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

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.

Contents

Tables

Figures

Abbreviations

AMSC	Area Maritime Security Committee
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOT	Department of Transportation
GPS	global positioning system
IT	information technology
MISLE	Marine Information for Safety and Law Enforcement
MTS	U.S. Maritime Transportation System
MTSA	Maritime Transportation Security Act
NIST	National Institute of Standards and Technology
NVIC	Coast Guard Navigation and Vessel Inspection Circular
OCS	outer continental shelf
OT	operational technology
SRMA	sector risk management agency

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

February 11, 2025

The Honorable Ted Cruz
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Sam Graves
Chairman
The Honorable Rick Larsen
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The U.S. Maritime Transportation System (MTS) is an essential element of the nation's critical infrastructure, handling more than $5.4 trillion in goods and services annually.[1] Owners and operators of maritime facilities and vessels (MTS owners and operators) collectively manage these goods and services via technology systems that are often interconnected with internal and external systems and networks, including the internet. Although these technologies facilitate MTS operations, they are also vulnerable to cyberattacks with the potential to cause significant and catastrophic damage to maritime infrastructure. Consequently, the safe operation of the MTS is critical to our national and economic security.

Although the maritime critical infrastructure subsector is owned and operated by private industry and state and local governments, the federal government has a significant role in addressing cybersecurity risks facing

[1] The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors, including Transportation Systems. According to the Cybersecurity and Infrastructure Security Agency, some critical infrastructure sectors that are diverse in both scope and function are divided into subsectors for the purposes of managing risk. The Maritime Transportation System is a subsector of the Transportation Systems sector.

the MTS.[2] The U.S. Coast Guard and other federal agencies coordinate efforts to identify and mitigate these risks.[3] As part of its broader mission, the Coast Guard, within the Department of Homeland Security (DHS), is responsible for assessing risks to the MTS, establishing and implementing programs for addressing those risks, and facilitating the exchange of threat information with MTS owners and operators.[4] We have previously reported that the Coast Guard could take further action to mitigate cybersecurity risks.[5] Additionally, in July 2024, the DHS Office of Inspector General reported that the Coast Guard should take additional steps to secure the MTS against cyberattacks, such as completing and publishing cybersecurity-specific regulations.[6]

Information security has been on our High-Risk List since 1997, and we expanded this area to include the protection of critical cyber infrastructure in 2003. In September 2018, we issued an update to the High-Risk List that identified actions needed to address cybersecurity challenges facing the nation—including protecting critical infrastructure. We later identified ensuring the nation's cybersecurity as one of nine high-risk areas that

[2] The White House National Security Council, National Security Memorandum/NSM-22: *National Security Memorandum on Critical Infrastructure Security and Resilience* (Washington, D.C.: Apr. 30, 2024). This memorandum outlines a national policy on how the federal government protects and secures our nation's critical infrastructure from cyber and all-hazard threats.

[3] The Coast Guard coordinates risk management activities (e.g., sharing information on cyber threats and incidents) for the MTS with the Department of Transportation's Maritime Administration and National Security Policy and Preparedness Division, Department of Justice's Federal Bureau of Investigation, Department of Interior's Bureau of Safety and Environmental Enforcement, and other Department of Homeland Security components including the Transportation Security Administration.

[4] The Coast Guard's 11 statutory missions are (1) aids to navigation; (2) defense readiness; (3) drug interdiction; (4) ice operations; (5) living marine resources; (6) marine environmental protection; (7) marine safety; (8) migrant interdiction; (9) other law enforcement; (10) ports, waterways, and coastal security; and (11) search and rescue. 6 U.S.C. § 468(a).

[5] GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, GAO-14-459 (Washington, D.C.: June 5, 2014); and *Coast Guard*: *Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands*, GAO-22-105208 (Washington, D.C.: Sept. 27, 2022).

[6] U.S. Department of Homeland Security, Office of Inspector General: *Coast Guard Should Take Additional Steps to Secure the Marine Transportation System against Cyberattacks*, OIG-24-37 (Washington, D.C.: Jul. 9, 2024). In January 2025, the Coast Guard issued regulations that include minimum cybersecurity requirements for most MTS owners and operators. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

need especially focused executive and congressional attention. We continue to identify the protection of critical cyber infrastructure as a component of this high-risk area, most recently in our June 2024 high-risk update on addressing critical cybersecurity challenges.[7]

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for us to conduct a study on cybersecurity threats to the MTS.[8] This report addresses (1) the cybersecurity threats and associated risks facing the MTS and the extent to which Coast Guard has established procedures for maintaining cybersecurity incident information; and the extent to which the Coast Guard has (2) taken action to assist and oversee MTS owners and operators in mitigating cybersecurity risks, (3) conducted strategic planning to mitigate cybersecurity risks to the MTS, and (4) implemented leading practices for cyber workforce competency assessments, including addressing our prior cyber workforce staffing recommendations.

For each of our objectives, we interviewed relevant Coast Guard headquarters officials, such as those with cyber responsibilities, those involved with facility and vessel compliance, and Human Resources. In addition, we conducted in-person or virtual site visits with the Coast Guard sectors responsible for a non-generalizable sample of four ports that we selected based on factors including volume of trade measured in tonnage, reported cybersecurity incidents, presence of ship-to-shore cranes, and geographic dispersion.[9] During these site visits, we interviewed Coast Guard sector officials to gather information and local perspectives on cybersecurity threats, oversight of MTS owner and

[7] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[8] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. K, tit. CXII, subtit. D, § 11230, 136 Stat. 2395, 4029 (2022).

[9] We conducted in-person and virtual site visits with ports in the following sectors: Houston/Galveston, Los Angeles/Long Beach, New York, and the Ohio Valley. During our in-person site visits, we observed facility security inspections in the Coast Guard New York sector and the Houston/Galveston sector. We included ship-to-shore cranes as a factor for selecting ports, due to the service's recent issuance of a related Maritime Security Directive: U.S. Coast Guard, *MARSEC Directive 105-4: Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies,* (February 21, 2024).

operator compliance with cybersecurity statutory requirements and relevant regulations, cyber-related information sharing, and cyber workforce competencies. We also interviewed members of each Area Maritime Security Committee representing the four ports that we selected to better understand the unique perspectives of public and private MTS owners and operators.[10] The information that we gathered from these interviews cannot be generalized to all ports and sectors across the United States. However, it can provide insight into MTS cybersecurity threats, information sharing, cyber risk mitigation efforts, oversight, and workforce structure.

For our first objective, we developed a list of cyber actors that could pose a threat to the MTS, reviewed vulnerable components that could be exploited and the potential impact of cyberattacks on the MTS, and assessed the reliability of Coast Guard's data on cybersecurity incidents. To develop the list of cyber threat actors, we reviewed our prior work on cyber-based threats facing critical infrastructure as well as federal threat reports, including Coast Guard's *2023 Cyber Trends and Insights in the Marine Environment*.[11] To confirm the accuracy of our cyber threat actor list, we interviewed officials and representatives from the Coast Guard, four relevant federal agencies, and four nonfederal stakeholders to confirm the accuracy of our cyber threat actor list.[12]

To identify vulnerable components that could be exploited and the potential impact of attacks on the MTS, we reviewed reports developed by relevant federal and industry stakeholders, as well as our previous

[10] The Maritime Transportation Security Act of 2002 established regional Area Maritime Security Committees. Pub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2081 (codified as amended at 46 U.S.C. § 70112). The function of the Committees is to, among other things, advise DHS on how to enhance communication between port stakeholders (including federal, state, and local agencies) and industry, and to improve security (cyber and traditional) within the port environment. 46 U.S.C. § 70112(a)(2).

[11] See, e.g., GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, GAO-23-105789 (Washington, D.C.: Oct. 26, 2022); Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024); Department of Homeland Security, *Office of Intelligence and Analysis, Homeland Threat Assessment 2024;* U.S. Coast Guard, Coast Guard Cyber Command, *2023 Cyber Trends and Insights in the Marine Environment*.

[12] The four federal agencies are the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), Department of the Interior's Bureau of Safety and Environmental Enforcement, Department of Justice's Federal Bureau of Investigation, and Department of Transportation's Maritime Administration. The four nonfederal stakeholders are Bechtel, Dragos, Gary Kessler Associates, and the MTS Information Sharing and Analysis Center.

work on cybersecurity risks to critical infrastructure.[13] To assess the reliability of Coast Guard's data on cybersecurity incidents impacting the MTS from July 2019 through May 2024, we compared the data to the definition that Coast Guard uses for a cybersecurity incident.[14] We determined that Coast Guard's data were not sufficiently reliable for our purposes of describing the number of reported cybersecurity incidents impacting the MTS.

For our second objective, we reviewed federal cybersecurity requirements as well as Coast Guard documentation on efforts to mitigate cybersecurity risks.[15] Further, we analyzed Coast Guard policies, procedures, and guidance related to overseeing MTS owner and operator compliance with federal statutes and regulations related to computer systems and networks and documenting cybersecurity risks. We also interviewed relevant Coast Guard headquarters and sector officials to confirm our understanding of this information. In January 2025, the Coast Guard finalized its rule on minimum cybersecurity requirements for most MTS owners and operators. We have included these updated requirements in our report, as applicable; however, the report does not address the implementation of these new minimum requirements as they will not begin to take effect until July 2025.[16] Additionally, we reviewed cybersecurity-related data recorded in Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) case management system for facility and vessel inspections in fiscal year 2019 through June 2024. However, we found that, for the purposes of our review, the MISLE

[13] We also interviewed federal agencies and obtained the perspectives of nonfederal stakeholders to identify potential cybersecurity vulnerabilities and any related reports, assessments, or data to identify any reported incidents and potential impacts on MTS infrastructure.

[14] Relevant regulations define a "cyber incident" as occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 33 C.F.R. §§ 6.01-8 (incorporating by reference the definition of "incident" in 44 U.S.C. § 3552(b)(2)); 101.615 (effective July 16, 2025, per Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025)).

[15] This documentation included cybersecurity guidelines, cyber threat information sharing methods, and information on voluntary advisory services and direct technical assistance provided to MTS owners and operators.

