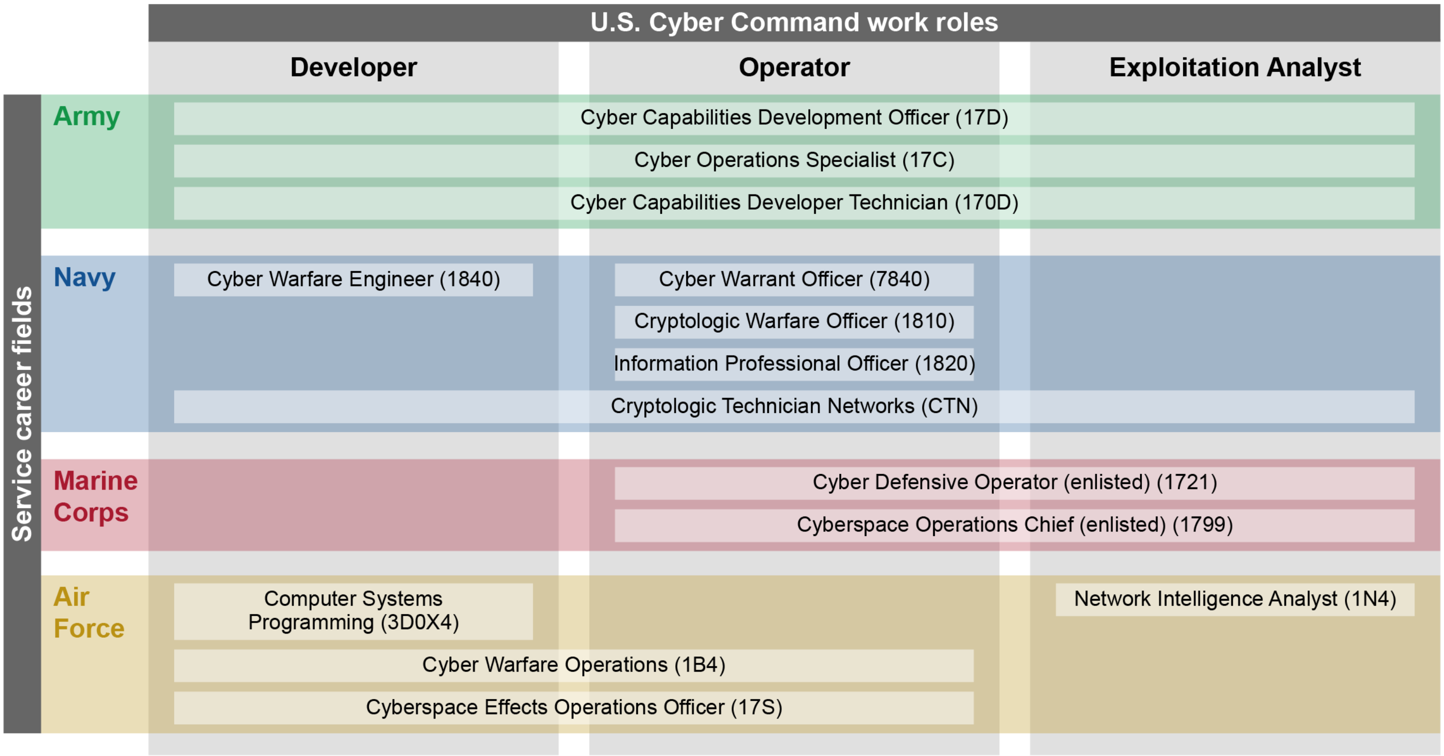
Exploitation Analyst.[16] Military career fields do not correlate directly to USCYBERCOM work roles, and a work role may be filled by individuals from multiple different career fields. Army Intelligence Center of Excellence and U.S. Army Cyber Command officials described this approach, stating that personnel are assigned to work roles using a "best athlete" model, with a focus on skill set rather than career field.

For example, if the Air Force provides personnel to fill the USCYBERCOM Cyberspace Capabilities Developer work role, those personnel may be drawn from the Computer Systems Programming or Developmental Engineer career fields, among others. Similarly, personnel in the Cyber Warfare Operations career field may be eligible to fill all non-intelligence-related Operator and Developer work roles at USCYBERCOM.[17] Further, according to USCYBERCOM officials, the military services may assign officers, enlisted service members, or warrant officers to fill the same work roles. See figure 1 for examples of USCYBERCOM work roles and the military service career fields that may fill them.

[16] According to U.S. Army Cyber Command officials, the military services also fill cyber positions similar to USCYBERCOM work roles internally. For example, the Army has operator and developer positions in a specific cyber warfare battalion.

[17] According to officials with the office of the Chief Information Officer, USCYBERCOM work roles are distinct from work roles defined in the National Initiative for Cybersecurity Education (NICE) framework, which is discussed in greater detail later in this report.

Figure 1: Examples of U.S. Cyber Command Work Roles and Military Career Fields That May Fill Them



Service career fields	U.S. Cyber Command work roles: Developer	U.S. Cyber Command work roles: Operator	U.S. Cyber Command work roles: Exploitation Analyst
Army	Cyber Capabilities Development Officer (17D)	Cyber Capabilities Development Officer (17D)	Cyber Capabilities Development Officer (17D)
Army	Cyber Operations Specialist (17C)	Cyber Operations Specialist (17C)	Cyber Operations Specialist (17C)
Army	Cyber Capabilities Developer Technician (170D)	Cyber Capabilities Developer Technician (170D)	Cyber Capabilities Developer Technician (170D)
Navy	Cyber Warfare Engineer (1840)	Cyber Warrant Officer (7840) Cryptologic Warfare Officer (1810) Information Professional Officer (1820)	
Navy	Cryptologic Technician Networks (CTN)	Cryptologic Technician Networks (CTN)	Cryptologic Technician Networks (CTN)
Marine Corps		Cyber Defensive Operator (enlisted) (1721)	Cyber Defensive Operator (enlisted) (1721)
Marine Corps		Cyberspace Operations Chief (enlisted) (1799)	Cyberspace Operations Chief (enlisted) (1799)
Air Force	Computer Systems Programming (3D0X4)		Network Intelligence Analyst (1N4)
Air Force	Cyber Warfare Operations (1B4)	Cyber Warfare Operations (1B4)	
Air Force	Cyberspace Effects Operations Officer (17S)	Cyberspace Effects Operations Officer (17S)	

Source: GAO analysis of military service information and interviews. | GAO-23-105423

Note: The Army established the career fields Cyber Capabilities Development Officer (17D) and Cyber Capabilities Developer Technician (170D) in fiscal year 2021. Prior to that, cyber personnel in these career fields were categorized in the Cyber Warfare Officer (17A) and Cyber Warfare Technician (170A) career fields.

Military Service Obligations and Training

In accordance with statute, DOD Instruction 1304.25 states that all officers and enlisted personnel incur a military service obligation of 8 years from the date of entry and directs the Secretaries of the military departments to establish procedures for fulfilling the military service obligation.[18] Personnel incur an initial active-duty military service obligation depending on factors such as how a person entered the military, among other things. For example, officers who graduate from a military service academy incur a 5-year active-duty service obligation. Each of the military services has guidance for fulfilling the military service obligation, including, for several of the military services, designating events that incur specific active-duty service obligations, such as training.

All personnel receive initial training upon joining the military. Enlisted recruits begin their careers with initial military training, which includes basic training and subsequent specific training relevant to their designated military career field. The nature and duration of the career-specific training varies widely, from a few weeks to several months, depending on the requirements of the career field.

Similarly, officer candidates must complete training programs, some of which take up to 4 years, before the candidates can be commissioned officers at the most junior level. This training may be completed at (1) military academies; (2) Reserve Officers' Training Corps; (3) the Officer Candidate School for the Army, the Navy, and the Marine Corps; or (4) the Officer Training School for the Air Force. The military services provide initial career field-specific training, including that completed by cyber personnel, but this initial training may not be cyber specific.

Once a service member from one of the military services is assigned to USCYBERCOM, they must complete additional training specific to their assigned work role and fulfill joint qualification requirements before they

[18] 10 U.S.C. § 651 and DOD Instruction 1304.25 Section 651 provides that, with certain exceptions and as provided in DOD regulations, each person who becomes a member of an armed force shall serve for an initial total period of not less than 6 years nor more than 8 years. Per section 651, any part of an individual's service obligation that is not active duty shall be performed in a reserve component. According to Army officials, graduates of the U.S. Military Academy who enter cyber officer career fields incur an additional year of active-duty service obligation, for a total obligation of 6 years. Similarly, Marine Corps officials stated that officers in the Cyberspace Officer (1702) career field incur an active-duty service obligation of 6 years after completion of training.

are considered fully trained and qualified to perform their assigned role.[19] According to USCYBERCOM officials, the length of time from the arrival at USCYBERCOM and the beginning of work varies across work roles, but may be 18 months or more. For example, officials noted that military cyber personnel assigned to the Interactive On-Net Operator (ION) work role must complete a series of courses lasting a year or more, depending on course availability and other factors. As with other military training, personnel may incur additional service obligations for this training. Such obligations vary depending on the training and across the military services, as discussed later in this report.

GAO's Related Work on DOD's Cyber Workforce

Cybersecurity remained a designated government-wide high-risk area in our 2021 biennial report that updated GAO's High-Risk Series—which identifies and recommends actions to help resolve serious weaknesses in areas that involve substantial resources and provide critical services to the public. We noted that federal agencies continued to face challenges addressing needs related to their cyber workforce, and reiterated the need to address such challenges.[20] This has been an area identified as high risk since 1997, when we designated information security as a government-wide high-risk area, and expanded this to include protecting cyber critical infrastructure in 2003. We reported in 2018 that the federal government needs to establish a comprehensive cybersecurity strategy and perform effective oversight, among other things, to include addressing cybersecurity workforce management challenges.

We have also identified challenges specific to DOD's cyber workforce. For example, in 2019, we reported on DOD's, among other agencies', use of the National Initiative for Cybersecurity Education (NICE) framework's

[19] In 2019 we reported on DOD's efforts to develop and maintain trained cyber mission forces, among other things. For more information on training for USCYBERCOM 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). U.S. Army Cyber Command officials stated that the Army has attempted to provide some work role-specific training directly as part of initial entry training for cyber personnel. However, the officials stated that requirements to follow specific course material and instructor mandates have made it difficult to ensure the training is effective in reducing the training time required after a service member is assigned to USCYBERCOM.

[20] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

work role codes to categorize cybersecurity positions. We recommended, among other things, that DOD review and assess the NICE framework work role codes and position descriptions for accuracy.[21] In September 2020, DOD stated that it had taken steps to decrease the number of positions that were assigned inappropriate codes and was continuing to monitor and track coding with the aim of addressing the recommendation by September 2022. We are continuing to monitor DOD's efforts to address this recommendation and have designated it as a priority recommendation.[22]

Moreover, in 2017, we found that the military services awarded Selective Reenlistment Bonuses to cybersecurity personnel in accordance with their broader military career field designation, rather than tailoring the awards to the skill sets within those specialties that have specific or unique staffing shortfalls. Although the military services had some cybersecurity-specific career fields at that time, according to military service officials, each military service had assigned cybersecurity personnel to career fields that include other types of personnel skill sets, such as intelligence or IT. As a result, the military services did not always specifically target these bonuses to cybersecurity personnel, instead awarding bonuses to specialties that may include personnel for whom the Selective Reenlistment Bonus was unneeded.[23]

To facilitate DOD's oversight of the military services' special and incentive pay programs, and to fully ensure the effectiveness of these programs, we recommended that the Secretary of Defense direct the Secretaries of the military departments to develop approaches to directly target Selective Reenlistment Bonuses to cybersecurity skill sets. Subsequently, in April 2017, this issue was included in our annual duplication, overlap, and fragmentation report.[24] In June 2022, we found that the military services had implemented our recommendations, creating specific cyber career fields and cyber skill codes. Given this realignment, the military

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

[22] GAO, *Priority Open Recommendations: Department of Defense,* GAO-21-522PR (Washington, D.C.: Aug. 2, 2021).

