July 2022

COAST GUARD

Actions Needed to Enhance IT Program Implementation

GAO Highlights

Highlights of GAO-22-105092, a report to congressional committees

Why GAO Did This Study

The U.S. Coast Guard, a component of the Department of Homeland Security, relies extensively on IT systems and services to carry out its 11 statutory missions. It also relies on operational technology, which encompasses a broad range of programmable systems or devices that interact with the physical environment, such as sensors and radar. Historically, the Coast Guard has had longstanding issues managing its technology resources. As such, it plans to spend $93 million to improve the reliability and performance of these resources in fiscal year 2022.

The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* included a provision for GAO to review several aspects of the Coast Guard's IT program. This report addresses, among other things, the extent to which the Coast Guard (1) has a process to plan for network capacity; (2) has cybersecurity risk management processes for IT and for operational technology; and (3) has incorporated federal requirements in its strategy for cloud computing.

To do so, GAO evaluated the Coast Guard's IT policies and procedures against common practices for network capacity planning. GAO also analyzed the Coast Guard's cybersecurity processes for IT and operational technology and assessed their application. Further, it assessed the cloud strategy and other related documentation against federal requirements and guidance.

What GAO Recommends

GAO is making eight recommendations to improve the Coast Guard's IT program implementation. The Department of Homeland Security agreed with all eight recommendations.

View GAO-22-105092. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

What GAO Found

The U.S. Coast Guard lacks a documented network capacity planning process. Network capacity planning is an important aspect of IT infrastructure planning that involves determining the network resources required to support an entity's mission. However, the Coast Guard uses an ad hoc process that does not fully align with five common practices GAO identified for network capacity. The table below describes the extent to which it implemented the practices. Without fully implementing these practices, the Coast Guard faces significant risks in resulting inefficiencies and disruptions in network availability to users.

Extent to Which Coast Guard Implemented Network Capacity Planning Practices

Common Practices	Implementation Status
Compile an inventory of hardware, software, and configurations	◑
Identify the baseline network utilization and traffic growth predictions	◑
Determine bandwidth allocation needs for variations and prioritize network traffic	◑
Run simulations and perform analyses of network usage	○
Make refinements to the network and continually monitor the health of the infrastructure	◑

Legend:
● = addressed: The Coast Guard demonstrated that it had fully implemented the practice; ◑ = partially addressed: The Coast Guard demonstrated that it implemented some, but not all of the practice; and ○= not addressed: The Coast Guard could not demonstrate that it had implemented the practice.

Source: GAO analysis of U.S. Coast Guard documentation and industry publications. | GAO-22-105092

In accordance with the January 2017 agreement between the Department of Homeland Security and Department of Defense (DOD), the Coast Guard is to follow DOD's Risk Management Framework. This framework establishes two different cybersecurity risk management processes for identifying and applying cybersecurity controls for IT and for operational technology resources. However, the Coast Guard did not consistently apply the framework for its operational technology. This inconsistency is due in part to the lack of a comprehensive and accurate inventory. In addition, it lacks a cybersecurity risk management process for two types of operational technology—industrial control systems and supervisory control and data acquisition systems. Without a consistently applied process, accurate inventory, and coverage for all systems, the Coast Guard cannot ensure effective management of cybersecurity risks.

In March 2021, the Coast Guard issued a cloud strategy that outlines its strategic objectives for cloud computing over the next five years. The cloud strategy and associated relevant documentation incorporated most federal cloud requirements and guidance. However, the Coast Guard did not address key actions related to security and its workforce. Updating its strategy to include all cloud-related requirements and guidance would further facilitate the migration to cloud services.