[16] See Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

inspection-related data that Coast Guard provided are likely not complete, which we discuss later in the report.[17]

For our third objective, we analyzed the service's efforts to develop approaches for implementing a cybersecurity strategy for the MTS subsector. This included comparing the Coast Guard's MTS cybersecurity strategy and plans against leading practices we identified in prior work on key characteristics for an effective national strategy.[18]

For the fourth objective, we reviewed documentation related to the Coast Guard's workforce competency efforts. We then compared these efforts against leading practices we identified in our prior work highlighting the importance of ensuring that staff are assigned the performance competencies to effectively carry out their duties.[19] We also interviewed Coast Guard officials on their efforts to develop competencies, as well as assess and address competency gaps for the service's cyber workforce, including efforts to address our prior relevant recommendations.[20] See appendix I for a more detailed description of all our objectives, scope, and methodology.

We conducted this performance audit from December 2023 to December 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The MTS includes approximately 360 commercial sea and river ports that account for more than $5.4 trillion in annual U.S. economic activity and support over 30 million jobs. A wide variety of goods—including automobiles, grain, and millions of cargo containers—travel through these ports each day by way of foreign-flagged and U.S.-flagged vessels. While no two ports are exactly alike, many share certain characteristics such as

[17] The MISLE system is the Coast Guard's primary data system of record for recording facility and vessel inspection data and information.

[18] GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[19] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

[20] GAO-22-105208.

their size, proximity to a metropolitan area, the volume of cargo they process, and connections to complex transportation networks.

MTS Operations and Supporting Technology

Systems and networks supporting the MTS are composed of, and connected to, enterprise Information Technology (IT) systems, Operational Technology (OT) systems,[21] and Global Positioning Systems (GPS) that provide numerous benefits to MTS critical infrastructure owners and operators, as described in table 1 below.

Table 1: Technology Supporting the Maritime Transportation System (MTS)

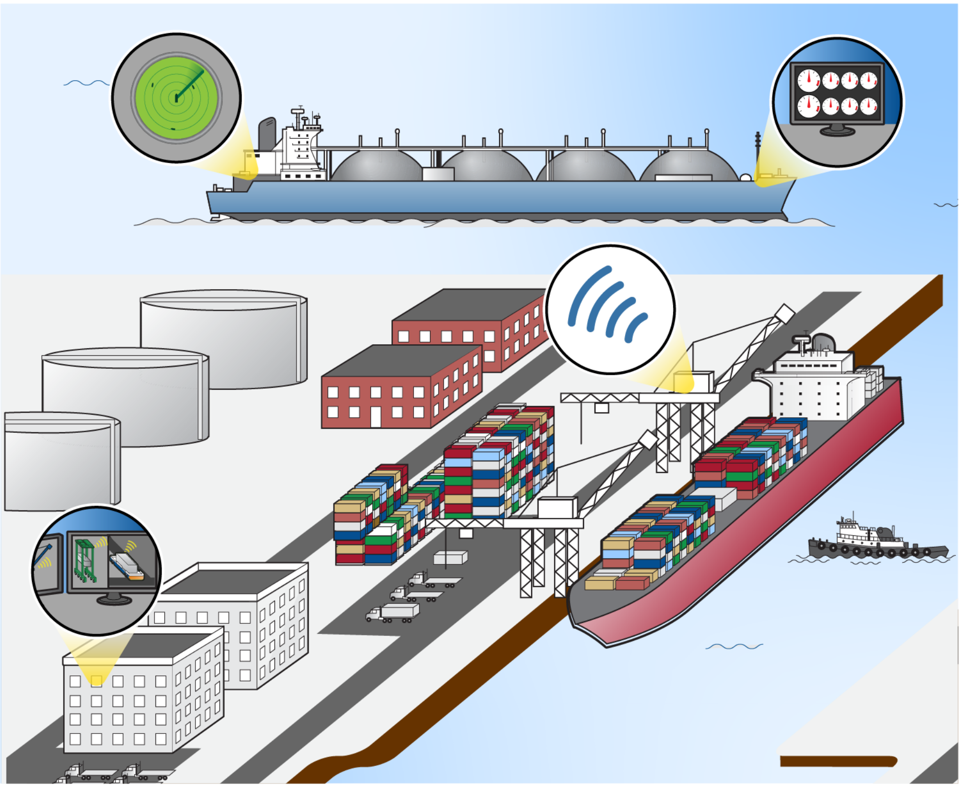
Technology	Description
Enterprise Information Technology (IT)	Traditional IT computing and communications hardware and software components that may be connected to the internet. Vessels may use enterprise IT to record voyage data, communicate with other vessels and facilities, and provide wireless internet access to the crew. Facilities often use enterprise IT to track cargo, monitor marine traffic, and assign crew.
Operational Technology (OT) systems	Vital systems that monitor and control sensitive processes and physical functions. A vessel may use OT to operate the propulsion and steering, power, and cargo management systems. In addition, a facility may use OT to operate and maintain ship-to-shore cranes and container transport vehicles.
Global Positioning System (GPS)	A satellite-based system that provides position, navigation, and timing information. MTS vessel operations rely on precision navigation and timing provided by GPS. For example, marine vessels use GPS and Automated Identification System position data in an electronic chart display to safely navigate in high-traffic, high-risk areas, such as ports and shallow water.

Source: GAO analysis of Coast Guard's documentation. | GAO-25-107244

IT and OT systems, as well as GPS, allow for interconnection across the MTS, including the range of facility and vessel operations at a port. Figure 1 shows technologies used by MTS owners and operators.

[21] Operational technology refers to programmable systems and devices that interact with the physical environment. As discussed in more detail later in this report, this technology is used by the MTS.

Figure 1: Examples of Technologies Used by Facilities and Vessels within the Maritime Transportation System



Automatic Identification System. A shipboard broadcast system that uses radio waves and global positioning systems to continuously send and receive location and position information within approximately 20 nautical miles.

Propulsion system. A system that uses operational technology to monitor a vessel's speed and make adjustments such as increasing or decreasing motor power to maintain appropriate speeds.

Terminal operating system. An enterprise IT software platform that communicates with all equipment in the terminal and directs their movements.

Remotely operated ship-to-shore cranes. A remotely located worker moves containers onto and off of vessels with the assistance of operational technology sensors (e.g., cargo weight).

Source: GAO analysis; GAO (illustrations). | GAO-25-107244

Of note, modern facilities and vessels are increasingly reliant on remote access capabilities and—in some cases—autonomous operations. For example, some modern facilities include ship-to-shore cranes that may be remotely operated and automated cargo transport vehicles (e.g., straddle carriers). In addition, modern vessels allow for a company's headquarters to remotely monitor vessel operations. Further, autonomous commercial ships in use today around the world are designed or adapted to perform a variety of specialized tasks (e.g., autonomous ships used to transport cargo and autonomous drone ships that recover rockets from spaceflights).[22]

Critical Infrastructure Protection Roles and Responsibilities

The National Security Memorandum on Critical Infrastructure Security and Resilience outlines a national policy on how the federal government strengthens and secures our nation's critical infrastructure from cyber and all-hazard threats.[23] The memorandum also reaffirmed the 16 critical infrastructure sector designations and the Sector Risk Management Agencies for each sector. Sector Risk Management Agencies are the federal entities responsible for providing institutional knowledge and specialized expertise for enhancing and protecting the security, including cybersecurity, of critical infrastructure.[24] The Department of Transportation and DHS are the Co-Sector Risk Management Agencies for the Transportation Systems sector (one of the 16 critical infrastructure sectors), which includes the MTS subsector.[25]

DHS designated Coast Guard as the agency to manage its critical infrastructure-related functions, roles, and responsibilities for the MTS. The National Security Memorandum also established DHS's Cybersecurity and Information Security Agency (CISA) as the National Coordinator for Security and Resilience of Critical Infrastructure. This memorandum includes leveraging the authorities of federal agencies to

[22] In particular, a Norwegian fertilizer company developed and deployed an autonomous cargo ship that entered service in April 2022. In addition, an American space company developed and deployed autonomous "drone ships" to recover rockets from spaceflights in April 2016. See GAO, *Coast Guard: Autonomous Ships and Efforts to Regulate Them,* GAO-24-107059 (Washington, D.C.: Aug. 8, 2024).

[23] The White House National Security Memorandum/NSM-22: *National Security Memorandum on Critical Infrastructure Security and Resilience* (Washington, D.C.: Apr. 30, 2024).

[24] Presidential Policy Directive-21 (PPD-21) previously called these agencies Sector-Specific Agencies. The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 codified Sector-Specific Agencies as Sector Risk Management Agencies. Pub. L. No. 117-263, div. G, tit. LXXI, subtit. E, § 7143(d)(5), 136 Stat. at 3663-64 (codified at 6 U.S.C. § 652a(c)(3)). In 2013, PPD-21 categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as Sector Risk Management Agency for the sector, although the number of sectors and Sector Risk Management Agency assignments are subject to review and modification. Those designations are still in effect.

[25] The Transportation Systems sector includes the following subsectors: aviation, highway and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping.

mitigate risk, including cybersecurity risks, in collaboration with partners.[26] As the lead risk management agency for the MTS, the Coast Guard is to protect it from all threats, including those related to cybersecurity. Specifically, the Coast Guard employs frameworks, standards, and best practices in prevention and response activities to identify and manage cybersecurity risks to the MTS. Coast Guard headquarters develops national strategies and policies for cybersecurity-related operations, while field units are to implement these policies.[27]

Within ports, the Coast Guard's Captains of the Port promote cyber risk management, accountability, and the development and implementation of response plans. For example, we have previously reported on the Coast Guard's responsibility as the lead risk management agency to share information with industry on cyber actors and their capabilities that threaten the MTS. Specifically, in September 2023, we reported that 14 of the federal agencies in our review—the Federal Bureau of Investigation, CISA, and 12 risk management agencies (including Coast Guard)—relied on 11 methods to share cyber threat information with critical infrastructure owners and operators, including those in the MTS.[28] Additionally, the Coast Guard deploys cyber workforce staff that augment each Coast Guard area commander and sector Captain of the Port by providing subject matter expertise, assessment, and incident response capabilities.

[26] For example, this memorandum directs Sector Risk Management Agencies as well as relevant federal departments and agencies to use tools and authorities to collect and share intelligence information with critical infrastructure owners and operators to understand and identify threats.

[27] The Coast Guard organizes its field structure under two area commands (Atlantic and Pacific). The two area commands oversee nine districts across the United States, which are further broken down across 37 sectors and other areas of responsibility such as marine safety units and detachments.

