GAO Highlights

Highlights of GAO-22-105208, a report to congressional committees

September 2022

COAST GUARD

Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands

Why GAO Did This Study

The Coast Guard, a multi-mission, maritime military service within the Department of Homeland Security (DHS), is responsible for ensuring the safety and security of the nation's maritime transportation system and maritime borders. It established cyberspace as an operational domain in 2015 to help protect the marine transportation system from threats. Such threats could be delivered through the internet, telecommunications networks, and computer systems.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to review issues related to the Coast Guard's cyberspace workforce. This report addresses the extent the Coast Guard has (1) identified its cyberspace workforce and determined its associated mission needs and (2) implemented selected leading practices in its cyberspace workforce recruitment, retention, and training. We selected the leading practices by reviewing those identified in relevant GAO reports and federal guidance. GAO analyzed Coast Guard documentation and data and interviewed cognizant Coast Guard officials.

What GAO Recommends

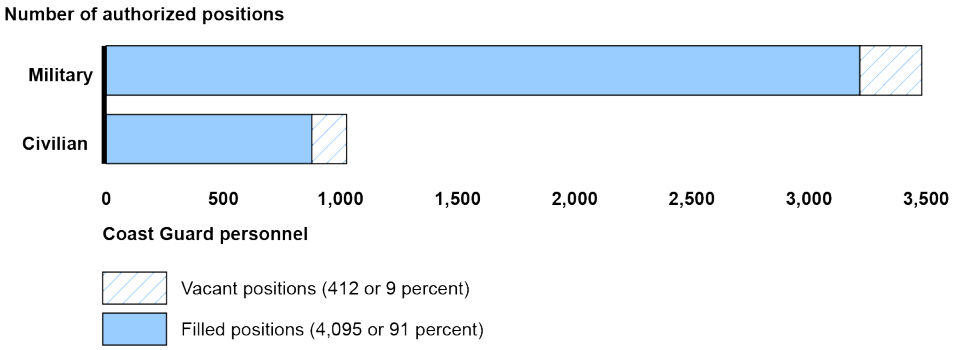
GAO is making six recommendations to the Coast Guard including to determine the cyberspace staff needed to meet its mission demands and fully implement five recruitment and retention leading practices, such as establishing a strategic workforce plan for its cyberspace workforce. DHS concurred with these recommendations.

View GAO-22-105208. For more information, contact Heather MacLeod at (202) 512-8777 or macleodh@gao.gov or David Hinchman at (214) 777-5719 or hinchmand@gao.gov.

What GAO Found

The Coast Guard is increasingly dependent upon its cyberspace workforce to maintain and protect its information systems and data from threats. As of September 2021, the Coast Guard determined it had 4,507 authorized cyberspace workforce positions (i.e., funded positions that could be vacant or filled), consisting of military and civilian personnel.

Authorized Coast Guard Cyberspace Positions, Filled and Vacant, as of September 2021



Source: GAO analysis of Coast Guard data. | GAO-22-105208

Coast Guard guidance calls for the service to use its Manpower Requirements Determination process to assess and determine necessary staffing levels and skills to meet mission needs. However, GAO found that the service had not used this process for a large portion of its cyberspace workforce. For example, as of February 2022, the Coast Guard had not used this process for three headquarters units that collectively represent 55 percent of its cyberspace workforce positions. Until such analysis is completed, the Coast Guard will not fully understand the resources it requires, including those to protect its information systems and data from threats.

Of 12 selected recruitment, retention, and training leading practices, the Coast Guard fully implemented seven, partially implemented three, and did not implement two. By fully implementing these leading practices, the Coast Guard could better manage its cyberspace workforce. For example, it has not developed a strategic workforce plan for its cyberspace workforce. According to leading recruitment practices, such a plan should include three elements: (1) strategic direction, (2) supply, demand, and gap analyses, and (3) solution implementation, along with monitoring the plan's progress to address all cyberspace competency and staffing needs. Without having such a plan, the Coast Guard will likely miss opportunities to recruit for difficult to fill cyberspace positions.