[23] GAO-17-39.

[24] GAO, *2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits,* GAO-17-491SP (Washington, D.C.: Apr. 26, 2017).

services should be better positioned to target Selective Reenlistment Bonuses at career fields that are focused on cyber skills in a cost-effective manner.

Navy and Air Force, but Not Army and Marine Corps, Ensure a Return on Investment for Advanced Cyber Training

Navy and Air Force Have Service Obligations for ION Training

The Navy and the Air Force have instituted, through service policy, a 3-year service obligation for service members who receive training to fill the USCYBERCOM ION work role.[25] Cyber personnel complete service-specific initial training and career field training prior to being assigned to USCYBERCOM, while work role-specific training and certification is completed after assignment to that work role. Military service officials stated that the advanced cyber training to fill the ION work role is lengthy, challenging, and expensive, consisting of a series of consecutive courses in addition to an individual’s training for a military career field. Specifically, training and subsequent certification to fill the ION work role may take from 1 to nearly 3 years to complete, and Army, Air Force, and Marine Corps officials estimated the training’s cost per service member at from $220,000 to $500,000.[26]

Given the associated commitment of resources, the Navy and the Air Force have taken steps to ensure a return on their investment by instituting a 3-year service obligation for those who receive training to fill the ION work role. Specifically, Military Personnel Manual 1306-980

[25] Military Personnel Manual 1306-980, *Navy Interactive On-Net (ION) Computer Network Exploitation (CNE) Operator Certification Program* (April 24, 2018); Air Force Manual 36-2100, *Military Utilization and Classification* (April 7, 2021).

[26] Army, Air Force, and Marine Corps officials with whom we spoke provided varying estimates of the cost of the training. According to Air Force and Army officials, the cost of training to fill an ION work role fluctuates based on the contract for the training and the number of students. Further, the cost does not include any travel expenses associated with the training. We were unable to independently estimate the cost of training due to these fluctuations. The estimated time required for training to fill an ION work role includes the relevant courses, as well as other certification requirements.

establishes a 3-year active-duty service obligation for enlisted Navy cyber personnel—the only Navy personnel eligible for ION training—who complete training to certify to fill the ION work role.[27] Bureau of Naval Personnel officials stated that this allows for a return on investment of approximately one assignment completed by cyber personnel after they are trained to fill the ION work role.

Similarly, Air Force Manual 36-2100 states that ION training incurs a 3-year active-duty service obligation.[28] Air Force Personnel Center officials stated that cyber personnel complete a 6- to 9- month Undergraduate Cyber Warfare Training immediately after being commissioned. Officers may follow this training with the training required to fill the ION work role, for a total of approximately 3 years in training before becoming certified. Further, these officials stated that enlisted cyber personnel may complete initial training and a 3-year assignment with an Air Force cyber unit prior to attending the training to fill the ION work role. Officials stated that the 3-year active-duty service obligation associated with completion of the training ensures the Air Force receives at least one assignment from service members after they complete the training, which these officials stated is considered a sufficient return on investment.

Army Requires General Service Obligations for Training, but Officials Face Challenges Implementing Obligations for ION Training

Army Regulation 350-100 directs that, for military and civilian schools, officers incur an active-duty service obligation of three times the length of the training, computed in days, not to exceed 6 years.[29] Army Regulation 614-200 includes active-duty service obligations for enlisted service members and discusses how such obligations enhance the Army's return on training investment.[30] For courses not specifically listed, the service obligation incurred is based on the length of training. On the basis of

[27] Military Personnel Manual 1306-980.

[28] Air Force Manual 36-2100.

[29] Army Regulation 350-100, *Officer Active Duty Service Obligations* (Sept. 26, 2017).

[30] Army Regulation 614-200, *Enlisted Assignments and Utilization Management* (Jan. 25, 2019). Army Regulation 350-100 similarly notes that active-duty service obligations are intended to assist in ensuring a reasonable return to the Army following the expenditure of public funds, among other purposes.

these requirements, we estimate that in training to fill the ION position, a service member may incur an active-duty service obligation of 687 days, or approximately 1.88 years, for officers, and 29 months, or approximately 2.4 years, for enlisted service members.

However, according to U.S. Army Cyber Command officials, implementation of service obligations outlined in regulations for cyber officers and enlisted members can be challenging. Specifically, many advanced cyber training courses, including the ION training course, are not listed in regulation or in Army or joint training systems of record.[31] These officials stated that Army career counselors therefore lacked the information needed to calculate and implement service obligations for ION and other advanced cyber training courses. For example, U.S. Army Cyber Command officials cited difficulties such as long breaks between the courses that make up ION training, delays between when candidates are nominated for training and when they attend, and fluctuations in the length of the ION training courses. As a result, officials stated that it is a challenge to hold personnel to general service obligations when they attend ION training. U.S. Army Cyber Command officials noted that at times this has resulted in an officer attending a year-long course costing hundreds of thousands of dollars —such as the training for ION certification—and then leaving the military soon after completing certification, leaving the Army without an adequate return on its investment.

U.S. Army Cyber Command officials stated that they are working to revise Army Regulations 350-100 and 614-200 to clearly define a service obligation of 36 months for completion of the ION training for officers and enlisted members. However, we reviewed a revised draft Army Regulation 350-100 and found that the draft did not include a designated service obligation for advanced cyber training, including ION training. Proposed revisions to Army Regulation 614-200 did include service obligations for advanced cyber training, including ION training. However, officials with U.S. Army Cyber Command and the Office of the Deputy Chief of Staff, G-1 Personnel—the proponent office for the policy—stated that these changes have not yet been accepted. Further, officials did not have an estimated timeline for finalizing revisions to the regulation, and

[31] The Army Training Requirements and Resources System is the Army's system of record to resource and manage training courses. It is an online IT system for support of institutional training missions and consists of a centralized training management database. Army Regulation 350-1, *Army Training and Leader Development* (Dec. 10, 2017).

G-1 officials stated that it would likely be 2 years before such revisions are published, assuming the proposed changes are approved.[32]

Our prior work identified key principles of human capital management, including that agencies should make targeted investments in employees, and that decisions about such investments should be based largely on expected improvement in agency results.[33] In addition, *Standards for Internal Control in the Federal Government* states that management should remediate deficiencies by, for example, completing and documenting corrective actions to remediate internal control deficiencies in a timely basis, and should implement control activities through policies.[34] However, the Army has not taken sufficient corrective action to clearly define service obligations for ION training, such as by issuing revised policies in a timely manner, to ensure adequate return on investment through service obligations for advanced cyber training.

USCYBERCOM and Army officials stated that they believe increased and clearly defined service obligations would create a better return on investment in critical cyber work roles, particularly in the ION work role. Without issuing revised guidance in a timely manner to clearly define service obligations for advanced cyber training—particularly ION training—for both officers and enlisted members, the Army risks not receiving an adequate return on its investment in such training and may find itself understaffed in critical cyber work roles.

Marine Corps Does Not Require Any Service Obligation for ION Training

According to Marine Corps officials, there is no additional active-duty service obligation tied to training for specific roles or positions, such as the training required for ION certification. As a result, according to Marine Corps Forces Cyberspace Command (MARFORCYBER) officials, the Marine Corps does not currently have a method by which to assign additional service obligations to lengthy and costly training like that required for ION certification. Marine Corps officials stated that they have

[32] U.S. Army Cyber Command officials noted that they could request an exception to policy to allow them to begin enforcing updates to the Army regulation after it is signed, assuming the proposed changes are approved, rather than waiting for publication.

[33] GAO, *A Model of Strategic Human Capital Management,* GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

[34] GAO-14-704G

not established service obligations related to ION certification training because only enlisted personnel are eligible to train as IONs, and service obligations for enlisted personnel are handled via enlistment contract.

MARFORCYBER officials stated that, due to the length of ION training and lack of additional service obligations, personnel have approximately 13 months remaining of their initial service obligation once they complete the training, assuming they began training as soon as they were eligible. These officials believe that, if instituted, additional service obligations should be tied to advanced cyber training for critical work roles, such as training for ION certification, to better ensure an adequate return on investment.

According to a MARFORCYBER official, that office has requested guidance to institute active-duty service obligation requirements for personnel who pursue training and certification to become an ION. Specifically, MARFORCYBER has requested permission to institute a service obligation of 54 months from the start of the lengthy and expensive ION training. However, while MARFORCYBER supports the change as soon as possible, an official with that office was unsure when or if the request would be approved and implemented.

Our prior work identified key principles of human capital management, including that agencies should make targeted investments in employees and that decisions about such investments should be based largely on expected improvement in agency results.[35] In addition, *Standards for Internal Control in the Federal Government* states that management should remediate deficiencies by, for example, completing and documenting corrective actions to remediate internal control deficiencies in a timely basis, and should implement control activities through policies.[36] However, the Marine Corps has not taken sufficient corrective action to address the lack of service obligations for advanced cyber training. Additionally, the Marine Corps has not developed guidance in a timely manner to establish active-duty service obligations for advanced cyber training—particularly ION training—to ensure an adequate return on investment.

USCYBERCOM and Marine Corps officials stated that they believe active-duty service obligations associated with advanced cyber training

[35] GAO-02-373SP.

[36] GAO-14-704G.

would create a better return on investment in critical cyber work roles, and particularly in the ION work role. Without developing guidance in a timely manner to clearly define service obligations for advanced cyber training—particularly ION training—the Marine Corps may continue to forego an adequate return on its investment in such training. In addition, the Marine Corps may find itself understaffed in critical cyber skills as a result of investing in training for personnel who may take those skills elsewhere immediately after completing the training and certification.

Gaps Exist between Active-Duty Cyber Authorizations and Staffing Levels, and Opportunities Exist to Better Track Work Role Data

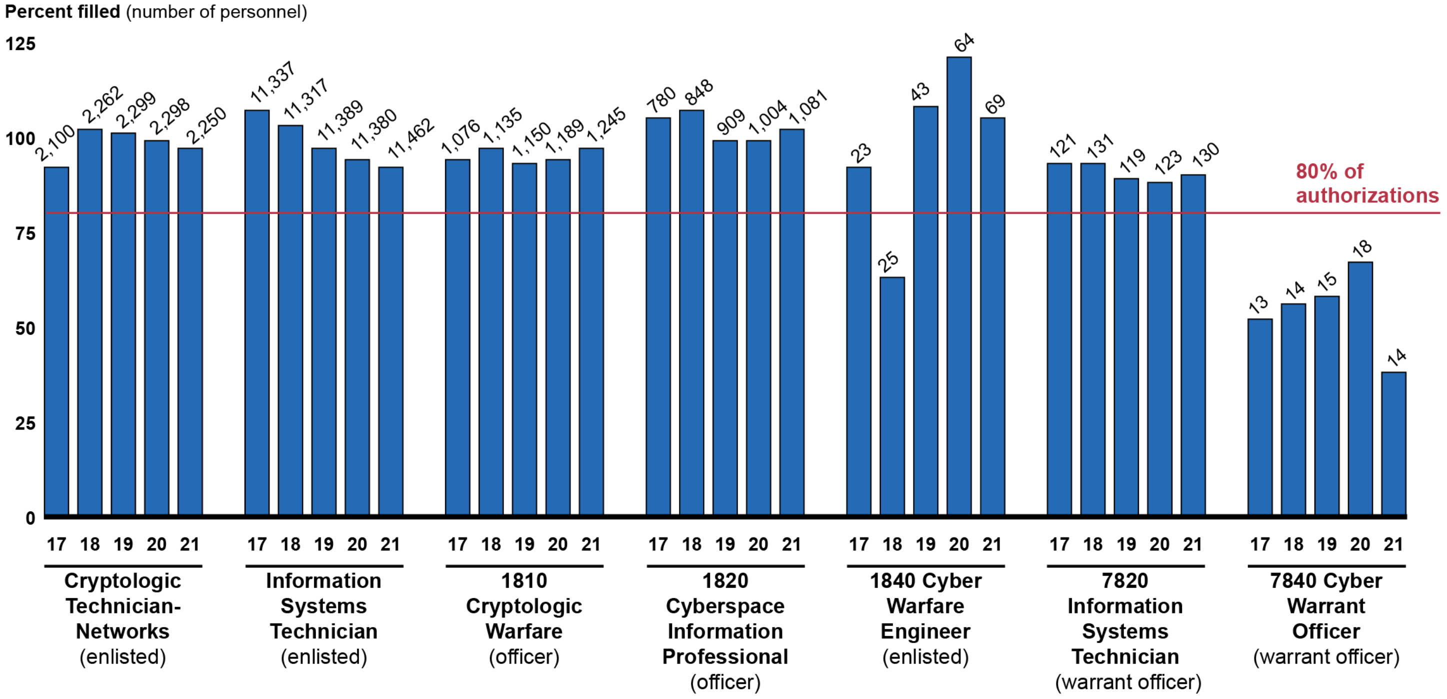
Some Gaps between Authorizations and Staffing Exist

We found that some staffing gaps exist to varying extents—predominately for warrant officers—between the number of personnel authorized and the number of personnel staffed to certain active-duty cyber career fields from fiscal years 2017 through 2021.[37] For most of the cyber career fields we reviewed, staffing was generally above 80 percent from fiscal years 2017 through 2021. Officials we spoke with were generally aware of these gaps and noted several key reasons for the staffing gaps, including the newness of some occupational specialties, challenges in successfully training specific occupational specialties, and retention, among others.