[28] GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, GAO-23-105468 (Washington, D.C.: Sept. 26, 2023). The 11 methods were 1) cyber threat briefings, 2) threat information products, 3) incident reporting services, 4) intrusion detection and/or prevention systems, 5) malicious activity analysis, 6) incident response services, 7) threat indicator sharing platforms, 8) exploited vulnerability catalog, 9) information sharing and analysis centers, 10) working groups and councils, and 11) federal cybersecurity collaboration centers. These agencies used each of the 11 methods to varying degrees. For example, CISA used all 11 methods and FBI used 6 methods—to share information with each of the 16 critical infrastructure sectors in a centralized approach, including the MTS.

Maritime Transportation System Laws, Regulations, and Policies

The Maritime Transportation Security Act (MTSA) and implementing federal regulations require the Coast Guard to oversee MTS owner and operator requirements to assess, document, and address identified vulnerabilities.[29] Coast Guard regulations require MTS owners and operators to document specific vulnerabilities in facility or vessel security plans, including vulnerabilities associated with their computer systems and networks, and submit those assessments and plans to the Coast Guard.[30] The Coast Guard must review and approve MTS owner and operator facility and vessel security assessments and plans every 5 years. In 2018, MTSA was amended to require that owners and operators assess, document, and address cybersecurity risks as well.[31] Accordingly, since 2018, MTS owners and operators have been required to identify their cybersecurity-related risks and determine what controls and

[29] Enacted in November 2002, the Maritime Transportation Security Act requires a wide range of security improvements for protecting U.S. ports, waterways, and coastal areas. Pub. L. No. 107-295, 116 Stat. 2064. DHS has authority under MTSA to promulgate implementing regulations. 46 U.S.C. § 70124. This authority was delegated to the Coast Guard by DHS Delegation No. 00170(II)(97)(a) through (c), Revision No. 01.3.

[30] Prior to January 17, 2025, the regulations only contained provisions related to documenting vulnerabilities with “radio and telecommunication systems, including computer systems and networks,” but did not directly address cybersecurity. See 33 C.F.R. §§ 104.305(d)(vii)(2)(v), 105.305(c)(1)(v), 106.305(c)(1)(v). Pursuant to a final rule issued on January 17, 2025, most MTS owners and operators will be required to submit separate cybersecurity-specific plans to the Coast Guard as of July 2027. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025) (promulgating 33 C.F.R. § 101.630).

[31] See Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, § 1805(d)(2)(D), 132 Stat. at 3535 (pertinent portion codified at 46 U.S.C. § 70103(c)(3)(C)(v)). Additionally, the Federal Aviation Administration Reauthorization Act of 2018 amended MTSA to require vessel and facility security plans to address cybersecurity risks. The act also directed U.S. Coast Guard to “issue voluntary guidance for the management of such cybersecurity risks in each facility security plan.” Id. at §1805 (c)(2)(B). In response, U.S. Coast Guard issued the Maritime Cybersecurity Assessment and Annex Guide. According to the Coast Guard, attaching a cybersecurity annex to a facility security plan in accordance with this guidance is a recommended voluntary process for identifying and describing cybersecurity vulnerabilities at facilities and is consistent with the National Institute of Standards and Technology Cybersecurity Framework (see appendix IV for more information about functions outlined in the annex guide).

measures would mitigate those risks.[32] However, implementing regulations for this requirement were not issued until January 2025.[33] As such, there were no specific cybersecurity controls or measures that MTS owners and operators were required to include in their security plans at the time of our review.

In February 2024, the President of the United States issued Executive Order 14,116: *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States*. This Executive Order gives Coast Guard authority to prescribe conditions and restrictions for vessels and waterfront facilities related to cybersecurity. Also, the Executive Order gives Coast Guard authority to prevent a person from boarding a vessel to prevent a cyber threat.[34]

That same month, Coast Guard issued Maritime Security Directive 105-4 *Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies*. This directive includes required cybersecurity risk management actions for owners or operators of ship-to-shore cranes manufactured by People's Republic of China companies, such as eliminating connections to the internet. Subsequently in November of 2024, the Coast Guard issued Maritime Security Directive 105-5, which includes additional cyber risk management requirements for these owners and operators.[35]

[32] There is a statutory requirement that MTS owners and operators assess, document, and address cybersecurity risks, but at the time of our review there were not minimum cybersecurity regulatory requirements in effect for owners and operators. See 46 U.S.C. § 70103(c)(3)(C)(v). While the Coast Guard has recently promulgated minimum cybersecurity regulatory requirements for most MTS owners and operators, they will not be in effect until July 16, 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025). Accordingly, for the purposes of this report, we refer to the statutory requirement and the regulations which existed as of December of 2024 as "cybersecurity-related requirements."

[33] Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[34] Exec. Order No. 14,116 (Feb. 26, 2024) (amending 33 C.F.R. pt. 6).

[35] U.S. Coast Guard, MARSEC Directive 105-4: *Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies,* (February 21, 2024); MARSEC Directive 105-5: *Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies*, (November 13, 2024). Pursuant to regulation, these directives contain security-sensitive information and cannot be made available to the general public. 33 C.F.R. § 101.405(a).

Most recently, in January 2025, Coast Guard finalized a rule entitled Cybersecurity in the Marine Transportation System,[36] which established minimum cybersecurity requirements applicable to technology systems for most MTS owners and operators subject to MTSA regulations.[37] The rule will become effective on July 16, 2025. Some new requirements go into effect on that date, while the rule allows regulated owners and operators 6 or 24 months from the time of publication to implement other requirements.

In the event of an actual or threatened cyber incident, MTS owners and operators are to report it to the Federal Bureau of Investigation, CISA, and the relevant Coast Guard Captain of the Port (or to their respective representatives).[38] Also, under federal regulations, as part of mandatory reports of transportation security incidents from certain MTS owners and operators, the Coast Guard receives reports of cybersecurity incidents through its National Response Center.[39] Appendix II lists the types of

[36] Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[37] These new requirements include automatic account lockout after repeated failed login attempts, minimum password strength, multifactor authentication, maintaining separate credentials for critical IT and OT systems, and maintaining an inventory of network-connected systems including the designation of critical IT and OT systems.

[38] 33 C.F.R. § 6.16-1. See also Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025) (promulgating 33 C.F.R. § 101.620(b)(7), requiring certain entities to report cyber incidents to the National Response Center as well from July 16, 2025).

[39] 33. C.F.R. § 101.305. The primary function of the National Response Center is to serve as the sole national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment anywhere in the United States and its territories. However, the National Response Center also takes maritime reports of suspicious activity and security breaches within the waters of the United States and its territories, including those related to cyber.

facilities and vessels that are subject to the federal regulations implementing MTSA.[40]

Coast Guard Cyber Workforce

According to the Coast Guard, as of 2023, the service employs about 200 cyber workforce staff to help protect the MTS from adversaries. The Coast Guard partners with MTS owners and operators by providing voluntary guidance to assist them in their efforts to mitigate cybersecurity risks. The Coast Guard provides these services to the MTS though two key positions:

- **Cybersecurity specialists** are civilian personnel who advise MTS owners and operators on cybersecurity practices, such as preventing or responding to a cybersecurity incident. There is one civilian cybersecurity specialist staff position at every Coast Guard area, district, and sector.[41]
- **Cyber protection teams** are deployable teams from the Coast Guard's office of Cyber Command who provide direct technical assistance to MTS owners and operators through assessment, threat hunting, and incident response.

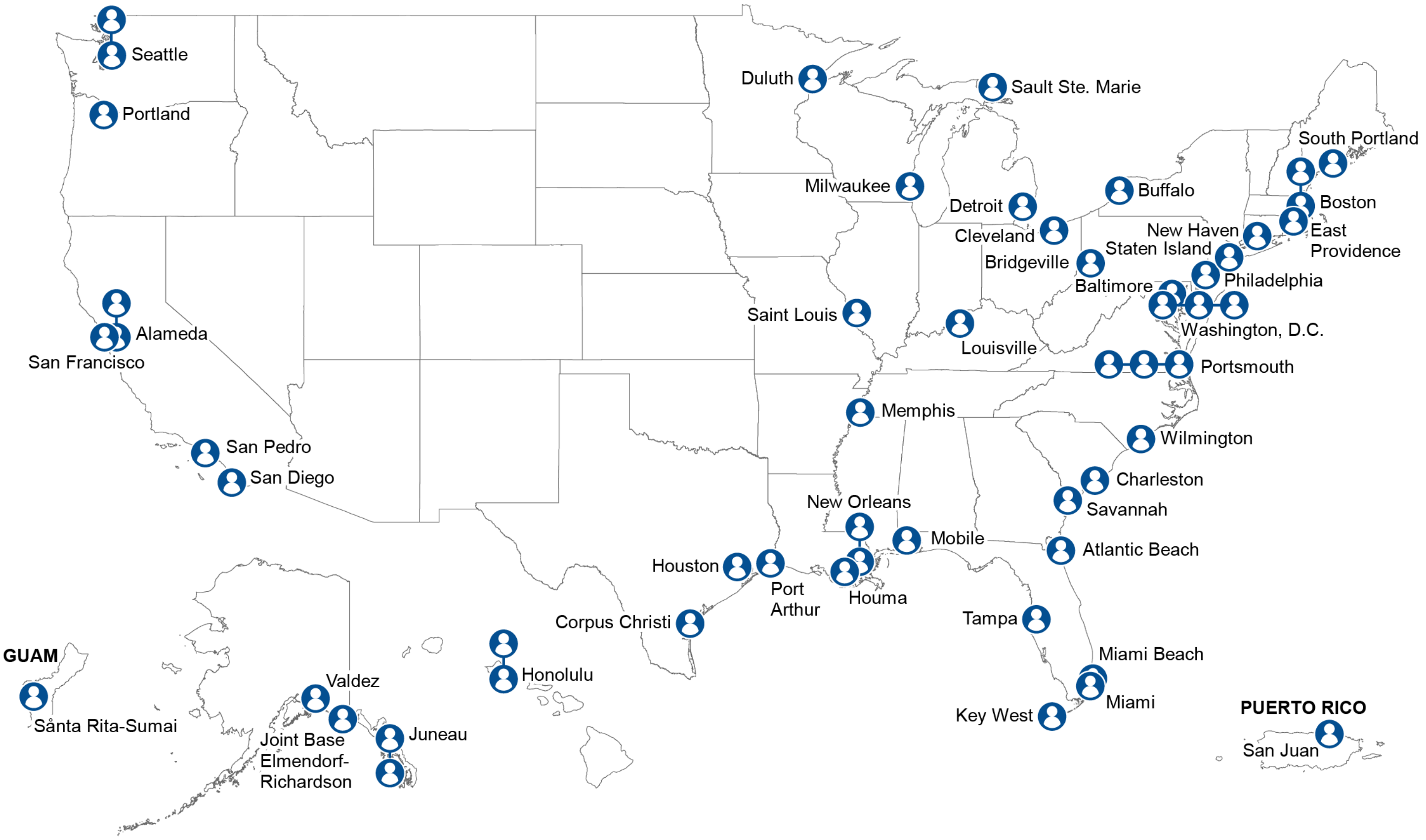
As shown in figure 2, there are 55 authorized civilian staff that serve as cybersecurity specialists at every Coast Guard sector (Captain of the Port office), district, and area office. In addition, there are currently four cyber protection teams totaling 156 authorized staff—three teams of 39 service members (less two civilian staff) and one team of 39 reservists. Three of

