December 2022

MILITARY CYBER PERSONNEL

Opportunities Exist to Improve Service Obligation Guidance and Data Tracking

GAO Highlights

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

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).

United States Government Accountability Office