Navy cyber career fields were generally above 80 percent. Our analysis of Navy data showed that the Navy was able to staff the majority of its cyber career fields at over 80 percent staffing to authorizations in fiscal years 2017 through 2021. Our analysis found that in fiscal year 2021 all of the career fields included in our scope met or exceeded 80 percent of authorizations, with the exception of one of the warrant officer career fields. Figure 2 provides staffing data for the Navy cyber career fields included in our scope for fiscal years 2017 through 2021.

[37] For purposes of this report, “authorized personnel” refers to the number of positions that the military services reported as authorized to be filled. According to officials, each of the military services maintains its own staffing level goals for cyber personnel. For the purposes of our report we define “staffing gaps” as below 80 percent staffing to authorized personnel. For additional details see appendix I.

Figure 2: Navy Cyber Career Field Staffing Data for Fiscal Years 2017 through 2021



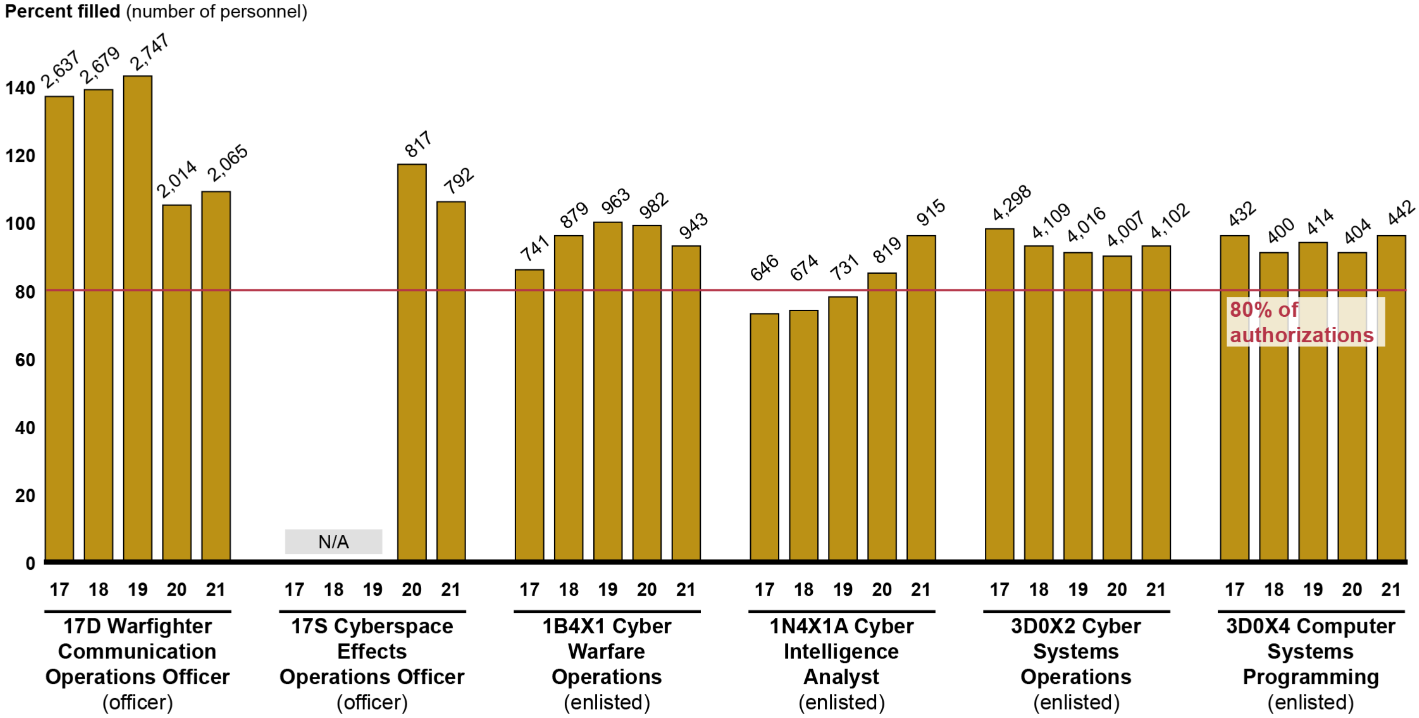
Source: GAO analysis of Navy data. | GAO-23-105423

Actual Staffing Levels and Percentage Above/Below Authorized Staffing Levels

Navy Cyber Career Fields	2017	2018	2019	2020	2021
Cryptologic Technician-Networks CTN (enlisted)	2,100 92%	2,262 102%	2,299 101%	2,298 99%	2,250 97%
Information Systems Technician IT (enlisted)	11,337 107%	11,317 103%	11,389 97%	11,380 94%	11,462 92%
1810 Cryptologic Warfare (officer)	1,076 94%	1,135 97%	1,150 93%	1,189 94%	1,245 97%
1820 Cyberspace Information Professional (officer)	780 105%	848 107%	909 99%	1,004 99%	1,081 102%
1840 Cyber Warfare Engineer (officer)	23 92%	25 63%	43 108%	64 121%	69 105%
7820 Information Systems Technical (warrant officer)	121 93%	131 93%	119 89%	123 88%	130 90%
7840 Cyber Warrant Officer (warrant officer)	13 52%	14 56%	15 58%	18 67%	14 38%

Air Force cyber career fields almost always exceeded 80 percent. Our analysis of Air Force data showed that staffing levels for all six cyber career fields included in our review almost always exceeded 80 percent staffing to authorizations in fiscal years 2017 through 2021. For example, the Air Force staffed two officer career fields (17D and 17S) above 95 percent of authorizations in fiscal years 2020 and 2021, according to our analysis. Similarly, the Air Force staffed the enlisted personnel's Cyber Warfare Operations (1B4X1) career field at about 99 percent of authorizations in fiscal year 2020 and at about 93 percent of authorizations in fiscal year 2021. Figure 3 provides staffing data for the Air Force cyber career fields included in our scope for fiscal years 2017 through 2021.

Figure 3: Air Force Staffing Data for Cyber Career Fields for Fiscal Years 2017 through 2021



Source: GAO analysis of Air Force data. | GAO-23-105423

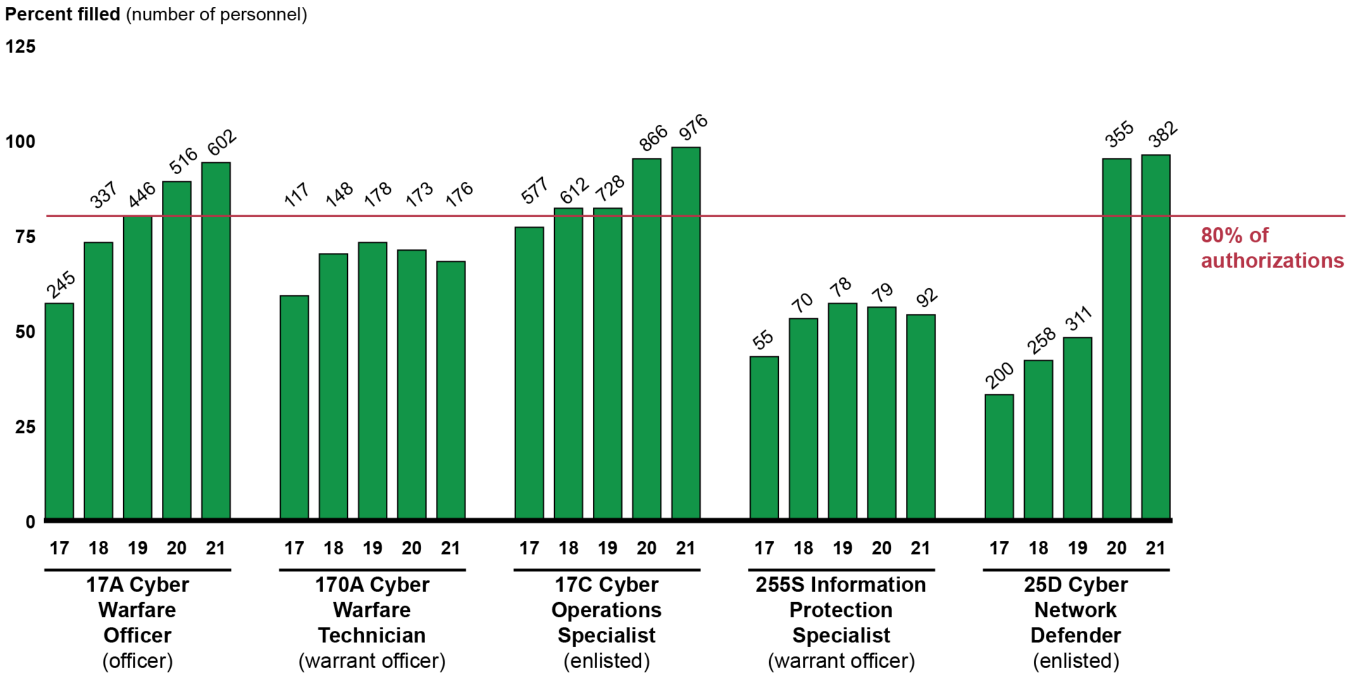
Note: According to Air Force officials, they have only begun tracking data on the 17S career field since fiscal year 2020, so we did not include earlier data.

Actual Staffing Levels and Percentage Above/Below Authorized Staffing Levels

Air Force Cyber Career Fields	2017	2018	2019	2020	2021
17D Warfighter Communication Operations Officer (officer)	2,294 102%	2,389 124%	2,479 129%	1,830 95%	1,897 99%
17S Cyberspace Effects Operations Officer (officer)[a]	11 2%	1 0%	1 0%	817 117%	747 106%
1B4X1 Cyber Warfare Operations (enlisted)	741 86%	879 96%	962 101%	982 99%	942 93%
1N4X1A Cyber Intelligence Analyst (enlisted)	645 73%	672 74%	729 78%	817 85%	910 95%
3D0X2 Cyber Systems Operations (enlisted)	4,192 96%	4,045 92%	3,913 89%	3,914 88%	3,979 91%
3D0X4 Computer Systems Programming (enlisted)	427 95%	396 90%	408 92%	393 89%	434 94%

Army cyber career fields generally improved to above 80 percent. Our analysis of Army data showed that overall staffing levels for Army cyber career fields generally improved from fiscal years 2017 through 2021. For example, staffing for the Cyber Warfare Officer and Cyber Operations Specialist (17A and 17C, respectively) career fields ranged from 94 percent of authorizations to almost 98 percent of authorizations in fiscal year 2021. The Army staffed the Cyber Network Defender (25D) career field at approximately 96 percent of authorizations for the same year. U.S. Army Cyber Command officials stated that this improvement in fill rates is indicative of efforts to stand up a new branch while increasing authorizations at the same time. Figure 4 shows Army staffing by cyber career field for fiscal years 2017 through 2021.