[40] According to the Coast Guard, in addition to vessels and facilities, there are also 33 Outer Continental Shelf facilities subject to the Maritime Transportation Security Act and separate implementing federal regulations. Outer Continental Shelf facilities are any artificial island, installation, or other complex of one or more structures permanently or temporarily attached to the subsoil or seabed of the Outer Continental Shelf, erected for the purpose of exploring for, developing, or producing oil, natural gas, or mineral resources. 33 C.F.R. § 101.105. MTSA regulations apply to these 33 facilities based on criteria such as more than 150 people on site at the facility for 12 hours or more in each 24-hour period continuously for at least 30 days, production of more than 100,000 barrels of oil per day, or production of more than 200 million cubic feet of natural gas per day. 33 C.F.R. § 106.105(a).

[41] For the purposes for this report, we refer to the Coast Guard's Maritime Transportation Security Specialists-Cyber position as cybersecurity specialists.

these teams, including the team of reservists, are based in Washington D.C., and one team is based in Alameda, California.[42]

Figure 2: Locations of Coast Guard Cybersecurity Specialists Advising the Maritime Transportation System



Source: GAO analysis of U.S. Coast Guard data; U.S. Census Bureau (map); GAO (illustrations). | GAO-25-107244

Coast Guard Facility and Vessel Inspection Workforce

A key part of the cybersecurity effort is the facility and vessel security inspection program, in which the Coast Guard works with MTS owners and operators to ensure compliance with federal statutes and regulatory requirements—one of the main objectives of an internal control system. The Coast Guard has 428 facility inspectors and 888 vessel inspectors

[42] The Coast Guard's office of Cyber Command mission includes defending Coast Guard cyberspace, protecting the MTS, and operating in and through cyberspace. Cyber Command staff also provide support functions such as collaborating with the intelligence community, conducting assessments and authorizations for Coast Guard information technology, and formulating annual budgets.

who conduct inspections to ensure compliance with MTSA.[43] According to Coast Guard officials, the service may staff a team of between 2 and 4 inspectors to conduct a facility or vessel inspection. These inspectors monitor compliance with federal statutes and regulatory requirements to achieve marine safety, security, and mission success.[44]

Prior GAO Work on Coast Guard Cybersecurity

We have previously reported on challenges in Coast Guard's management of MTS cybersecurity and its cyber workforce. Specifically, in June 2014, we reported that the Coast Guard and other stakeholders had taken limited steps to address cybersecurity in the maritime environment.[45] For example, we found that Coast Guard had not included cybersecurity-related risks in its biennial assessment of risks to the maritime environment. In addition, we also found that Coast Guard did not address cybersecurity-related risks in its guidance for developing port area and port facility security plans. We recommended that the Coast Guard include cybersecurity-related risks in its updated risk assessment for the maritime environment and address these risks in its guidance for port security plans. Coast Guard implemented our recommendations, which should enhance the cybersecurity of critical infrastructure in the MTS.

Further, in September 2022, we found that because the Coast Guard had not determined necessary staffing levels and skills to meet mission needs, it was not positioned to fully understand the resources such a workforce requires.[46] We recommended that the Coast Guard take six actions, including to determine the cyberspace staff needed to meet its mission demands and fully implement five recruitment and retention

[43] According to Coast Guard officials, the service's inspectors also ensure adherence to the International Maritime Organization's International Safety Management Code for the safe operation of ships and for pollution prevention. The Coast Guard requires its inspectors to conduct two annual security inspections of regulated facilities each year—one unannounced visit and one announced. The inspection schedule for vessels depends on the type of vessel.

[44] The Coast Guard inspectors monitor compliance with certain federal statutes and regulatory requirements for prevention activities associated with the safe operation of vessels and facilities. More specifically, Coast Guard facility inspectors help the Coast Guard's Office of Port and Facility Compliance achieve maritime safety and security, and environmental stewardship; while vessel inspectors help the Coast Guard's Office of Commercial Vessel Compliance achieve marine safety, security, and stewardship mission success related to domestic, foreign, and fishing vessels.

[45] GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, GAO-14-459 (Washington, D.C.: June 5, 2014).

[46] GAO-22-105208.

leading practices, such as establishing a strategic plan for its cyberspace workforce.

As of September 2024, the Coast Guard completed a Workforce Requirements Determination for its office of Cyber Command, but otherwise has not implemented our recommendations and noted that they are in various stages of implementation. Fully addressing these recommendations could help the Coast Guard better understand the resources it requires, including those to protect its information systems and data from threats.

The Maritime Transportation System Faces Cyber Risks, but Coast Guard Does Not Maintain Accurate Incident Information

The MTS infrastructure faces cybersecurity risks resulting from various threat actors and vulnerabilities due to increasing reliance on technology. Threat actors have become more capable of carrying out attacks on critical infrastructure, including the MTS. At the same time, the technology used in the MTS is increasingly vulnerable to being exploited in cyberattacks. In addition, future cyberattacks could result in serious harm to human safety, the environment, and the economy. However, when they have occurred, the Coast Guard has not maintained accurate information on cybersecurity incidents impacting the MTS.

The Maritime Transportation System Faces Risks from Cyber Threat Actors

According to the 2024 *Annual Threat Assessment of the U.S. Intelligence Community* and agency officials whom we interviewed, China, Iran, North Korea, Russia, and transnational criminals pose the greatest cyber threats to the MTS.[47] In addition, hacktivists (i.e., ideologically motivated actors that exploit cyber vulnerabilities to further political goals) and insiders pose significant threats to the MTS, according to federal agency officials and representatives of nonfederal organizations whom we interviewed. For example, as shown in table 2, hacktivists no longer need a great amount of skill to compromise enterprise IT systems because of the growing availability of public and commercial cyberattack tools.

[47] The John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the National Security Commission on Artificial Intelligence as an independent commission to review advances in artificial intelligence, related machine learning developments, and associated technologies. Pub. L. No. 115-232, tit. X, subtit. D, § 1051(a)(1), 132 Stat. 1636, 1962 (2018). Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024).

Table 2: Threat Actors Who May Pose Significant Threats to the Maritime Transportation System (MTS)

Threat actor	Description	Example
Nations	Nations, including nation-states, state-sponsored, and state-sanctioned groups, or programs, use cyber tools to further economic, military, and political goals. Chinese, Russian, Iranian, and North Korean cyber threat actors have previously targeted U.S. critical infrastructure and could target the MTS.	• In February 2024, several federal agencies authored an advisory (in coordination with several foreign partners) noting that a Chinese-sponsored cyber group known as Volt Typhoon is seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.[a] In addition, the advisory stated that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in four U.S. critical infrastructure sectors, including the Transportation Systems sector. • In April 2022, several federal agencies authored an advisory (in coordination with several foreign partners) summarizing the malicious cyber operations carried out by Russian government and military organizations, including disruptive attacks against U.S. critical infrastructure.[b] In addition, the advisory stated that Russian government and military organizations, including—the Russian Federal Security Service and Russian General Staff Main Intelligence Directorate—had previously targeted a variety of critical infrastructure organizations, including those in the Transportation Systems sector.
Transnational criminal groups	Transnational criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. Further, these groups are increasing the number, scale, and sophistication of ransomware attacks that threaten to cause greater disruptions of critical services.	• In October 2023, the Coast Guard published an alert stating that the service had observed malicious cyber activity linked to the Cl0p Ransomware Group that was affecting the MTS and entities that directly support the MTS.[c] According to that alert, many of the group's victims are either direct members of the MTS or provide critical services to the maritime industry. • In June 2023, the Coast Guard published an alert stating that the service had recently observed a surge in BlackBasta Group Ransomware campaigns targeting the MTS.[d] The alert added that the campaigns include, but were not limited to, an attack in May 2023 impacting an automation technology provider known in the MTS for its role supporting critical infrastructure sectors, including maintenance services offered for ship-to-shore cranes.
Hacktivists	Hacktivists are ideologically motivated actors who use cyberattack tools to further political goals.	• In August 2022, the Coast Guard issued an alert stating that the Russian-based Killnet hacktivist group had made dark-web posts threatening the U.S. Energy sector's segment in the MTS.[e] According to the Coast Guard, the group gained notoriety for their distributed denial of service attacks against numerous U.S. critical infrastructure websites.
Insiders	Insiders are authorized individuals or entities within an environment with the potential to wittingly or unwittingly cause harm through destruction, disclosure, modification of data, or denial of service due to their level of access.	• In 2015, a Coast Guard official made statements regarding a cybersecurity incident where malware was unintentionally introduced onto a vessel—specifically, a mobile offshore drilling unit. According to the Coast Guard, the malware affected the dynamic positioning system, which resulted in the need to maneuver to avoid an accident.

Source: Prior GAO work and summary of Coast Guard and relevant CISA and ODNI documentation. | GAO-25-107244

[a] CISA and co-authors, Joint Cybersecurity Advisory, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Alert Code AA24-038A (Feb. 7, 2024).

[b] CISA, and co-authors, Joint Cybersecurity Advisory, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, Alert Code AA22-110A (April 20, 2022).

[c] U.S. Coast Guard, Threat from Cl0p Ransomware Group, U.S. Coast Guard Cyber Command Maritime Cyber Alert 03-23 (Oct. 4, 2023).

[d] U.S. Coast Guard, BlackBasta Ransomware Group, U.S. Coast Guard Cyber Command Maritime Cyber Alert 02-23 (Jun. 15, 2023).

[e] U.S. Coast Guard, Threat from Cyber Criminal Group KILLNET, U.S. Coast Guard Cyber Command Maritime Cyber Alert 03-22 (Aug. 17, 2022). According to cybersecurity researchers, Killnet is a hacktivist group whose ideologies and goals (e.g., conducting cyberattacks on western nations) are known to be similar to nation state actors from Russia.

