GAO Highlights

Highlights of GAO-23-106031, a report to congressional committees

May 2023

CYBERSECURITY

DOT Defined Roles and Responsibilities, but Additional Oversight Needed

Why GAO Did This Study

DOT was established in part to build, maintain, and oversee a vast national transportation system. To support its mission, the department relies on information systems to secure sensitive information.

The Infrastructure Investment and Jobs Act includes a provision for GAO to report on the cybersecurity roles and responsibilities of senior IT officials at DOT and its component operating administrations.

This report examines the extent to which DOT (1) has defined cybersecurity roles and responsibilities for department and component agency senior officials and managers; (2) provides cybersecurity support to components, and (3) provides oversight of component cybersecurity activities and managers.

To do so, GAO analyzed department policies, processes, and documentation. It also reviewed federal guidance and GAO and IG reports, and interviewed cognizant officials.

What GAO Recommends

GAO is making three recommendations to DOT to use annual reviews to address prior IG cybersecurity recommendations in areas such as training; ensure that senior managers' performance plans include cybersecurity-related expectations; and ensure that the DOT CIO be involved in evaluating component CIOs' performance. DOT concurred with the recommendations.

View GAO-23-106031. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Consistent with federal guidance, U.S. Department of Transportation (DOT) policy documents cybersecurity roles and responsibilities for senior officials. The policy also describes roles and responsibilities for senior managers at the nine component mission-oriented operating administrations (see figure).

Department of Transportation (DOT) Mission-Oriented Operating Administrations

Source: DOT, images: ipopba/stock.adobe.com, davooda/stock.adobe.com, EvrenKalinbacak/stock.adobe.com. | GAO-23-106031

DOT's Office of the Chief Information Officer (CIO) regularly communicates with component agencies by sharing information through daily cyber operations meetings and periodic informational emails. Further, component agency managers stated that the office provides access to cybersecurity tools for incident and vulnerability management and other technical assistance. DOT also supported managers by providing cybersecurity role-based training. However, the DOT Inspector General (IG) reported deficiencies in the clarity of training requirements, such as the required number of hours, and the monitoring of training completion. The IG's 2019 and 2021 recommendations to address these deficiencies are not yet implemented.

To provide oversight, DOT policy requires annual reviews of component agency cybersecurity programs. However, the reviews have not been effective in taking needed actions to implement the 63 unresolved cybersecurity recommendations as reported by the IG in a September 2022 report. Using the reviews to address the recommendations could improve the department's cybersecurity program.

To assess managers' performance, DOT established performance plans for its component agency senior IT managers. However, while DOT's strategic plan identified cybersecurity as an organizational objective, 15 of 18 managers' performance plans did not include cybersecurity-related expectations. Further, the department CIO did not always participate in evaluating the performance of component agency CIOs. This is inconsistent with department regulations and results in less assurance that component agencies are aligned with the department in carrying out cybersecurity-related responsibilities.