Figure 4: Army Staffing Data for Cyber Career Fields for Fiscal Years 2017 through 2021



Source: GAO analysis of Army data. | GAO-23-105423

Actual Staffing Levels and Percentage Above/Below Authorized Staffing Levels

Army Cyber Career Fields	2017	2018	2019	2020	2021
17A Cyber Warfare Officer (officer)	245 57%	337 73%	446 80%	580 89%	602 94%
170A Cyber Warfare Technician (warrant officer)	117 59%	148 70%	178 73%	173 71%	176 68%
17C Cyber Operations Specialist (enlisted)	577 77%	612 82%	728 82%	866 95%	976 98%
255S Information Protection Specialist (warrant officer)	55 43%	70 53%	78 57%	79 56%	92 54%
25D Cyber Network Defender (enlisted)	200 33%	258 42%	311 48%	355 95%	382 96%

The Army experienced staffing gaps for two career fields, both of which are staffed by warrant officers, in fiscal years 2017 through 2021. Specifically, the Army staffed the 170A and 255S career fields at 68 percent and 54 percent of authorizations, respectively, in fiscal year 2021, as shown in the figure above. Army officials stated that staffing levels for warrant officers are a challenge across the Army. Specifically, officials stated that warrant officers are in high demand across the Army and that the COVID-19 pandemic resulted in the cancellation or delay of Warrant Officer Candidate School. Officials estimated that it will take 2 years to rebuild staffing in these career fields.

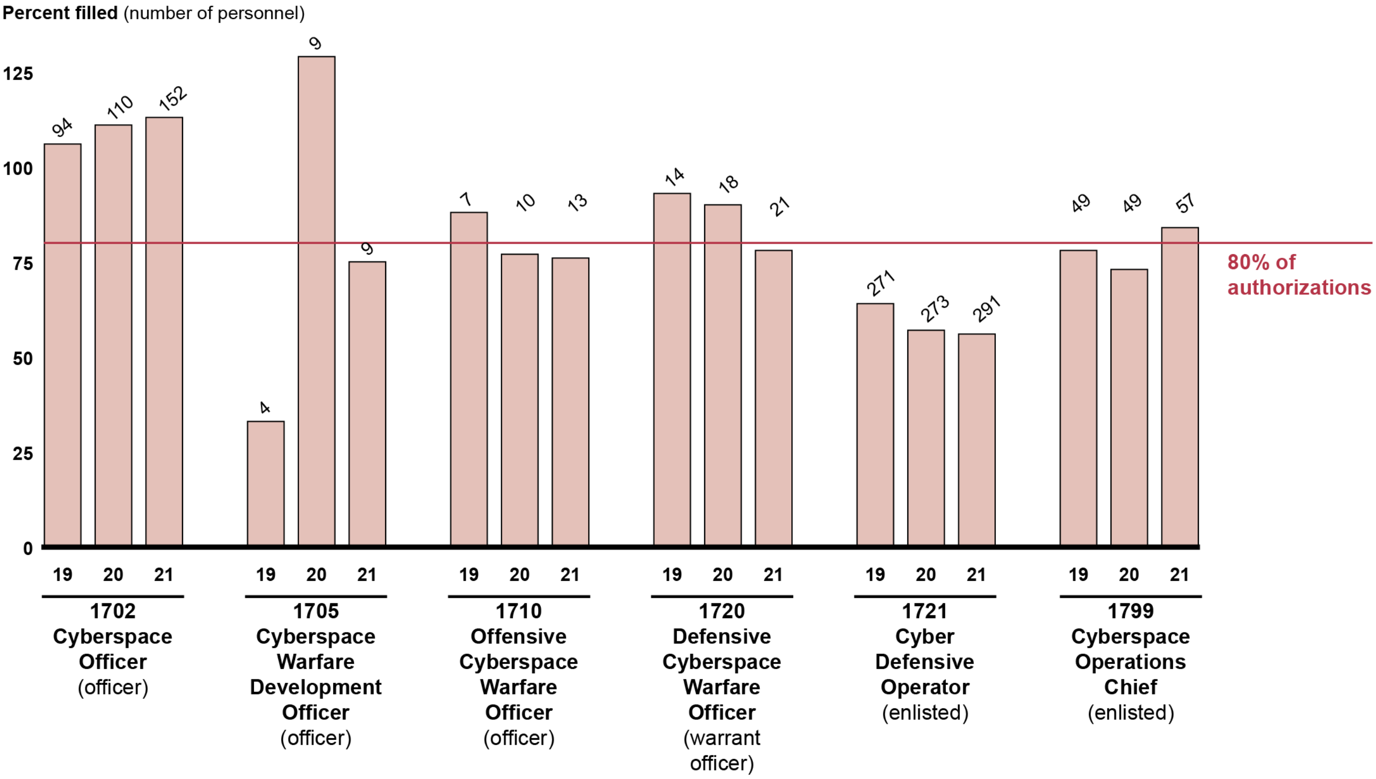
Moreover, the Army's cyber career fields Cyber Network Defender (25D) and Information Protection Specialist (255S) are difficult career fields to recruit personnel to staff, according to officials. These career fields are staffed by soldiers (enlisted and warrant officers, respectively) who move—or cross-train—from another career field within the Army. Officials stated that there are a limited number of applicants because these positions require soldiers to hold a Top Secret security clearance and acquire an additional 36-month service obligation because of the additional training specific to these career fields.[38]

Marine Corps cyber career fields generally did not exceed 80 percent. Our analysis of Marine Corps data showed some gaps between staffing and authorizations for fiscal years 2019 through 2021. Data for fiscal years 2017 and 2018 are not available because, according to Marine Corps officials, the 17XX career field was not established until 2018.

We included six types of cyber personnel within the 17XX career field in our analysis, including officers, warrant officers, and enlisted personnel. Only two of the 17XX types of cyber personnel in our analysis met Marine Corps 80-percent staffing to authorizations in fiscal year 2021, and some career fields experienced more significant gaps than others. For example, in fiscal year 2021, the Marine Corps staffed 1721 Cyber Defensive Operator, an enlisted career field, at 56 percent of authorizations. Similarly, the Marine Corps staffed some officer and warrant officer career fields at 75 to 78 percent of authorizations in fiscal year 2021. In contrast, the Marine Corps staffed the 1702 Cyberspace Officer career field above 100 percent of authorizations in fiscal years 2019 through 2021. Figure 5 shows Marine Corps staffing data for the 17XX cyber career field for fiscal years 2019 through 2021.

[38] The 36-month service obligation for the Enlisted Network Defender (25D) and warrant officer Information Protection Technician (255S) is due to the training received when those soldiers transfer into the career fields, according to officials.

Figure 5: Marine Corps Staffing Data for 17XX Cyber Career Field for Fiscal Years 2019 through 2021



Source: GAO analysis of Marine Corps data. | GAO-23-105423

Actual Staffing Levels and Percentage Above/Below Authorized Staffing Levels

Marine Corp Cyber Career Fields	2019	2020	2021
1702 Cyberspace Officer (officer)	94 106%	110 111%	152 113%
1705 Cyberspace Ware Development Officer (officer)	4 33%	9 129%	9 75%
1710 Offensive Cyberspace Warfare Officer (officer)	7 88%	10 77%	13 76%
1720 Defensive Cyberspace Warfare Officer (warrant officer)	14 93%	18 90%	21 78%
1721 Cyber Defensive Operator (enlisted)	271 64%	273 57%	291 56%
1799 Cyberspace Operations Chief (enlisted)	49 78%	49 73%	57 84%

Marine Corps officials we met with were aware of staffing gaps in some cyber career fields. These officials stated that staffing was low due to a variety of factors, including delays in obtaining security clearances and other challenges associated with building a new career field.

Opportunities Exist to Better Track Work Role Data

The military services routinely track military cyber personnel authorizations and staffing data at the military career field level, as discussed above. Military service officials stated that they use career field data to track overall career field health, target recruitment, and identify demand for training.

While maintaining and tracking data on military career fields is important for the military services to manage career fields, military personnel are not assigned to USCYBERCOM based on their career field, according to DOD officials. Rather, USCYBERCOM uses the work role designation to assign personnel to cyber mission teams. These work roles each have specific requirements and certifications that are needed in order for cyber personnel to execute that work role’s functions, according to officials. Moreover, these work roles can be filled by military personnel from one career field or be drawn from one of several different career fields.

Although all of the military services track staffing levels by career field data, not all of them track staffing levels by work roles. Specifically, the Navy tracks staffing by cyber work roles by using enlistment codes to mimic USCYBERCOM work roles and additional qualifications designators for officers to track training and skills, according to Navy officials. However, the Air Force, Army, and Marine Corps do not track cyber work role data.

According to Air Force officials, while the Air Force tracks the 17S cyber career field, it does not directly track what work roles the 17S may fill in the personnel system of record used by Air Force A-1 Manpower, Personnel, and Services. Similarly, Army officials noted that if the Army G-1 Personnel has to brief on work roles and associated personnel issues that information comes directly from a lower level that has visibility over those data. Finally, Marine Corps officials stated that the Marine Corps only tracks personnel by career field and not by work role because the Marine Corps manages marines by career field.

Many of the cyber career fields and work roles are newly established, and USCYBERCOM made several revisions over the past few years that resulted in changes or modifications to work roles and guidance, according to military service officials. Further, the Army, Air Force, and Marine Corps had some visibility over which military personnel are staffed to specific USCYBERCOM work roles. This visibility typically resided at lower levels within the military service and not at the military personnel command level. USCYBERCOM officials acknowledged that the Army, Air Force, and Marine Corps can compile personnel data by work roles; however, these data are not easy to compile and the processes for doing so are involved and take time. USCYBERCOM officials stated that this is generally only done for high-priority meetings or events, such as congressional briefings or when a senior official requests the data.

USCYBERCOM officials we met with stated that having data tracked by work role available to stakeholders across the enterprise, such as in the military services' personnel systems of record, would be beneficial. Specifically, USCYBERCOM officials stated that tracking personnel data by work role would provide them and the military services with greater visibility of current and projected staffing levels for work roles. For example, these officials stated that the Army assigns personnel in the 17C career field to fill eight different USCYBERCOM work roles. While the 17C career field was staffed at 98 percent in fiscal year 2021 according to our analysis, USCYBERCOM officials stated that this can mask staffing shortages in some work roles. Specifically, while five of the work roles filled by 17C career field personnel are staffed at healthy levels, USCYBERCOM officials stated that three—which are considered high value to USCYBERCOM—are critically understaffed.

Similarly, officials with the office of the DOD Chief Information Officer stated that tracking data by work role allows for identifying gaps in the workforce. For example, officials provided a demonstration of the system they use to track civilian cyber positions by work role. In this system, some occupations appeared healthy when viewed at the occupation level, but when sorted by work role, gaps in specific work roles were identified. DOD guidance related to DCWF, DOD Instruction 8140.02, outlines the requirements for identifying and tracking cyberspace workforce requirements, including for work roles.[39] Specifically, the instruction requires the military services to identify and code cyber positions. Further, it requires the military services to configure authoritative personnel

[39] DOD Instruction 8140.02.

systems to meet the identification and tracking requirements outlined in the instruction, among other guidance. Finally, the instruction also requires the military services to report on these data to support the current and long-term management of critical cyberspace resources.

While this guidance currently applies to the DCWF, officials with the office of the DOD Chief Information Officer stated they are working with USCYBERCOM to integrate USCYBERCOM's work roles into the DCWF. Specifically, these officials also stated they are in the process of developing a memorandum of understating with USCYBERCOM to incorporate USCYBERCOM work roles for military personnel into this system. Officials stated that this memorandum should be completed in 2023. However, the military services would still need to include work role data in their systems in order for the office of the DOD Chief Information Officer to see the data in its system.

The *Standards for Internal Control in the Federal Government* states that management should use quality information to achieve the entity's objectives.[40] Further, this internal control states that management should obtain relevant data on the identified information requirements and process relevant data from reliable sources into quality information within the entity's information system. However, the military services, with the exception of the Navy, do not track staffing levels of active-duty cyber personnel by USCYBERCOM work role, according to officials. As a result, officials do not have visibility over USCYBERCOM's ability to fill its work role billets.