Furthermore, threat actors may become even more capable—particularly with advances in artificial intelligence. For example, in March 2021, the National Security Commission on Artificial Intelligence stated that artificial intelligence will enable malware to mutate into thousands of different forms, find vulnerabilities, and attack selectively.[48] The commission added that the expanding application of artificial intelligence cyber capabilities will make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale.

Technology Used by the Maritime Transportation System is Increasingly Vulnerable to Cyberattacks

As previously mentioned, systems and networks supporting the MTS are composed of, and connected to, enterprise IT systems, OT systems, and GPS. These systems are vulnerable to cyberattacks for a number of reasons, including their complexity and interconnections with other systems and the internet (see table 3).

[48] The John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the National Security Commission on Artificial Intelligence as an independent commission to review advances in artificial intelligence, related machine learning developments, and associated technologies. Pub. L. No. 115-232, tit. X, subtit. D, § 1051(a)(1), 132 Stat. 1636, 1962 (2018). National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

Table 3: Technology Used by the Maritime Transportation System (MTS) and Associated Vulnerabilities

Technology	Description	Vulnerabilities
Enterprise Information Technology (IT) systems	Traditional IT computing and communications hardware and software components that may be connected to the internet.	• The complexity of enterprise IT systems increases the difficulty of identifying, managing, and protecting their numerous operating systems, applications, and devices. • The systems and networks used by MTS owners and operators also are often interconnected with other internal and external systems and networks, including the internet. This has led to increased points in a network where attackers can try to enter or extract information.
Operational Technology (OT) systems	Vital systems that monitor and control sensitive processes and physical functions.	• The increased access to OT systems, particularly through remote means and connections to enterprise IT systems, makes these systems more vulnerable to cyberattacks. • The reliance of OT systems on older components makes these systems less secure because they were not designed with cybersecurity protections. • The amount of time to address known cybersecurity vulnerabilities for OT components may increase because they must be taken offline so that owners and operators can apply security patches. However, this may not happen in a timely manner because the devices must remain highly available to support critical functions.
Global Positioning System (GPS)	A satellite-based system that provides position, navigation, and timing information.	• The low power signal of current GPS satellites makes the system vulnerable to interference. • The lack of a capability to prevent GPS manipulation makes the system vulnerable to inauthentic GPS signals. .

Source: GAO analysis of prior GAO, Coast Guard, and- MTS related documentation. | GAO-25-107244

Cyber threat actors use a variety of tactics and techniques to exploit vulnerabilities and attack these systems. Specifically:

- Attackers tend to follow common methodologies to compromise **enterprise IT and OT systems** and achieve their goals, according to MITRE's ATT&CK® Framework. For example, attackers often seek to gain initial access to a target enterprise IT network by using spear phishing emails.[49] By contrast, OT networks should not have internet-accessible email systems, so attackers will need to use another technique to gain initial access to them. Examples of such techniques include leveraging access to an enterprise IT network to migrate to a connected OT network or compromising the supply chain of an OT product. (See the sidebar for more detail on the potential to compromise the supply chain of ship-to-shore cranes).

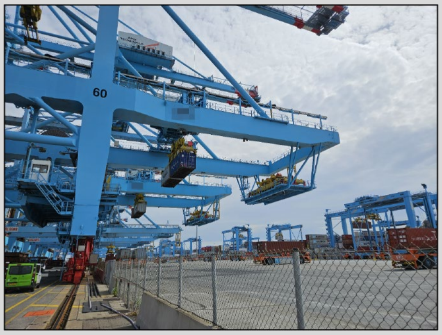
After gaining initial access, attackers will often use a variety of other techniques—such as running malicious code and moving through various systems—to exploit vulnerabilities and position themselves to achieve their ultimate goals. Appendix III includes additional information about cyberattack tactics and techniques associated with enterprise IT and OT.

- Attackers also use two types of attacks, jamming and spoofing, to interfere with GPS. Jamming occurs when a device referred to as a "jammer" emits signals that block or degrade the GPS signal. Spoofing occurs when a device referred to as a "spoofer" replaces the GPS signal with a manipulated signal that may provide incorrect position, navigation, and timing information.

Ship to Shore Crane Supply Chain Threats

According to the U.S. Department of Transportation's Maritime Administration, one China-based company maintains the largest share, by sales revenue, of the ship-to-shore crane market worldwide. These cranes may, depending on their individual configurations, be controlled, serviced, and programmed from remote locations, and those features potentially leave them open to exploitation.

To date, Coast Guard teams have conducted evaluations of over 90 cranes manufactured by this Chinese-based company at U.S. ports. According to the Department of Transportation's Maritime Administration, these Coast Guard evaluations did not identify unique vulnerabilities or exploitations specific to foreign ship to shore cranes. Instead, they found that potential vulnerabilities present in foreign cranes reflect weaknesses present across other OT systems and implementations. Most notably, many MTS OT systems remain exposed to cyberattack due to poor cyber hygiene (e.g., poor password policies, lack of network segmentation, unpatched systems, and exposed services).



Source U.S. Department of Transportation, Maritime Administration Study of Cybersecurity and National Security Threats Potentially Posed by Foreign Manufactured Cranes at United States Ports; GAO photo. | GAO-25-107244

[49] Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack. A phishing attack is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

U.S. Cybersecurity Incidents Reportedly Have Affected Operations; Potential Impacts of Future Incidents Could be Severe

According to Coast Guard officials, at least two U.S. cybersecurity incidents have disrupted operations at port facilities.[50] Specifically:

- In June 2017, the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation conducted the “NotPetya” malware attacks that impacted organizations across the globe, including international shipping company A.P. Møller-Maersk. Once NotPetya infected a machine, it was capable of automatically spreading through a network and infecting other machines. The attack began in Ukraine and spread and infected organizations across the globe—including Maersk. As a result of the attack, computers throughout Maersk were shut down, bringing port operations (including U.S. operations) to a halt and leaving ships idle at sea. According to Maersk, the incident cost the company approximately $250 to $300 million.
- In December 2019, Coast Guard issued a bulletin regarding a ransomware attack on an MTS facility’s network. The service believed that the malicious actor may have gained initial access to the facility by way of a phishing email that contained a malicious link. Once clicked, the malicious link led to the delivery of the “Ryuk” ransomware on the facility’s network.[51] Once the “Ryuk” ransomware payload was delivered, the threat actor encrypted significant enterprise IT files crucial to operations—thus preventing access to those files and causing disruption to the entire corporate IT network. Additionally, the malware compromised OT systems that monitor and control cargo transfer and disrupted camera and physical access control systems, which led to a 30-hour shutdown of primary operations.

The Coast Guard reports that none of the incidents in the United States have disrupted (1) OT systems used by vessels, or (2) GPS. However,

[50] As discussed in more detail later in this report, the Coast Guard has not fully established and implemented a process for maintaining a list of cybersecurity incidents. As such, we are not able to quantify how many incidents have occurred in the United States.

[51] According to an FBI May 2019 alert, Ryuk encrypts files on network drives and an infected computer’s file system. FBI, *Indicators of Compromise Associated with Ryuk Ransomware*, Alert Number MC-000103-MW (May 2, 2019). The alert added that, once the victim has been compromised, the actors encrypt all the network’s files and demand sums of up to $5 million worth of Bitcoin in exchange for a decryptor program. FBI’s alert noted that Ryuk’s targets are varied and indiscriminate, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. According to an April 2021 briefing from the Department of Health and Human Services Office of the Chief Information Officer, the Russian cybergang referred to as “UNC1878” and “WIZARDSPIDER” had documented involvement in Ryuk ransomware.

attacks on GPS impacting vessels have been reported in other countries. For example,

- In March 2024, an average of 35 ships per day transiting the Mediterranean and Black Seas experienced Automatic Identification System or GPS spoofing, according to the Coast Guard.
- In April 2024, 117 cargo vessels in the Mediterranean and Black Sea experienced spoofing in a single day, according to the Coast Guard.
- In September 2019, civilian vessels experienced GPS jamming in port cities across the Mediterranean Sea, according to the Department of Transportation's Maritime Administration.[52]

In addition, significant disruptions and other harms that resulted from successful cyberattacks on OT in other critical infrastructure sectors can serve as proxies for potential impacts to the MTS. Table 4 describes five publicly reported examples of impacts from cyberattacks on OT in other critical infrastructure sectors that could be similar to the effects of attacks to the MTS.

Table 4: Potential Impacts of Cyberattacks on Operational Technology (OT) Systems in the Maritime Transportation System

Potential Impact	Description[a]	Example
Damage to property	Malicious actors may damage or destroy infrastructure, equipment, and the surrounding environment when attacking control systems. This may result in device and operational equipment breakdown or represent tangential damage from other techniques used in an attack.	In December 2014, a cyberattack resulted in the misoperation of an OT system, including the improper shutdown of a furnace and physical damage to a German steel mill's facilities.[b]
Loss of productivity and revenue	Attackers may cause loss of productivity and revenue by damaging or disrupting the availability or integrity of industrial control systems operations, devices, and related processes.	In December 2019, a form of ransomware named EKANS infected various OT devices, reportedly in the United States, Europe, and Japan, by encrypting files and displaying a ransom note. The file encryption impaired operations.[c]
Loss of safety	Attackers may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.	In 2017, Russian cyber actors manipulated a foreign oil refinery's safety devices, which resulted in the refinery shutting down for several days.[d]
Loss or denial of control	Malicious actors may seek to prevent operators and engineers from interacting with process controls.	In 2015, Russian attackers uploaded malicious software to certain devices in Ukraine, with the intent of ensuring that utility operators could not issue remote commands to bring electricity substations back online.[e]

[52] According to the Department of Transportation officials, attacks on vessels' GPS occur worldwide.

Potential Impact	Description[a]	Example
Manipulation of control	Command messages are used in OT networks to give direct instructions to devices. Attackers may send unauthorized command messages to instruct industrial control system devices to perform actions outside their desired functionality for process control.	In 2015, during the Ukrainian attacks, Russian attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers.[e]

Source: Prior GAO work and summary of relevant information from the MITRE ATT&CK® Matrix for Enterprise and Matrix for Industrial Control Systems. | GAO-25-107244

[a] These tactics that affect OT are not mutually exclusive. Some tactics may be used in conjunction with one another.

