GAO Highlights

Highlights of GAO-25-107244, a report to congressional committees

February 2025

COAST GUARD

Additional Efforts Needed to Address Cybersecurity Risks to the Maritime Transportation System

Why GAO Did This Study

The Maritime Transportation System (MTS) is an essential critical infrastructure subsector, handling more than $5.4 trillion in goods and services annually. As the lead risk management agency for the subsector, the Coast Guard is to protect the system from all threats, including those related to cybersecurity.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for GAO to review cybersecurity risks to the MTS, including vessels and facilities. This report addresses (1) cybersecurity risks to the MTS, Coast Guard's efforts to (2) assist and oversee MTS owner and operator actions on cyber risks, (3) strategic planning to mitigate these risks, and (4) implementation of leading practices on cyber workforce competencies.

GAO reviewed federal and industry reports on MTS cybersecurity risks; federal statutes and regulations; and Coast Guard documentation and inspection data from fiscal year 2019 through June 2024. GAO also interviewed federal and non-federal stakeholders at four ports based on volume of trade, geographic dispersion, and other factors.

What GAO Recommends

GAO is making five recommendations, including that Coast Guard (1) update its system of record to provide ready access to complete cyber deficiency data, (2) ensure its cyber strategy and plans align with all key characteristics of a national strategy, and (3) analyze, assess, and address workforce competency gaps. The Department of Homeland Security concurred with GAO's recommendations.

For more information, contact Tina Won Sherman at (202) 512-8777 or ShermanT@gao.gov or Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov.

What GAO Found

The Maritime Transportation System (MTS) faces significant and increasing cybersecurity risks including:

- **Threat actors**. China, Iran, North Korea, Russia, and transnational criminal organizations pose the greatest cyber threats to the MTS.
- **Vulnerabilities**. MTS facilities and vessels increasingly rely on technology that is vulnerable to cyberattacks.
- **Impacts.** According to federal and nonfederal officials, cyber incidents have affected port operations, and the potential impacts of future incidents could be severe.

To help address these risks, the Coast Guard assists MTS owners and operators through offering direct technical assistance, providing voluntary guidelines for implementing cybersecurity practices, and sharing cyber threat information. The service also provides oversight through facility and vessel inspections, including the identification and documentation of cybersecurity-related deficiencies. However, Coast Guard cannot readily access complete information on inspection results specific to cybersecurity from its system of record (Marine Information for Safety and Law Enforcement). Updating its system to provide ready access to complete information on all cybersecurity-related deficiencies would help the Coast Guard better provide oversight of owners and operators and help position the service to prevent cyberattacks that could impact the MTS.

Although the Coast Guard developed a cyber strategy to address MTS cybersecurity risks, it did not fully address all of the key characteristics needed for an effective national strategy. Specifically, the cyber strategy fully addressed the key characteristic related to purpose, scope, and methodology, but did not fully address the other four characteristics, as shown in the table below. Addressing all of the key characteristics would better position the Coast Guard to ensure its actions and resources are addressing the highest cybersecurity risks.

GAO Assessment of How Coast Guard's Cyber Strategy Addresses Key National Strategy Characteristics

Characteristic	GAO assessment
Purpose, scope, and methodology	●
Problem definition and risk assessment	◑
Goals, subordinate objectives, activities, and performance measures	◑
Resources and investments	◑
Roles, responsibilities, and coordination	◑

Legend: ● Fully addresses ◑ Partially addresses. ○ Does not address.

Source: GAO analysis of Coast Guard's strategy and accompanying plans. | GAO-25-107244

Further, the Coast Guard has not fully addressed leading practices to ensure its cyber workforce has the competencies needed to address MTS cybersecurity risks. Specifically, the Coast Guard has not fully developed competency requirements. In addition, the Coast Guard has not fully assessed and addressed competency gaps for its cyber workforce. Until it does, the Coast Guard will not have assurance it is effectively mitigating cybersecurity risks to the MTS.