The military services rely on personnel staffing data in order to determine if career fields are healthy and if the career field is eligible for special pays such as reenlistment bonuses. However, without the ability to systematically track data at the work role level at the personnel commands, military service officials will be unable to ascertain if specific work roles are experiencing staffing gaps. As noted above, cyber mission forces are expected to grow in the coming years. Tracking staffing data at the work role level within the Army's, Air Force's, and Marine Corps' personnel systems of record would allow the military services the opportunity to identify and address staffing challenges that the military services might face in providing the right personnel to USCYBERCOM.

[40] GAO-14-704G.

Military Service Use of Special and Incentive Pays in Cyber Career Fields Varies but Retention Challenges Persist

From fiscal years 2017 through 2021, the military services have used special and incentive pays to recruit and retain active-duty military personnel in cyber career fields.[41] The military services' use of special and incentive pays is intended to help ensure that military pay is sufficient to recruit and retain hard-to-fill or critical specialties, such as cyber, that require special skills and training for which higher compensation may be available in the civilian labor market.[42] The military services determine how to distribute special and incentive pays according to department guidance to meet strategic priorities, including to fill specific positions or encourage personnel to work in specific locations. The special and incentive pays used by the military services for the cyber workforce fall into three general categories: enlistment bonuses, assignment incentive pay, and retention bonuses.

Enlistment Bonuses

Enlistment bonuses include payments provided for enlistment and are intended to entice personnel to enlist for a given time period to perform strategically important career fields. The decision to award enlistment bonuses is up to the military services, based on their ability to meet their target recruitment goals. For example, while the Navy, Air Force, and Marine Corps offered enlistment bonuses during our reporting period, the Army did not, according to officials.

[41] We use the term "special and incentive pays" to refer to special pays, incentive pays, and bonuses authorized in chapter 5 of Title 37 of the U.S. Code. Terms may vary by military service, but for the purposes of this report we have combined related pays into three categories: enlistment bonuses, assignment incentive pay, and retention bonuses.

[42] In addition to monetary incentives, such as special pays, the military services may offer personnel non-monetary incentives to stay in cyber-related positions. However, according to officials, unlike special pays, non-monetary benefits are awarded on a case-by-case basis, not according to any particular DOD policy. Such incentives tend to be unofficial handshake agreements between personnel and their supervisors. For example, officials from the Army and Navy said they are sometimes able to extend a person's deployment or identify an assignment in the same location to incentivize a person to remain in a cyber-related position.

- **Navy.** The Navy offers enlistment bonuses to cyber personnel in the Cryptologic Technicians Networks rating, one of two cyber fields for enlisted personnel. Since 2017, the first year we collected data, enlisted personnel in this rating have been eligible to receive a signing bonus of $5,000 and an additional bonus of $30,000 upon completion of relevant training.
- **Air Force.** The Air Force offers enlistment bonuses to 3DXXX and 1N3XX career fields. Since fiscal year 2017, these bonuses have ranged from $12,000 to $20,000 for the 3DXXX career fields to a 6-year bonus of $18,000 for the 1N3XX career field. In addition, the bonus amounts varied during this time period from as much as $46,000 in fiscal year 2017 to $16,000 in fiscal year 2019. For fiscal year 2021, the bonus amount was $36,000.[43]
- **Marine Corps.** The Marine Corps offers an enlistment bonus for the 1711 and 1721 cyber career fields. This bonus has been offered since fiscal year 2019, when the cyber career field was created. For fiscal year 2022, the enlistment bonus amount was $2,000.[44]

Assignment Incentive Pay

Assignment incentive pays are intended to provide monetary incentive in the assignment process to encourage service members to volunteer for difficult-to-fill or less desirable assignments, locations, or units. The military departments may disburse assignment incentive pays based on service-specific needs, primarily to include addressing personnel shortages and a unit's ability to meet mission requirements, according to DOD policy.[45] The Army, Navy, and Marine Corps are currently offering these pays to personnel in certain cyber career fields, but the Air Force is not offering these pays, according to officials.

- **Army.** The Army has offered both Special Duty Assignment Pay and Cyber Assignment Incentive Pay since fiscal year 2017, according to officials. Specifically, according to the U.S. Army Cyber School, Special Duty Assignment Pay is granted only for enlisted personnel

[43] According to Air Force data, from fiscal year 2017 through fiscal year 2021, a small percentage—from 7 percent to 2 percent of Air Force service members in these career fields—were awarded enlistment bonuses.

[44] MARADMINS 454/21, *FY22 Enlistment Incentive Programs* (Aug. 27, 2021).

[45] DODI 1340.26 defines "Special Duty Assignment Pay" as designed to recognize service members assigned duties determined to be extremely demanding, requiring a greater than normal degree of responsibility or difficulty or requiring special qualifications.

and ranges from $150 to $300 per month with dollar amounts based on experience levels. In contrast, officials said that Cyber Assignment Incentive Pay was initially only offered for three specific work roles. Army officials also stated that Cyber Assignment Incentive Pay is authorized for officers, warrant officers, and enlisted personnel. According to officials, in 2018 the Army expanded the pay to include any solider working in the Cyber Mission Force and from fiscal year 2017 through fiscal year 2021, awarded between $500 and $2,950 annually to personnel in the 25D career field.[46] In 2020, the Army expanded Cyber Assignment Incentive Pay to any soldier who is trained and certified in a USCYBERCOM or U.S. Army Cyber Command work role. The pay amounts are contingent upon experience levels. Beginning in fiscal year 2020, Cyber Assignment Incentive Pay ranged from $250 to $600 per month for Cyber Mission Force work roles. However, for critical work roles, such as ION, this pay ranged from $1,000 to $1,500 per month.

- **Navy.** The Navy offers Special Duty Assignment Pay to eligible cyber personnel, according to officials. Specifically, since 2017 the Navy has paid Special Duty Assignment Pay of $150 to $300 per month to personnel qualified to fill the ION work role.
- **Marine Corps.** The Marine Corps offers assignment incentive pay to enlisted personnel serving in cyber-related positions. Specifically, the Marine Corps has been paying assignment incentive pay since fiscal year 2020 to the 17XX career field, according to officials. In fiscal year 2020, the average pay was $336 per month, and in fiscal year 2021 the average pay was $364 per month.[47]

Retention Bonuses

Retention bonuses are used on a discretionary basis to retain personnel in specific work roles. The military services determine eligibility for these bonuses based on the overall health of a career field, for example, if the military services are generally staffing a career field near its authorized staffing level. There are two types of retention bonuses available to personnel in the cyber career fields. The Selective Reenlistment Bonus is a monetary incentive employed to encourage the reenlistment of sufficient

[46] In fiscal year 2017, no bonuses were awarded. The highest level of bonuses (i.e., $2,950 total for 10 people for the year) was awarded in fiscal year 2020.

[47] According to Marine Corps data, 141 service members received assignment incentive pay in fiscal year 2020, and 258 service members received this pay in fiscal year 2021.

numbers of qualified enlisted personnel in critical skills specialties with high training costs or demonstrated retention shortfalls. The other bonus, referred to as the Critical Skills Retention Bonus, provides an incentive for qualified enlisted and officer personnel with skills designated as critical to remain on active duty for key positions.[48]

The Army, Navy, Air Force, and Marine Corps have all offered retention bonuses for certain cyber career fields.

- **Army.** The Army awards retention bonuses to enlisted personnel. Specifically, the Army has offered retention bonuses to enlisted cyber operations specialists since 2017. While the number of personnel who accepted retention bonuses has generally declined since 2017, the amount of the bonuses has increased, according to Army data. For example, 100 Cyber Operations Specialists received $2.9 million in bonuses in fiscal year 2017 compared with fiscal year 2021 when 72 specialists received $3.5 million in bonuses. Also, the average bonus levels for personnel in the 17C career field have increased over time. U.S. Army Cyber Command officials explained that the Army was developing efforts to provide higher value bonuses to more advanced skill identifiers within a career field. In addition, the Army offered a small number of senior enlisted personnel in the 17C career field a written bonus agreement of either $60,000 for an additional 36-month active-duty commitment or $100,000 for a 48-month active-duty commitment.[49]
- **Navy.** Since 2017, the Navy has offered retention bonuses to both the Cryptologic Technicians Networks and IT enlisted cyber career fields, but Navy officials noted that the use of retention bonuses has varied over time. For example, retention bonuses were awarded to personnel in the IT cyber career field in fiscal years 2017 through 2021 with the exception of fiscal year 2019 when none were awarded. Navy officials

[48] The Army, Marine Corps, and Air Force refer to bonus moneys leveraged to entice personnel to continue service as a “Selective Retention Bonus,” and the Navy refers to them as a “Selective Reenlistment Bonus.” For clarity, we are using the term “retention bonuses” to refer to both Selective Reenlistment Retention Bonuses and Selective Retention Bonuses.

[49] Written bonus agreements are rare, according to officials. For example, in fiscal year 2020 only eight were awarded, compared with 74 standard retention bonuses for personnel in cyber career fields. According to Army officials, written bonuses are intended for personnel who are eligible for retirement at 20 years of service.

stated that retention bonuses can be as high as $100,000 for Cryptologic Technicians Networks and $60,000 for IT personnel.[50]

- **Air Force.** According to officials, the Air Force used retention bonuses to help fill cyber mission forces until they reached full operational capacity in 2018. However, the military service has continued to award retention bonuses. From 2017 through 2021 the Air Force decreased retention bonuses from $45 million in fiscal year 2017 to approximately $27 million in fiscal year 2021.
- **Marine Corps.** Use of retention bonuses began in fiscal year 2019 to help maintain the newly established 17XX career field, according officials. Specifically, these bonuses were used as incentives for marines to cross-train into and remain on active duty in these career fields.[51] These bonuses were from $29,000 to $53,000 for 4-year reenlistments in fiscal year 2022 for the 1711 and 1721 cyber career fields, a Marine Corps official told us. Officials noted that although the Marine Corps met its reenlistment goal for the 17XX career field in fiscal year 2022, it is keeping the bonuses in place given current staffing challenges discussed above.

[50] According to data provided by Navy officials, 1,192 service members in cyber work roles were awarded a total of about $11 million in retention bonuses in fiscal year 2021.

[51] The Marine Corps provided data in fiscal years 2019 through 2021, because, according to Marine Corps officials, the 17XX career field was not established until fiscal year 2018. From fiscal years 2019 through 2021, the Marine Corps awarded $19.4 million in retention bonuses to 304 marines.

Even with Special Pays, Cyber Personnel Retention Challenges Continue across All Services

The military services spent at least $160 million on cyber retention bonuses annually in fiscal years 2017 through 2021.[52] However, officials have acknowledged that while the military services offer retention bonuses and special pays, they continue to experience challenges retaining qualified cyber personnel. Per DOD guidance, the military services can determine how they use special pays.[53] DOD guidance regarding bonuses indicates that the military services provide special pays to attract and retain personnel when less costly methods have proven inadequate or impractical, and directs the military services to exercise this authority in the most cost-effective manner.[54] However, DOD and we have reported on the need for assessments of the cost-effectiveness of special pays.

In DOD's December 2020 *Thirteenth Quadrennial Review of Military Compensation*, DOD noted that for certain military career fields, including cyber, military pay falls behind pay in the civilian labor market, and special and incentive pays are among the tools used to help ensure that military pay is comparatively competitive.[55] DOD recommended a study to

[52] U.S. Army Cyber Command officials noted that money spent on retention bonuses is offset by the costs of recruitment, career field training, and work role training to replace military cyber personnel. For example, these officials noted that the replacement cost for a service member in the 17C career field who is certified to fill the ION work role is about $400,000, while the retention bonus offered to an individual with that training is $92,000 spread over 6 years.