[b] SANS Industrial Control Systems, *ICS CP/PE (Cyber-to-Physical or Process Effects) (case study paper): German Steel Mill Cyber Attack* (Rockville, Maryland: Dec. 30, 2014).

[c] Dragos, EKANS Ransomware and ICS Operations https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.(accessed November 25, 2020).

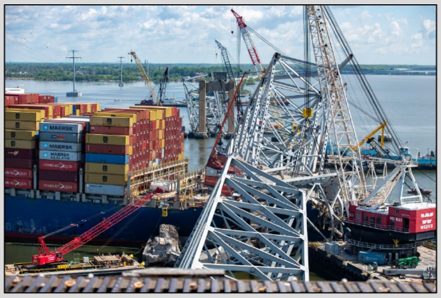
[d] Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Energy, *Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector*, Alert (AA22-083A) (Mar. 24, 2022).

[e] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, D.C.: Mar. 18, 2016).

Further, Coast Guard officials and several nonfederal organizations we met with told us that the effects of a successful cyberattack on OT systems and GPS could be severe. For example,

Francis Scott Key Bridge Collapse

According to a preliminary report from the National Transportation Safety Board, in 2024, a major bridge in Baltimore, Maryland collapsed after a non-cyber incident where a vessel lost power and subsequently could not avoid impact with the bridge causing fatal injuries to six construction crewmembers. The Coast Guard classified the accident as a major marine casualty event. Coast Guard officials told us that a cyberattack on OT used by a large vessel could have the potential to create a similar situation.



Source: National Transportation Safety Board; Defense Visual Information Distribution Service, U.S. Navy photo by Mass Communication Specialist Petty Officer 2nd Class Christine Montgomery. | GAO-25-107244

- Coast Guard officials and one nonfederal organization we met with told us that a cyberattack on OT used by a large vessel could cause that vessel to crash into a large bridge. This could result in an impact similar to the March 2024 non-cyber incident in which a major bridge in Baltimore, Maryland collapsed. (See the sidebar for more details on this incident.) Researchers from Rutgers University raised the possibility of a similar attack that blocks a port entryway.[53]
- Researchers from Rutgers University also raised the possibility of a cyberattack causing an explosion on a vessel carrying hazardous materials while docked in a facility.[54]
- One nonfederal organization we met with told us that vessels could be lucrative targets for threat actors. Researchers from Rutgers University have also raised the possibility of such an attack in which threat actors could seek to disrupt a shipboard OT system and stop a vessel until a ransom is paid.[55]

However, as discussed in more detail later in this report, Coast Guard officials that we interviewed were not aware of any comprehensive federal risk assessments of cyberattacks on (1) OT systems used by vessels or (2) GPS used by the MTS. As such, the likelihood and impact of cyberattacks on these systems are unknown.

Coast Guard Does Not Maintain Accurate Information on Cyber Incidents

To make informed decisions regarding cybersecurity, it is important that Sector Risk Management Agencies acquire, store, and retrieve pertinent information about incidents reported in their sectors to inform future risk management decisions.[56] Relevant regulations define a “cyber incident” as an occurrence that actually or imminently jeopardizes, without lawful

[53] Roberts et. al, *Combined Cyber and Physical Attacks on the Maritime Transportation System*. The researchers operated under separate grants from the Department of Homeland Security and National Science Foundation. Those researchers also described several possible scenarios in which this could be done, such as attacking the (1) electronic chart display and information system of a vessel during a “night-time passage through a narrow canal” to alter the system’s display to look normal while the actual ship’s position sends the vessel aground; or (2) hull stress monitoring system, to create an imbalance when containers are loaded without the crew’s knowledge.

[54] Roberts et. al, *Combined Cyber and Physical Attacks on the Maritime Transportation System*.

[55] Ibid.

[56] As previously mentioned, sector risk management agencies are federal entities responsible for providing institutional knowledge and specialized expertise for enhancing and protecting the cybersecurity of critical infrastructure.

authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[57]

While the Coast Guard—a lead risk management agency for the MTS subsector—maintains a list of cybersecurity incident information pertaining to the MTS, not every event included in the Coast Guard's list appears to meet the above definition of a cyber incident.[58] For example:

- Twenty-one entries are identified as an email server related vulnerability but do not have other information to clarify the event, such as what specifically occurred and whether the vulnerability was exploited.[59]
- Three events have conflicting information about whether they pertain to the MTS. For example, one event is categorized in the Coast Guard's list as pertaining to the MTS, but also includes a description suggesting that the event pertains to the Water and Wastewater Systems sector.
- One of the events is listed as a "non-incident" with the attack vector listed as "software update," and no additional clarifying information.
- One of the events is categorized as "physical security," and does not have other information to clarify the event, such as whether any cyber tactics and techniques were used.

[57] 33 C.F.R. §§ 6.01-8 (incorporating by reference the definition of "incident" in 44 U.S.C. § 3552(b)(2)); 101.615 (effective July 16, 2025, per Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025)). Coast Guard guidance issued in February 2024 clarified that MTS owners and operators should report those incidents that lead to or, if still under investigation, could reasonably lead to any of the following: (1) substantial loss of confidentiality, integrity, or availability of information systems, networks, or operational technology; (2) a disruption or significant adverse impact on the MTS stakeholder's or MTSA-regulated entity's ability to engage in business operations or deliver goods, or services; (3) disclosure or unauthorized access directly or indirectly to non-public personal information; or (4) potential operational disruption to other critical infrastructure systems or assets. U.S. Coast Guard, *Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents*, Navigation and Vessel Inspection Circular No. 02-24 (Feb. 21, 2024). New reporting requirements will take effect on July 16, 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[58] Coast Guard provided a spreadsheet with over 190 entries pertaining to cybersecurity incidents in the MTS since July 2019.

[59] These email-related vulnerabilities were labeled with the incident type of "Exchange Server Vulnerability."

At the conclusion of our review, the Coast Guard provided procedures, stating that they guide the agency in identifying and tracking cybersecurity incident data. The procedures describe a high-level process for conducting incident response investigations, reporting relevant information to stakeholders, and recording pertinent data in MISLE. However, they do not outline the steps or procedures needed to maintain an accurate list of cybersecurity incidents impacting the MTS. Until the Coast Guard develops and implements procedures to ensure the accuracy of the incident information it identifies and tracks, the service's ability to fully assess MTS cyber risks and their impact and make informed decisions on how to prevent or mitigate incidents will be limited.

Coast Guard Assists and Oversees MTS Cybersecurity Efforts but Cannot Readily Access Complete Inspection Data

Coast Guard Provides Technical Assistance to MTS Owners and Operators to Mitigate Cybersecurity Risks

MTS owners and operators are required to identify cybersecurity-related vulnerabilities in security assessments and document controls or measures to mitigate these vulnerabilities in their security plans. The Coast Guard also offers voluntary technical assistance to MTS owners and operators to assist them in their efforts to mitigate cybersecurity risks.[60] This includes providing cybersecurity specialists to advise MTS owners and operators on cybersecurity practices, cyber protection teams to provide direct technical services upon request, and voluntary guidelines to help with implementing key cybersecurity practices. Once MTS owners and operators submit their security plans to the Coast Guard, the Coast Guard reviews and approves the plans, while ensuring that the plans include controls or measures that mitigate the vulnerabilities identified in the corresponding security assessments. Additionally, the Coast Guard and Department of Transportation share

[60] See 46 U.S.C. § 70103(c)(3)(C)(v), (c)(3)(D). As of July 2027, most MTS owners and operators will also be required to submit separate cybersecurity-specific plans to the Coast Guard. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025) (promulgating 33 C.F.R. § 101.630). At the time of our review, federal regulations did not include minimum cybersecurity requirements. As such, the technical assistance we reviewed did not address these requirements, which were promulgated in Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

cyber threat information with these owners and operators to help mitigate cybersecurity risks to the MTS.

Cybersecurity specialists collaborate and provide technical assistance and guidance within their area of responsibility (e.g., Coast Guard sector) to field-level administrators of the Area Maritime Security Committee, as well as other committees, that include governmental agencies and MTS owner and operator members. These specialists coordinate with MTS owners and operators, including developing and maintaining relationships with stakeholders such as state and local government agencies (e.g., state highway patrol and county office of emergency management), and private industry to strengthen cybersecurity. Cybersecurity specialists are also responsible for leading responses to crises or urgent situations to assist in mitigating immediate and potential cybersecurity threats when requested.

Additionally, cybersecurity specialists provide professional expertise, assistance, and recommendations internally to the Coast Guard District Commander, Captain of the Port, and other Coast Guard staff. For instance, cybersecurity specialists are to:

- assist the Coast Guard’s facility and vessel inspectors with the cybersecurity portion of their security inspections;
- review and analyze new laws, regulations, and other directives impacting cybersecurity within the MTS;
- develop, coordinate, plan, and implement new cybersecurity-related policy changes and directives as necessary;
- assist with training content development, communications, and training program management in support of cybersecurity awareness; and
- assist with sharing information related to cybersecurity threats and incidents.

Distinct from cybersecurity specialists, Coast Guard’s cyber protection teams deploy in support of operational commanders and MTS owners and operators through three core mission types: assessment, threat hunting, and incident response (see table 5).

Table 5: Number and Type of Voluntary Services Coast Guard Cyber Protection Team Provided from January 2021 through September 2024

Voluntary Service	Number provided[a]	Description
Assessment	60	Assessments include penetration tests that emulate threat actors by employing their attack techniques to find vulnerabilities in an Information Technology (IT) or Operational Technology (OT) system. These techniques allow the cyber protection teams to show maritime owners and operators how an attacker could move from initial access to full compromise of the network. During an assessment, the team identifies vulnerabilities and can make general recommendations to mitigate them.
Threat hunting	21	Threat hunting is a deliberate approach with highly tailored deployment of network, endpoint, and cloud-environment detection tools. Cyber protection teams search networks and systems to identify compromises that have already bypassed network defenses and established a foothold, prior to causing an incident. Attackers may remain in networks for months, collecting data, searching for confidential material, and moving across systems to achieve their objectives. These teams can report compromises to IT and OT systems.
Incident response	9	Incident response is responding to an actual cyber incident and occurs more rapidly than threat hunting. The methods used (e.g., detection tools) are dependent on the specific incident. Cyber protection teams describe how the threat entered a system, determine whether the threat is still present, and provide any analysis. During an active incident, Coast Guard officials typically use the affected entity's systems and data to provide guidance. Following an incident, Coast Guard recommends that the affected entity utilize the team's cybersecurity assessment or threat hunting services to ensure that the incident no longer poses a risk.

