GAO

Highlights

Highlights of GAO-24-106879, a report to congressional committees

May 2024

CYBER PERSONNEL

Navy Needs to Address Accuracy of Workforce Data

Why GAO Did This Study

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

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

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

What GAO Recommends

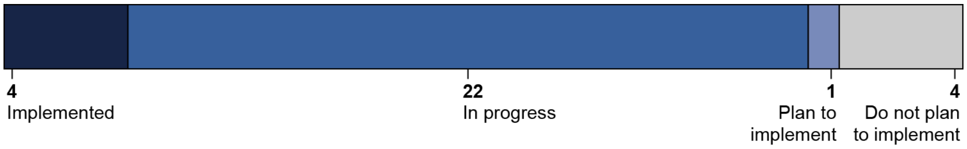
GAO continues to maintain that DOD should fully implement the 2019 priority recommendation to review work roles and position descriptions for accuracy (*see* GAO-23-106305).

View GAO-24-106879. For more information, contact Joe Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

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

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



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

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

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

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