[53] DOD Instruction 1304.31 provides parameters for how and under what circumstances the military services may use bonus pays for enlisted members. For example, the enlistment bonus for a designated military skill or the cumulative amount of enlistment bonuses for any individuals must not exceed $50,000 for a minimum 2-year service obligation. See DOD Instruction 1304.31, *Enlisted Bonus Program (Nov. 5, 2020).*

[54] DOD Instruction 1304.29, *Administration of Enlistment Bonuses, Accession Bonuses for New Officers in Critical Skills, Selective Reenlistment Bonuses, and Critical Skills Retention Bonuses for Active Members* (Dec. 15, 2004), (incorporating change July 11, 2016). According to this policy, for example, the military services are to use enlistment, accession, reenlistment, and retention bonuses as incentives to meet personnel requirements. The intent of bonuses is to influence personnel inventories in situations in which less costly methods have proven inadequate or impractical. Retention bonuses described by officials included Selective Reenlistment Retention Bonuses and Selective Retention Bonuses.

[55] Department of Defense, Report of the Thirteenth *Quadrennial Review of Military Compensation*, vol. 1 (Dec. 2020).

examine a more expansive view of military pay, including special and incentive pays that are targeted at recruitment and retention. According to DOD, including these types of pays in a compensation study could provide a better view of the relationship between compensation and recruiting and retention. As of August 2022, this effort was ongoing, according to officials.

In 2017, we reported, among other things, that the military services had largely applied key principles of effective human capital management in the design of the special and incentive pay programs for cybersecurity occupations.[56] We found, however, that, according to officials, DOD and the military services had not taken steps to fully ensure consistent application of the principles. For example, DOD had not reviewed whether it used special and incentive pays efficiently for recruitment and retention in selected high-skill occupations, including cybersecurity personnel. In the absence of measures for ensuring efficiency in special and incentive pay programs, DOD and the military services generally assessed their special and incentive pay programs' effectiveness by the extent to which they achieved desired staffing targets. However, this approach did not ensure that special and incentive pay programs were using resources in the most efficient manner, as DOD guidance requires.

As a result, we recommended that DOD, in coordination with the military services, review whether special and incentive pay programs had incorporated key principles of effective human capital management, and prioritize and complete the establishment of measures for the efficient use of resources. DOD partially concurred with this recommendation, but has not implemented it. We continue to believe that fully implementing this recommendation in the cyber career fields would help DOD determine the effectiveness of special and incentive pays in recruiting and retaining a highly skilled workforce. Specifically, until DOD implements this recommendation, DOD and the military services may lack assurance that

[56] GAO-17-39. The key principles are as follows: decision-making about human capital investment that is based largely on the expected improvement of agency results and is implemented in a manner that fosters top talent; consideration of replacement costs when deciding whether to invest in recruitment and retention programs; assessments of civilian supply, demand, and wages that inform updates to agency plans as needed; approaches that are tailored to meet organizational needs by identifying and evaluating unique staffing issues; current and historical retention data that are collected and reviewed to evaluate the effects and performance of human capital investments; and opportunities for improvement that are identified and incorporated into planning cycles.

special and incentive pay programs are effective and that resources are optimized for the greatest return on investment.

Conclusions

DOD's ability to sustain a ready cyber workforce is critical to help ensure the department can protect its networks, IT systems, and data. Moreover, DOD has stated that it plans to significantly increase the size of its cyber forces in the coming years. In addition to the competition DOD faces for people with these cyber skills in the private sector and from other federal government agencies, the department faces challenges that may hinder its efforts to grow this workforce. Specifically, two of the four military services are not positioned to ensure adequate return on their investment in lengthy and expensive cyber training. Personnel who complete training to fill the ION work role—which may take a year or more and costs the department hundreds of thousands of dollars—may not remain in the military to use those skills for a significant length of time after training. While the Air Force and Navy have set service obligations for ION training, Army service members incur a shorter service obligation and Marine Corops service members do not incur an obligation at all for ION training. Without updating or issuing new guidance to specify service obligation lengths, the Army and the Marine Corps are unable to ensure they receive an adequate return on their investment for ION training.

DOD's visibility over its ability to fill key work roles as part of the cyber mission force is hindered because the military services, with the exception of the Navy, do not track staffing levels by work role. USCYBERCOM uses work roles to assign personnel from the military services to cyber mission teams. While the Navy's personnel system is equipped to track data by work roles, Army, Air Force, and Marine Corps systems are not. As a result, the Army, Air Force, and Marine Corps may not be equipped to identify staffing gaps and project staffing needs for critical work roles.

By addressing the issues we have identified, DOD will be better positioned to recruit and retain a knowledgeable and skilled military cyber workforce in the face of increased competition from across the private and public sectors for this workforce's skills, as well as in the face of recruitment challenges across the department.

Recommendations for Executive Action

We are making a total of six recommendations, including three to the Secretary of the Army, two to the Secretary of the Navy, and one to the Secretary of the Air Force. Specifically:

The Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 614-200 in a timely manner to clearly define active-duty service obligations for ION training, for the Army's relevant cyber enlisted personnel. (Recommendation 1)

The Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 350-100 in a timely manner to clearly define active-duty service obligations for ION training, for the Army's relevant cyber officers. (Recommendation 2)

The Secretary of the Navy should ensure that the Commandant of the Marine Corps develops guidance in a timely manner to establish active-duty service obligations for ION training. (Recommendation 3)

The Secretary of the Army should ensure that the Chief of Staff of the Army takes the necessary steps to integrate U.S. Cyber Command work roles into the Army's personnel system of record to track cyber personnel data by work role. (Recommendation 4)

The Secretary of the Air Force should ensure that the Chief of Staff of the Air Force takes the necessary steps to integrate U.S. Cyber Command work roles into the Air Force's personnel system of record to track cyber personnel data by work role. (Recommendation 5)

The Secretary of the Navy should ensure that the Commandant of the Marine Corps takes the necessary steps to integrate U.S. Cyber Command work roles into the Marine Corps' personnel system of record to track cyber personnel data by work role. (Recommendation 6)

Agency Comments

We provided a draft of this report to DOD for review and comment. In its written comments, included in appendix II, DOD concurred with the recommendations. DOD also 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 Army, the Secretary of the Navy, the Secretary of the Air Force, and the Commandant of the Marine Corps. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or members of your staff have any questions regarding this report, please contact me at (202) 512-3604 or farrellb@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 III.

Brenda S. Farrell

Brenda S. Farrell
Director, Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

This report examines the extent to which (1) a service obligation exists for military cyber personnel receiving advanced cyber training, (2) the Department of Defense (DOD) has experienced staffing gaps for active-duty military cyber personnel for fiscal year 2017 through fiscal year 2021 and tracked cyber work roles, and (3) the military services have used special and incentive pays since fiscal year 2017 to address any recruiting and retention challenges.[1]

For our first objective, we reviewed federal law, DOD and military service guidance related to the implementation of service obligations for military cyber personnel.[2] We interviewed military service officials about how they implement personnel guidance and what can affect the length of service obligations, such as training, permanent changes of station, or special pays. USCYBERCOM identified three critical work roles: Interactive On-Net Operator (ION), Capabilities Developer, and Exploitation Analyst. Further, DOD and military service officials identified the advanced cyber training to fill the ION work role as resource-intensive and lengthy.

[1] DOD Instruction 1304.29 states that it is DOD policy that the military services use enlistment, accession, reenlistment, and retention bonuses (what we refer to as “special and incentive pays” in this report) as monetary incentives to influence personnel levels. Each military service sets its own policies for when to award special pays and how much to award.

[2] Section 651 of title 10 of the United States Code provides that, with certain exceptions, each person who becomes a member of an armed force shall serve in the armed force for a total initial period of not less than 6 years or more than 8 years, as provided in regulations prescribed by the Secretary of Defense for the services under his/her jurisdiction (or, in the case of the Coast Guard when it is not operating as a service in the Navy, regulations prescribed by the Secretary of Homeland Security). DOD Instruction 1304.25, *Fulfilling the Military Service Obligation* (Oct. 13, 2021) states that all officers and enlisted personnel incur a military service obligation of 8 years from their date of entry and directs the Secretaries of the military departments to establish procedures for fulfilling the military service obligation. The military services use a variety of terms to refer to active-duty service commitments associated with entry into the military or with events such as training, promotions, or assignments. For simplicity, we refer to these as active-duty service obligations throughout this report.

Accordingly, this report focuses on service obligations related to that training.

We determined that the control environment component of internal control was relevant to this objective.[3] Specifically, we identified the underlying principles that management should remediate deficiencies by, for example, completing and documenting corrective actions to remediate internal control deficiencies on a timely basis, and should implement control activities through policies. Additionally, our prior work identified key principles of human capital management, including that agencies should make targeted investment in employees, and that decisions about such investments should be based largely on expected improvement in agency results.[4] We assessed DOD and military service guidance related to service obligations to determine the extent to which they met these principles. In addition, we compared the information we gathered from our review of DOD and military service guidance and interviews with DOD and military service guidance to assess the extent to which service obligations aligned with existing guidance.[5]

For our second objective, we evaluated the extent to which DOD has experienced staffing gaps for active-duty military cyber personnel. To do this, we selected specific military career fields related to the cyber force by working with the military services, their personnel offices, and career field managers to determine which career fields are primarily cyber in their function.[6] See table 2 for a list of the cyber career fields identified and included in our review.

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

[4] GAO, *A Model of Strategic Human Capital Management,* GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

[5] DOD Instruction 1304.25, *Fulfilling the Military Service Obligation* (Oct. 13, 2021); Army Regulation 350-100, *Training: Officer Active Duty Service Obligations* (Sept. 26, 2017); and Army Regulation 614-200, *Assignments, Details and Transfers: Enlisted Assignments and Utilization Management* (Jan. 25, 2019).

[6] Military career fields are referred to differently by each military service. In the Army, career fields are referred to as Military Occupational Specialties; in the Air Force, as Air Force Specialty Codes; in the Navy, as Navy Ratings (enlisted) or Designator (officer); and in the Marine Corps, as Primary Military Occupational Specialties. For the purposes of this report, we use the term military career field to refer to these positions. See the background section of this report for a full list of career fields selected from each military service.

Table 2: Military Cyber Career Fields Reviewed by GAO

Military service	Career field designation	Career field title
Army	17A	Cyber Warfare Officer (officer)
	17C	Cyber Operations Specialist (enlisted)
	170A	Cyber Warfare Technician (warrant officer)
	255S	Information Protection Technician (warrant officer)
	25D	Cyber Network Defender (enlisted)
Navy	1810	Cryptologic Warfare (officer)
	1820	Cyberspace Information/Information Professional (officer)
	1840	Cyber Warfare Engineer (officer)
	7820	Information Systems Technical (warrant officer)
	7840	Cyber Warrant Officer (warrant officer)
	CTN	Cryptologic Technician-Networks (enlisted)
	IT	Information Systems Technician (enlisted)
Marine Corps	1702	Cyberspace Officer (officer)
	1705	Cyberspace Warfare Development Officer (officer)
	1710	Offensive Cyberspace Warfare Officer (warrant officer)
	1711	Offensive Cyberspace Exploitation Operator (enlisted)
	1720	Defensive Cyberspace Warfare Officer (warrant officer)
	1721	Cyber Defensive Operator (enlisted)
	1799	Cyberspace Operations Chief (enlisted)
Air Force	17D	Warfighter Communications Operations Officer (officer)
	17S	Cyberspace Effects Operations Officer (officer)
	1B4X1	Cyber Warfare Operations (enlisted)
	1N4X1A	Cyber Intelligence Analyst (enlisted)
	3D0X2	Cyber Systems Operations (enlisted)
	3D0X4	Computer Systems Programming (enlisted)

Source: GAO analysis of Department and military service information. | GAO-23-105423

Note: Effective fiscal year 2022, the Army established the career field 17D, Cyber Capabilities Development Officer. Some cyber personnel previously in the 17A, Cyber Warfare Officer career field were recoded to this new career field. The Army also established the career field 170D, Cyber Capabilities Developer Technician, which included some cyber personnel previously in the 170A, Cyber Warfare Technician career field. Air Force officials stated that the 3D0X2 and 3D0X4 have been updated to 1D7X1B, Cyber Systems Operations and 1D7X1Z, Software Development Operation respectively.