Source: Coast Guard. | GAO-25-107244

[a]The Coast Guard first formed cyber protection teams in 2021.

Coast Guard's cyber protection team services are available to MTS owners and operators upon request.[61] According to Coast Guard officials, cyber protection teams provided these services within three of the four sectors that we visited: Houston/Galveston, Los Angeles/Long Beach, and New York.[62] For instance, officials in Coast Guard's New York sector told us that these teams conducted assessments of a waterway facility, port authority, bridge authority, and some of the larger ferry systems at the request of owners and operators.

Coast Guard officials at Marine Safety Unit Paducah stated that the cyber protection teams have not conducted any cybersecurity assessments for MTS owners and operators within their area of responsibility in the Ohio

[61] Cyber protection teams are deployable teams from the Coast Guard's office of Cyber Command who provide direct technical assistance to MTS owners and operators through assessment, threat hunting, and incident response.

[62] We conducted in-person site visits with the New York and Houston/Galveston sectors, and virtual site visits with the Los Angeles/Long Beach and Ohio Valley sectors.

Valley sector. The Coast Guard Ohio Valley sector officials and Area Maritime Security Committee members explained that the likelihood of a cybersecurity incident is relatively low for smaller companies in Paducah, Kentucky—such as an operator of a small vessel that does not maintain complex IT or OT systems. In addition, Area Maritime Security Committee members told us that cybersecurity would have much more of an impact on larger operations and therefore is typically addressed by a company's headquarters rather than its local facilities.

Because these services are voluntary, MTS owners and operators may not elect to use these services for various reasons. For instance, owners and operators from one sector we visited told us that some entities may have concerns when a regulatory agency, such as the Coast Guard, provides voluntary services that require access to a regulated entity's computer networks and systems. There is also reluctance to accept assistance, such as those provided by the cyber protection teams, that go beyond current Coast Guard cybersecurity-related requirements. Furthermore, according to Coast Guard headquarters officials, some MTS owners and operators prefer assistance from a third-party instead of the service's cyber protection team, despite the Coast Guard's services being provided at no-cost. Additionally, according to the Coast Guard, some private MTS owners and operators may not want to invest significant resources for enhancements to their information technology equipment.

Coast Guard Provides Voluntary Guidelines for Implementing Key Practices and Shares Cyber Threat Information to Mitigate Cybersecurity Risks

Although MTSA requires MTS owners and operators to document and address cybersecurity risks in their security plans, the regulations that included minimum cybersecurity requirements were not issued until January of 2025.[63] Accordingly, they did not specify the types of cybersecurity vulnerabilities and mitigating controls to include in MTS owner and operator security plans as this rule will not begin to take effect until July 2025. Therefore, the Coast Guard provided voluntary guidelines on implementing key cybersecurity practices to owners and operators, such as those outlined in the National Institute of Standards and

[63] Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025). In January 2025, Coast Guard finalized its rule on minimum cybersecurity requirements for most MTS owners and operators, which will not begin to take effect until July 2025. Some new requirements go into effect on that date, while the rule allows regulated owners and operators 6 or 24 months from the time of publication to implement other requirements.

Technology (NIST) Cybersecurity Framework.[64] For instance, these guidelines provide details on recommended cybersecurity practices MTS owners and operators should consider when conducting their security assessments and how best to address cybersecurity vulnerabilities in their security plans. Furthermore, the following guidelines refer to using judgment in choosing, interpreting, modifying, and applying the available guidelines to specific cyber-related problems or issues. As discussed below, the Coast Guard and Department of Transportation also rely on a range of methods to facilitate sharing of cyber threat information with critical infrastructure owners and operators in the MTS.

- **Coast Guard Navigation and Vessel Inspection Circular No. 01-20:** *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities* provides guidance to facility owners and operators on how to comply with requirements to assess, document, and address computer system or network vulnerabilities. The Coast Guard also developed the *Maritime Cybersecurity Assessment and Annex Guide* to correspond with this circular and serve as a recommended, voluntary process for identifying and describing cybersecurity vulnerabilities at facilities.[65] According to Coast Guard officials, both the circular and the annex guide, and protections needed to address them, are consistent with the NIST Cybersecurity Framework (see appendix IV for more information about functions outlined in the annex guide).[66]
- **Coast Guard Work Instruction No. 27**. *Vessel Cyber Risk Management Work Instruction* provides guidance to vessel owners

[64] The framework proposes a risk-based approach to managing cybersecurity risk and includes a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors.

[65] The Federal Aviation Administration Reauthorization Act of 2018 amended MTSA to require vessel and facility security plans address cybersecurity risks. Pub. L. No. 115-254, § 1805(d)(2)(D), 132 Stat. at 3535 (codified at 46 U.S.C. § 70103(c)(3)(C)(v)). Simultaneously, the act directed U.S. Coast Guard to "issue voluntary guidance for the management of such cybersecurity risks in each facility security plan." Pub. L. No. 115-254, §1805(c)(2)(B), 132 Stat. at 3535. In response, U.S. Coast Guard issued the *Maritime Cybersecurity Assessment and Annex Guide*.

[66] U.S. Coast Guard, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*, Navigation and Vessel Inspection Circular No. 01-20, February 26, 2020; U.S. Coast Guard, *Maritime Cybersecurity Assessment and Annex Guide (MCAAG)*, January 2023.

and operators on assessing cybersecurity risks.[67] This instruction references the International Maritime Organization's guidelines that adhere to the NIST Cybersecurity Framework.[68] This work instruction describes the NIST framework's key functions and emphasizes basic cyber hygiene practices. Additionally, this guidance includes recommendations for Coast Guard inspectors, including evaluating whether a system failure required for a vessel's navigation or operation is due to a cybersecurity incident (the inspection process is discussed in more detail below).

- **Guidance on facility and vessel inspections.** The Coast Guard developed the *Facility Inspector Cyber Job Aid* to help familiarize facility inspectors with cybersecurity practices at MTS facilities. This facility job aid is also available as guidance to facility owners and operators on the Coast Guard's web site. For instance, the job aid recommends that facility cybersecurity staff should interact with their Area Maritime Security Committee to discuss cybersecurity concerns and obtain best practices. The job aid includes recommended questions inspectors may ask facility owners and operators related to federal regulations, including questions concerning cybersecurity control or measures in a facility security plan.[69] The service also has vessel guidelines distributed and available on its web site to owners and operators that also serve as guidance on cybersecurity practices. These vessel guidelines also include recommended questions inspectors may ask owners and operators related to federal regulations, including questions concerning cybersecurity controls or measures in a vessel security plan. See appendix V for the facility job aid's recommended questions.

The Coast Guard and Department of Transportation, as the co-Sector Risk Management Agencies for the subsector, reported relying on a range of methods to facilitate sharing of cyber threat information with

[67] U.S. Coast Guard, *Vessel Cyber Risk Management Work Instruction*, CVC-WI-027(2), February 18. 2022.; International Maritime Organization, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3/Rev.1, June 14, 2021.

[68] The International Maritime Organization is the United Nations' specialized agency with responsibility for the safety and security of shipping and the prevention of marine and atmospheric pollution by ships. The Maritime Safety Committee Resolution 428(98), *Cyber Risk Management in Safety Management Systems* provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

[69] U.S. Coast Guard, *Facility Inspector – Cyber Job Aid*, Rev. 2, (Washington, D.C.: January 2023).

critical infrastructure owners and operators in the MTS. In particular, the Coast Guard and Department of Transportation collectively relied on six methods to share cyber threat information specifically with the MTS subsector. These methods were (1) cyber threat briefings, (2) threat information products (e.g., alerts and advisories), (3) incident reporting services, (4) incident response services, (5) working groups and councils (e.g., Area Maritime Security Committee's subcommittee on cybersecurity), and (6) information sharing and analysis centers.[70] For example, the Coast Guard produced 19 cyber threat information products from January 2019 through June 2024: eight maritime information sharing bulletins, eight maritime cyber alerts, and three other maritime cyber bulletins on cyber threats.[71] Department of Transportation produced 14 maritime advisories that focused on cybersecurity during that same period.[72]

Coast Guard Oversees Compliance with Cybersecurity Statutory Requirements through Its Security Inspection Process

The Coast Guard's security inspection process for cybersecurity includes reviews of MTS owner and operator cybersecurity-specific portions of their associated security assessment and plan. In addition to these reviews, prior to physically observing a facility or vessel, inspectors can also review a copy at the facility or on board a vessel to ensure that it matches documentation retained by the Coast Guard. As part of the inspection process, the Coast Guard also conducts physical observations of areas where computer workstations are located. However, the Coast Guard does not directly test owner or operator networks or systems as part of the inspection process. According to the Coast Guard, the service conducts two annual security inspections of each regulated facility owner or operator, and the frequency of inspections for each vessel owner or operator vary depending on the type of regulated vessel.

According to Coast Guard officials, during an inspection, inspectors observe physical areas of a facility or vessel for potential risks to

[70] Information sharing and analysis centers are sector-based organizations that facilitate the sharing of cyber and physical threat information between government and the private sector.

[71] For example, the service developed a May 2024 Maritime Information Safety Bulletin highlighting phishing emails that are impersonating Coast Guard personnel. Coast Guard, MSIB Number: 04-24, *Phishing Emails Impersonating U.S. Coast Guard*, (May 7, 2024).

[72] For example, in February 2024, the Department of Transportation produced a maritime advisory that shared emerging cyber threat information on potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure. Department of Transportation, 2024-002-Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence, (Feb. 21, 2024).

cybersecurity, such as openly displayed password information or cellular phones connected to computers. Coast Guard officials stated that inspectors should also ask questions about cybersecurity-related topics such as email communication, security cameras, access gates, and other potential cybersecurity touchpoints. For example, according to the Coast Guard, vessel inspectors look for any operational issues such as when a radar is inoperable or when the vessel's operator last updated the associated software.

