Cybersecurity Risks to the Maritime Transportation System

Marisol Cruz Cain April 15, 2025

Source: Yellow Boat/stock.adobe.com.

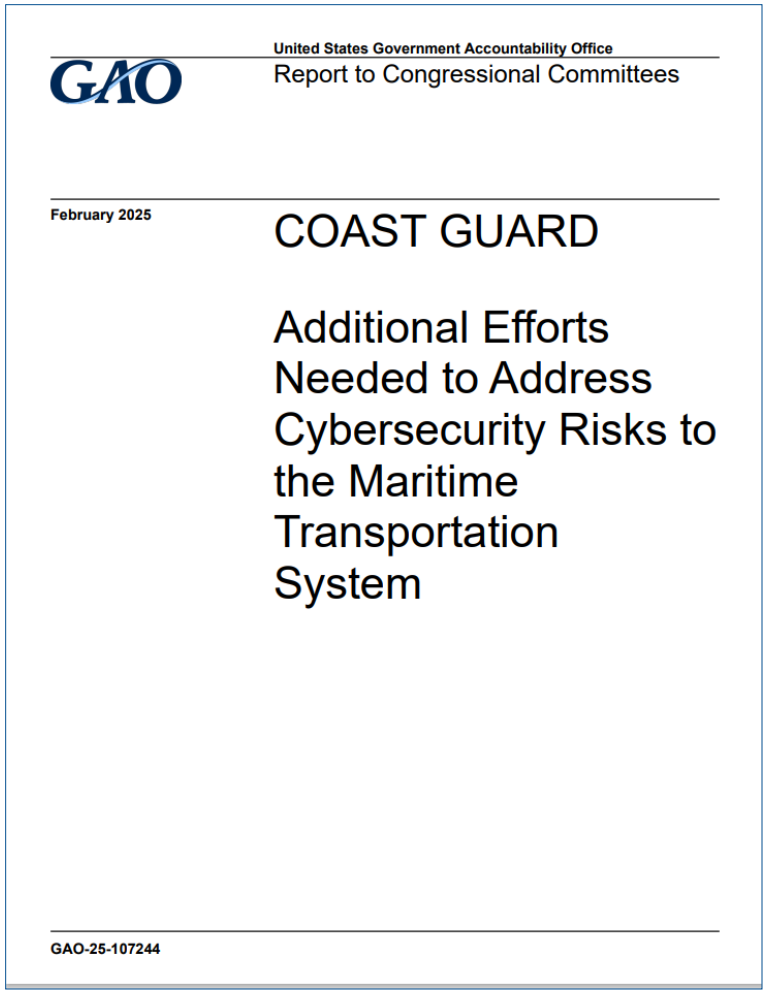
Overview of GAO

GAO is an independent, nonpartisan agency that works for Congress by

- auditing agency operations to determine whether federal funds are being spent efficiently and effectively;
- reporting on how well government programs are meeting their objectives;
- making recommendations for improving government services; and
- issuing legal decisions and opinions such as bid protest rulings.

Our Report

- The National Defense Authorization Act for Fiscal Year 2023 included a provision for us to review cybersecurity risks to the Maritime Transportation System (MTS), including vessels and facilities.
- Our report (GAO-25-107244) examined
  - (1) cybersecurity risks to the MTS,
  - Coast Guard's efforts to:
    - (2) assist and oversee MTS owner and operator actions on cyber risks,
    - (3) conduct strategic planning to mitigate these risks, and
    - (4) implement leading practices on cyber workforce competencies.