Next, we collected and analyzed data on current staffing, authorizations, and military service-specific goals for the included career fields for fiscal years 2017 through 2021—the most recent years for which complete data were available across the military services.[7] Specifically, we created a data collection instrument to collect information on career field and work role retention rates, staffing levels, and available special pays. We compared staffing levels for cyber career fields against service authorizations. Finally, we compared the information with our review of military service data, DOD guidance, and interviews with DOD to determine if the military services were collecting and tracking data on cyber work roles.[8]

For our third objective, we identified which special and incentive pays the military services used to help recruit and retain cyber personnel for fiscal years 2017 through 2021—the most recent years for which data were available. We interviewed officials from the military services on how special and incentive pays for cyber personnel are used to address retention challenges. Further, we reviewed military service data for special and incentive pays offered in fiscal years 2017 through 2021. We also reviewed the extent to which DOD has taken steps to implement prior recommendations related to special and incentive pays directed at military cyber personnel.[9]

We assessed the reliability of the data we collected on staffing, authorizations, and special and incentive pay options by reviewing the data for completeness and interviewing officials knowledgeable about the implementation of the data systems. We found these data to be sufficiently reliable for comparing staffing levels for cyber personnel against service authorizations, and for understanding the types of special pays and amount offered to cyber personnel.

[7] Staffing goals by military services vary and are not documented in guidance. Officials from the respective military services stated that the staffing goal for the Navy was 98 percent, the Marine Corps was 85 percent, and the Army was 85 percent. The Air Force did not report having a specific staffing goal for cyber personnel. For consistency in our analysis of the military services, we applied 80 percent as a threshold for identifying staffing gaps. Further, our prior work identified 80 percent as a minimum threshold for staffing personnel who perform maintenance work at DOD depots. See GAO, *DOD Depot Workforce: Services Need to Assess the Effectiveness of Their Initiatives to Maintain Critical Skills*, GAO-19-51 (Washington, D.C.: Dec. 14, 2018).

[8] DOD Instruction 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements* (Dec. 21, 2021).

[9] GAO, *Military Compensation: Additional Actions Are Needed to Better Manage Special and Incentive Pay Programs,* GAO-17-39 (Washington, D.C.: Feb. 3, 2017).

For all three objectives, we conducted interviews with DOD and military service personnel in the Army, Navy, Marine Corps, and Air Force to gather information about topics covered in this review.[10] See table 3 for the organizations contacted for this review.

Table 3: Department of Defense Organizations Contacted by GAO for This Review

Organization	Offices and installations contacted
Department of Defense	• Under Secretary of Defense for Personnel and Readiness • Office of the Chief Information Officer • Office of the Principal Cyber Advisor • U.S. Cyber Command
Department of the Army	• U.S. Army Cyber Command • U.S. Army Signal School • U.S. Army Human Resources Command • Office of the Deputy Chief of Staff, G-1 Personnel • U.S. Army Training and Doctrine Command • U.S. Army Cyber Center of Excellence • U.S. Army Intelligence Center of Excellence
Department of the Navy	• Office of the Navy Principal Cyber Advisor • Office of the Deputy Chief of Naval Operations for Information Warfare) • Bureau of Naval Personnel • Navy Personnel Command Career Management Pillar
United States Marine Corps	• Office of the Deputy Commandant for Information (DC I) • DC I Information Maneuver Division • Office of Manpower and Reserve Affairs (M&RA) • M&RA Manpower Military Policy Branch
Department of the Air Force	• Office of the Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations • Air Education and Training Command • Office of the Deputy Chief of Staff for Manpower, Personnel and Services • Air Force's Personnel Center • Air Force's Cyber (16th Air Force)

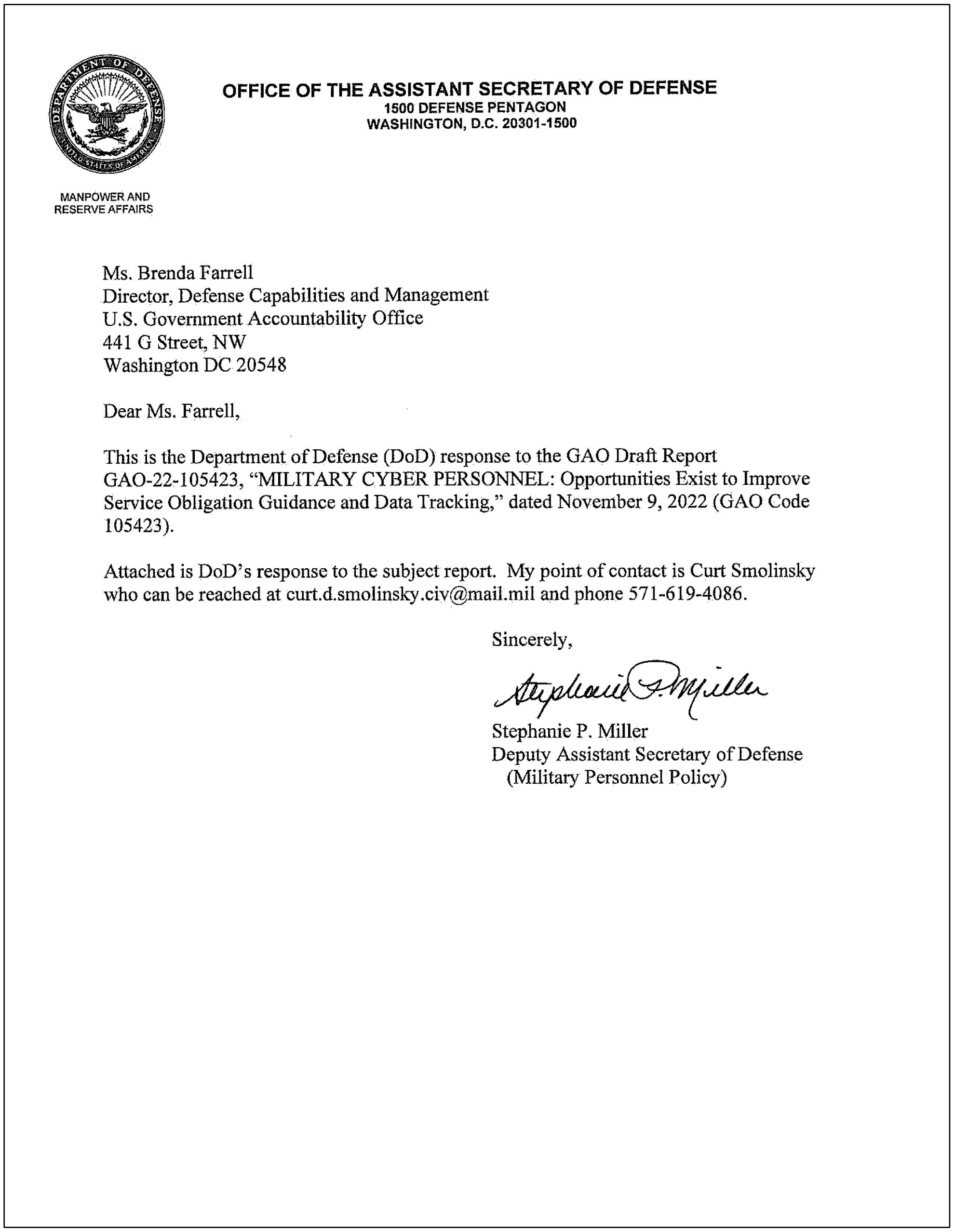
Source: GAO. | GAO-23-105423

We conducted this performance audit from September 2021 to December 2022 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

[10] We did not include the Space Force or the Coast Guard in this review because they do not currently provide cyber personnel to U.S. Cyber Command to fill cyber mission team positions.

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
1500 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1500

MANPOWER AND
RESERVE AFFAIRS

Ms. Brenda Farrell
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Farrell,

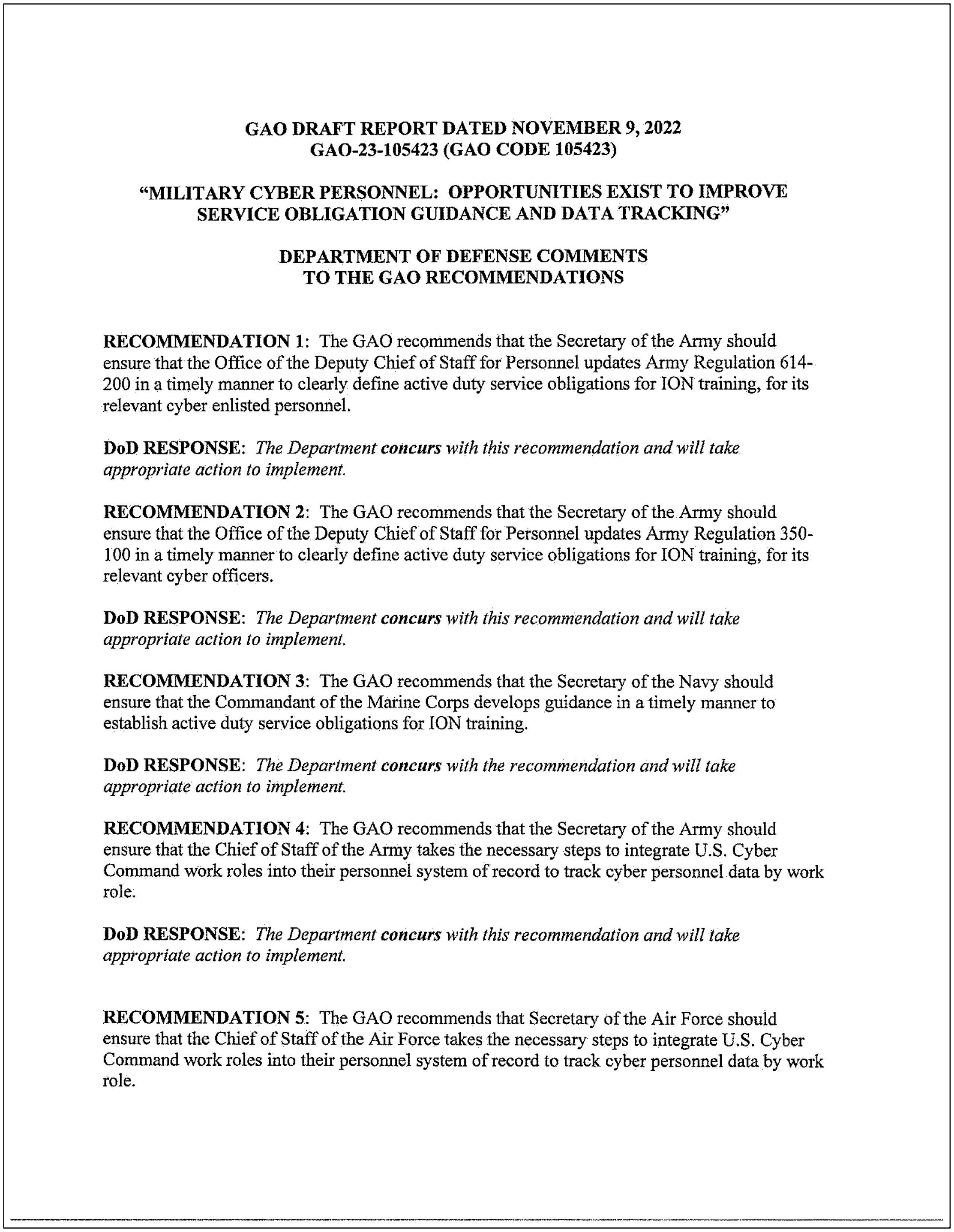
This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-105423, "MILITARY CYBER PERSONNEL: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking," dated November 9, 2022 (GAO Code 105423).

Attached is DoD's response to the subject report. My point of contact is Curt Smolinsky who can be reached at curt.d.smolinsky.civ@mail.mil and phone 571-619-4086.

Sincerely,

Stephanie P. Miller

Stephanie P. Miller
Deputy Assistant Secretary of Defense
(Military Personnel Policy)



GAO DRAFT REPORT DATED NOVEMBER 9, 2022
GAO-23-105423 (GAO CODE 105423)

"MILITARY CYBER PERSONNEL: OPPORTUNITIES EXIST TO IMPROVE SERVICE OBLIGATION GUIDANCE AND DATA TRACKING"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 614-200 in a timely manner to clearly define active duty service obligations for ION training, for its relevant cyber enlisted personnel.

DoD RESPONSE: *The Department **concurs** with this recommendation and will take appropriate action to implement.*

RECOMMENDATION 2: The GAO recommends that the Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 350-100 in a timely manner to clearly define active duty service obligations for ION training, for its relevant cyber officers.

DoD RESPONSE: *The Department **concurs** with this recommendation and will take appropriate action to implement.*

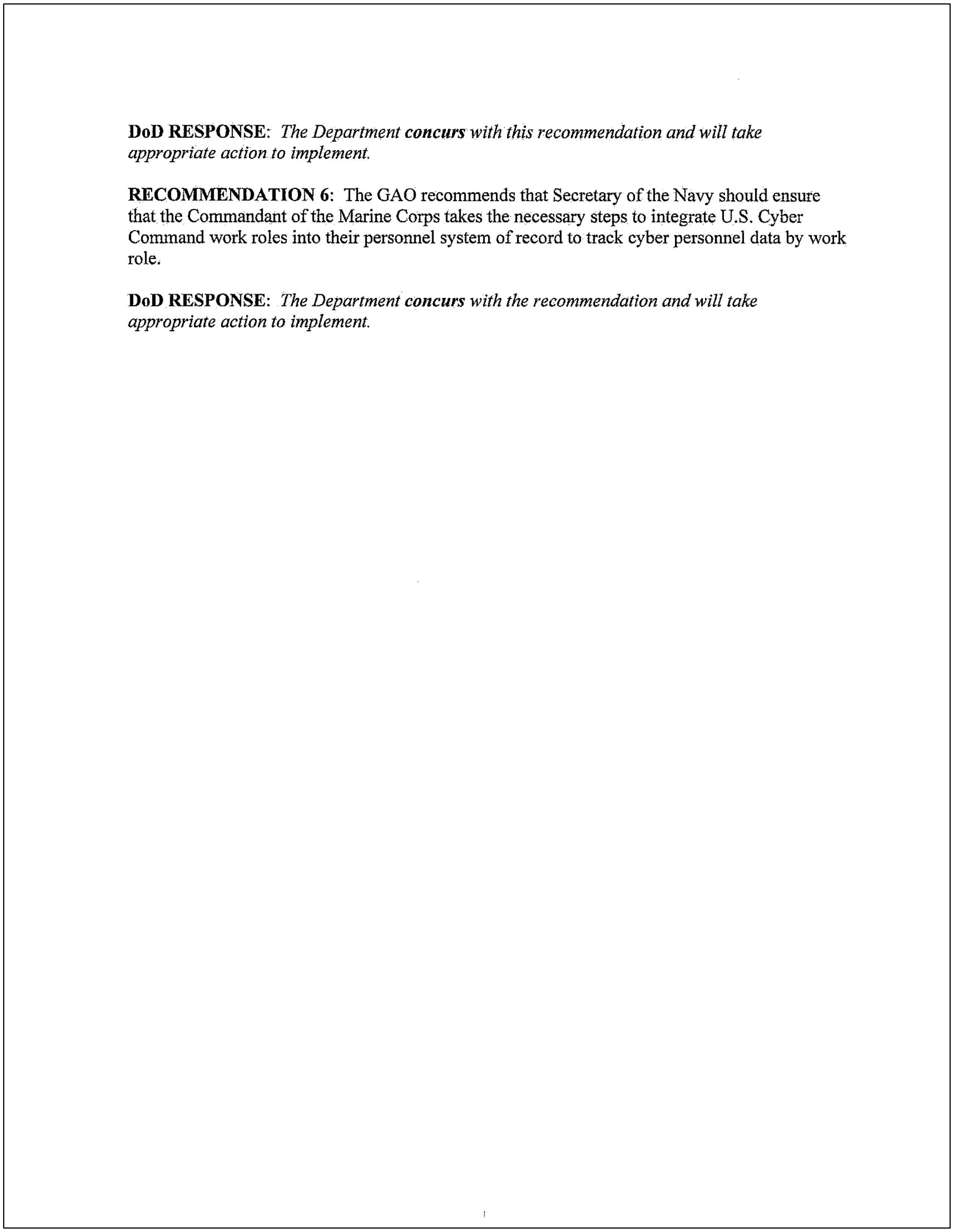
RECOMMENDATION 3: The GAO recommends that the Secretary of the Navy should ensure that the Commandant of the Marine Corps develops guidance in a timely manner to establish active duty service obligations for ION training.

DoD RESPONSE: *The Department **concurs** with the recommendation and will take appropriate action to implement.*

RECOMMENDATION 4: The GAO recommends that the Secretary of the Army should ensure that the Chief of Staff of the Army takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.

DoD RESPONSE: *The Department **concurs** with this recommendation and will take appropriate action to implement.*

RECOMMENDATION 5: The GAO recommends that Secretary of the Air Force should ensure that the Chief of Staff of the Air Force takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.



DoD RESPONSE: *The Department **concurs** with this recommendation and will take appropriate action to implement.*

RECOMMENDATION 6: The GAO recommends that Secretary of the Navy should ensure that the Commandant of the Marine Corps takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.

DoD RESPONSE: *The Department **concurs** with the recommendation and will take appropriate action to implement.*

Agency Comment Letter

Text of Appendix II: Comments from the Department of Defense

Ms. Brenda Farrell
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Farrell,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-105423, "MILITARY CYBER PERSONNEL: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking," dated November 9, 2022 (GAO Code 105423).

Attached is DoD's response to the subject report. My point of contact is Curt Smolinsky who can be reached at curt.d.smolinsky.civ@mail.mil and phone 571-619-4086.

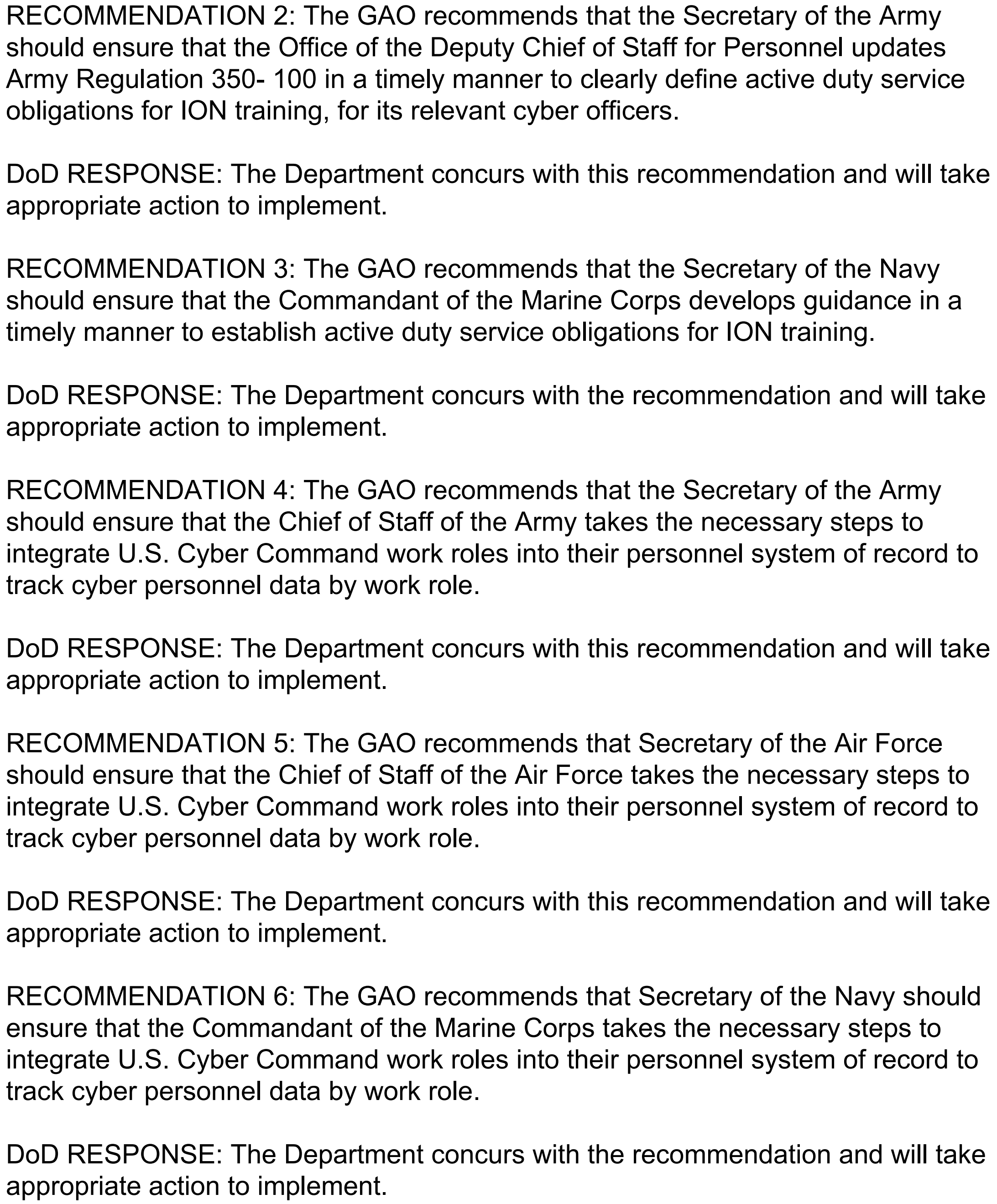
Sincerely,

Stephanie P. Miller
Deputy Assistant Secretary of Defense
(Military Personnel Policy)

GAO DRAFT REPORT DATED NOVEMBER 9, 2022 GAO-23-105423 (GAO CODE 105423)
"MILITARY CYBER PERSONNEL: OPPORTUNITIES EXIST TO IMPROVE SERVICE OBLIGATION GUIDANCE AND DATA TRACKING"
DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 614- 200 in a timely manner to clearly define active duty service obligations for ION training, for its relevant cyber enlisted personnel.

DoD RESPONSE: The Department concurs with this recommendation and will take appropriate action to implement.



RECOMMENDATION 2: The GAO recommends that the Secretary of the Army should ensure that the Office of the Deputy Chief of Staff for Personnel updates Army Regulation 350- 100 in a timely manner to clearly define active duty service obligations for ION training, for its relevant cyber officers.

DoD RESPONSE: The Department concurs with this recommendation and will take appropriate action to implement.

RECOMMENDATION 3: The GAO recommends that the Secretary of the Navy should ensure that the Commandant of the Marine Corps develops guidance in a timely manner to establish active duty service obligations for ION training.

DoD RESPONSE: The Department concurs with the recommendation and will take appropriate action to implement.

RECOMMENDATION 4: The GAO recommends that the Secretary of the Army should ensure that the Chief of Staff of the Army takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.

DoD RESPONSE: The Department concurs with this recommendation and will take appropriate action to implement.

RECOMMENDATION 5: The GAO recommends that Secretary of the Air Force should ensure that the Chief of Staff of the Air Force takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.

DoD RESPONSE: The Department concurs with this recommendation and will take appropriate action to implement.

RECOMMENDATION 6: The GAO recommends that Secretary of the Navy should ensure that the Commandant of the Marine Corps takes the necessary steps to integrate U.S. Cyber Command work roles into their personnel system of record to track cyber personnel data by work role.

DoD RESPONSE: The Department concurs with the recommendation and will take appropriate action to implement.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Brenda S. Farrell, (202) 512-3604 or farrellb@gao.gov

Staff Acknowledgments

In addition to the contact named above, Lori Atkinson (Assistant Director), James Krustapentus (Analyst in Charge), Ava E. H. Bagley, Tracy Barnes, Sara Brinegar, Molly Callaghan, Chad Hinsch, Mae F. Jones, Angela Kaylor, Amie Lesser, Lillian I. Ofili, and Michael Silver made significant 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