United States Government Accountability Office

Report to Congressional Committees

February 2025

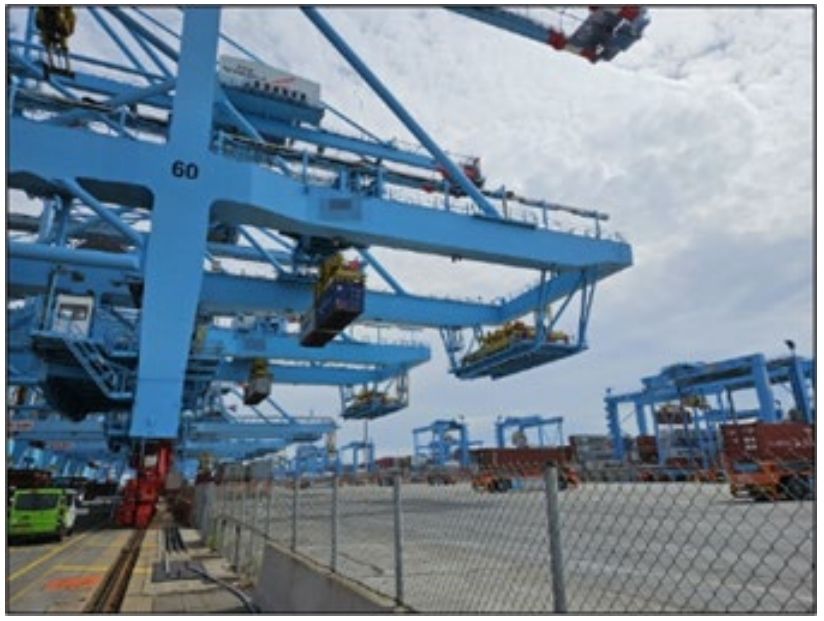
COAST GUARD

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

GAO-25-107244

Cyber Risks to Maritime

- **Threat Actors.** Ports and vessels are increasingly targeted by threat actors, including nation-states, criminal groups, and insiders, each with varying capabilities and motives.
- **Vulnerabilities.** Maritime systems rely heavily on IT, OT, and GPS systems that support critical operations including navigation, cargo handling, and communication networks, making them susceptible to exploitation by cyber threats.
- **Impacts.** Cyber incidents in the maritime domain can lead to major disruptions, financial losses, and cascading effects across global supply chains.
  - **Cyber Incident Procedures.** We found that the Coast Guard did not have documented procedures to accurately track information on cyber incidents within the MTS, limiting its ability to fully assess cyber risks and their impact and make informed decisions on how to prevent or mitigate incidents.



Coast Guard Efforts to Address Those Risks

- **Efforts to assist and oversee maritime owner and operator actions on cyber risks.** The Coast Guard has a number of regulatory and non-regulatory efforts to address maritime cyber risks (e.g., rules, info sharing, etc.). Further, Coast Guard inspectors record information on cyber related deficiencies after inspections of facilities and vessels into their case management system. However, complete information on these deficiencies was not readily accessible in the system, including categories to identify cyber related deficiencies.
- **Efforts to conduct strategic planning to mitigate these risks.** We found that while the Coast Guard has developed a cybersecurity strategy and implementation plan, these documents did not fully address all risks to the MTS (e.g., vessel OT cyberattacks) and lacked performance measures to assess the effectiveness of their efforts.
- **Efforts to implement leading practices on cyber workforce competencies**. The Coast Guard has recognized the need for specialized cyber expertise and established some cyber-specific positions. However, we found that the Coast Guard did not assess gaps in competencies for all its personnel that address MTS cyber risks. Further, it did not develop and implement plans for addressing gaps in competencies for all of its personnel that address MTS cyber risks.

Recommendations

As a result, we made five recommendations aimed at enhancing the Coast Guard's approach to managing cybersecurity risks, including:

- **Efforts to address cybersecurity risks to the MTS**. Develop and implement documented procedures to ensure the accuracy of cybersecurity incident information that the service identifies and tracks.
- **Efforts to assist and oversee maritime owner and operator actions on cyber risks.** Ensure that the case management system for facility and vessel security inspections provides ready access to complete data on specific cybersecurity deficiencies identified during those inspections.
- **Efforts to conduct strategic planning to mitigate these risks.** . Ensure its cybersecurity strategy and plans address the key characteristics of an effective national strategy, including a full assessment of cybersecurity risks to the MTS.
- **Efforts to implement leading practices on cyber workforce competencies.**

  Develop future competency needs for all of the service's personnel with MTS cyber responsibilities for mitigating cyber risks to the MTS and analyze the gaps between current competencies and future needs.

  Using the gap analysis of current and future competency needs for personnel with MTS cyber risk mitigation responsibilities, address any gaps in competencies, such as through training.