According to Coast Guard officials, facility and vessel inspection staff are generally not subject matter experts on cybersecurity. Therefore, Coast Guard officials also told us that cybersecurity specialists may also accompany inspectors during an inspection to answer any technical related questions and advise MTS owners and operators on how to mitigate specific cybersecurity vulnerabilities. Based on these inspection activities, if the Coast Guard determines that an MTS owner or operator is not in compliance with cybersecurity-related requirements in their assessments or plans, it will formally issue an inspection result of deficiency (inspection deficiency).[73]

Based on our review of facility and vessel cybersecurity-related inspection deficiency data associated with Coast Guard's review of required security assessments and plans, these deficiencies can be identified based on a variety of reasons.[74] For instance, one facility inspection deficiency report stated that the entity did not conduct or submit a security assessment that included vulnerabilities related to computer systems and networks. Another facility inspection deficiency report stated that the security plan did not describe how the entity would address vulnerabilities related to network and surveillance equipment. According to Coast Guard, inspection findings can also include the improper use of usernames and passwords (e.g., multiple personnel using the same credentials),

[73] For the purposes of this report, a deficiency is the result of a security inspection for instances when an MTS owner or operator is found by the Coast Guard to be noncompliant with federal statutory or regulatory requirements, including cybersecurity-related requirements. According to Coast Guard officials, the service does not impose fines or other actions on MTS owners and operators in the event of a deficiency related to cybersecurity. Additionally, Coast Guard stated that it monitors corrective actions to ensure they are completed and address any deficiencies. Our review of deficiency data occurred prior to Coast Guard's finalization of minimum cybersecurity regulatory requirements for most MTS owners and operators in January 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[74] We reviewed Coast Guard facility and vessel inspection data from fiscal year 2019 through June 2024.

unsecured IT equipment (e.g., Wi-Fi router), laptops connected directly to servers, and other cyber hygiene-related issues.

According to Coast Guard officials, the scope of an inspection may vary based on the size of the facility or vessel and the complexity of the MTS owner and operator IT and OT system. For example, inspectors might only have an opportunity to interview a facility or vessel owner or operator's safety officer at some locations with smaller operations that do not have dedicated cybersecurity personnel, such as a cybersecurity system officer. However, because some owners and operators of larger facilities or vessels have more complex IT and OT systems, such as a modern cruise ship as shown below in figure 3, inspectors may have an opportunity at these locations to conduct more in-depth interviews with facility or vessel owners or operators' dedicated cybersecurity personnel to ascertain how they meet requirements or implement cybersecurity practices.

Figure 3: Engine Control Room of a Modern Cruise Ship

Source: U.S. Coast Guard photo. | GAO-25-107244

Coast Guard Cannot Readily Access Complete Data on Cybersecurity-related Deficiencies

When Coast Guard inspectors identify a cybersecurity-related deficiency, they record information on these deficiencies for facilities and vessels into their case management system, known as MISLE.[75] However, complete information on these deficiencies is not readily accessible in the system. Although we observed that other program activities are categorized by activity or subtype in the case management system, there is no such category to record cybersecurity deficiencies identified during a facility and vessel inspection. As a result, Coast Guard inspectors enter

[75] Coast Guard designed MISLE to only capture noncompliance with federal regulations.

deficiency information into a free-form narrative text field used for case descriptions (deficiency description field).

While the Coast Guard has issued guidance on how to record cybersecurity-related deficiencies for vessels into this field in the system, our review of vessel inspection data showed that inspectors are not following this guidance. Additionally, Coast Guard's guidelines do not specify text that inspectors should use when recording this information for facilities. Therefore, retrieving cybersecurity deficiency data from the deficiency description field may not yield complete results.

For cybersecurity-related deficiencies resulting from inspections of vessels, Coast Guard guidance specifies text that inspectors should use when entering this information into the case management system. According to this guidance, inspectors are instructed to enter "Cybersecurity-MTSA" at the beginning of their deficiency description field related to cyber to aid with data analysis. However, of the 157 publicly available vessel inspection deficiency records we reviewed, we determined that 31 were likely related to cybersecurity based on the narrative in the deficiency description field.[76] However, none of these 31 records included the text "Cybersecurity-MTSA" anywhere in the deficiency description field. For instance, one inspection deficiency stated that the inspector observed a viewable username and password list on the vessel's bridge. In another example, the inspection deficiency stated that the owner or operator had not updated its operating system. Lastly, another example of a related deficiency stated the crew of a vessel connected personal phones to the vessel's network.

For cybersecurity-related deficiencies resulting from inspections of facilities, Coast Guard's guidelines do not specify text that inspectors should use when recording this information into the case management system. The Coast Guard identified 145 records that were deemed to be cybersecurity-related by querying the deficiency description fields for the

[76] Our review included records from fiscal year 2019 through June 2024. To identify the 157 data records, we selected those records with deficiency descriptions related to cybersecurity from a total of over 155,000 data records representing all types of vessel inspection deficiencies. We also selected other records for review from Coast Guard program components or activities designated with deficiency codes such as "Other/International Safety Management," or deficiency description fields containing frequently used, related terms such as "cyber." We determined that a record was related to cybersecurity if the deficiency description field described gaps that would impact the cybersecurity of technology used on a vessel, such as protecting networks, devices, or data from unauthorized access or criminal use.

key words “cyber,” “computer,” and “network.”[77] For instance, one deficiency record stated that the facility owner did not include controls to mitigate risks to their IT system in the security plan. Additionally, another deficiency report stated that the facility security assessment did not address vulnerabilities associated with computers and networks.

Given that vessel inspectors are not following guidance for documenting cybersecurity-related deficiencies and a lack of guidance for facility inspections, we determined that Coast Guard’s cybersecurity-related deficiency data are likely not complete. Specifically, since there are numerous terms that inspectors can use to describe cybersecurity vulnerabilities and mitigating controls or measures in the case management system, there is no assurance that the deficiency entries retrieved in its case management system list all applicable cybersecurity-related deficiency data.[78] Further, in the absence of a standardized way to record these deficiencies, the Coast Guard’s method for manual entry of facility and vessel data into its case management system is vulnerable to inconsistencies. More specifically, Coast Guard officials also told us that word searches may not retrieve all cybersecurity-related deficiencies if inspectors misspell or neglect to add appropriate cybersecurity related terms or identifiers.[79] To have assurance of complete deficiency data for facilities and vessels, the Coast Guard would have to manually review all inspection case deficiency description fields to determine whether they are related to cybersecurity.

The Coast Guard’s Commandant Instruction 5200.10A, *Management’s Responsibility for Internal Control* directs the agency’s management to establish, maintain, review, and improve internal controls through active involvement in assessments that support assurances that the Coast Guard is accomplishing its intended objectives. In addition, GAO’s *Standards for Internal Control in the Federal Government* states that

[77] Our review included records from fiscal year 2019 through June 2024. Coast Guard queried its facility inspection deficiency data by searching a free-form text field (deficiency description field) using the terms “cyber,” “computer,” and “networks” to retrieve data records that contained at least one of these terms.

[78] Based on our analysis of facility inspection results, the Coast Guard’s method for extracting data on cybersecurity-related deficiencies also retrieved a few cases not related to cybersecurity. Given these results of their method, to ensure complete data, the Coast Guard would have to manually review each case deficiency description.

[79] A data query method that does not retrieve all applicable data records needed by management to conduct control activities (e.g., monitoring) is not a method that produces complete data because there are no defined data fields or categories in MISLE.

management should clearly document significant events in a manner that allows the documentation to be readily available for examination, by recording data to maintain their relevance and value to management in controlling operations and making decisions. To maintain relevant data that helps management oversee operations and make informed decisions, internal control standards state that management should design an information system considering the detailed information required for each of the entity's operational processes and the validity of the information (completeness of the data).

Coast Guard officials told us that its case management system was created before the incorporation of cybersecurity into the federal statute applicable to the service's security inspections. In addition, Coast Guard officials also told us that they would benefit from having the ability to retrieve in a timely fashion all cybersecurity-related deficiencies identified during their inspections, through improved capabilities in its case management system. For instance, officials stated this information could inform future job aids and guidance provided to MTS owners and operators. The officials noted that having a standard method to document all cybersecurity-related deficiencies, such as dedicated data categories or fields, would be helpful.

According to the Coast Guard, its existing case management system is undergoing a multi-year modernization project entitled Coast Guard Case Management.[80] As we reported in July 2020, this system has longstanding issues including data errors, incomplete or missing records, and inconsistent data entry.[81] We made four recommendations in this report related to improving this system, including assessing and addressing data errors and inconsistent entries, developing a plan for improving the consistency and accuracy of the data, identifying needed system enhancements, and selecting the preferred solution for these enhancements to meet mission needs. As of October 2024, the Coast Guard has partially implemented our recommendation related to data

[80] Coast Guard officials stated that the MISLE database is currently undergoing a multi-year modernization program: *Coast Guard Case Management*. The overall estimated completion date for this program is December of 2028.

[81] GAO, *Actions Needed to Ensure Investments in Key Data System Meet Mission and User Needs*, GAO-20-562 (Washington, D.C.: July 16, 2020). In this 2020 report, we analyzed Coast Guard strategic planning and program performance reports to identify MISLE's role in achieving mission results, as well as any MISLE-specific issues that the Coast Guard identified that hindered its achievement of results. Additionally, we interviewed Coast Guard officials about MISLE data entry and quality. We did not report on any cybersecurity-specific issues in 2020.

errors and inconsistent entries, and the service has fully implemented our recommendation related to identifying needed system enhancements. For the remaining two recommendations, the Coast Guard told us that it plans to take actions to implement them, and we are continuing to monitor their progress. However, implementing these recommendations would not address the concerns we have raised in this report.

By ensuring that its case management system provides ready access to complete data on the number and types of cybersecurity-related deficiencies identified during security inspections, the Coast Guard would be better positioned to conduct its oversight of and help address cybersecurity risks within the MTS. Additionally, these data could help inform future job aids, guidance, and implementation and enforcement of the new regulations for MTS owners and operators.[82]

Coast Guard Has Not Fully Defined a Strategy to Address Maritime Transportation System Cybersecurity

While the Coast Guard has taken steps toward outlining strategy for addressing cyber threats to the MTS, it does not fully address all key characteristics needed for an effective national strategy. Delegated by DHS as the lead risk management agency for the MTS subsector, the Coast Guard has led efforts to develop and implement a cybersecurity strategy, including an overarching strategy and two agency plans. In August 2021, the Coast Guard developed a *Cyber Strategic Outlook* that lays out a strategy for its cybersecurity activities.[83] The strategy is organized across three lines of effort, including one line of effort focused on managing cyber risk to the MTS subsector.

To accompany the strategy, the Coast Guard developed a subsequent implementation plan in October 2023 that describes the initiatives and supporting actions to fulfil the *Cyber Strategic Outlook* as well as the milestones and responsible offices for implementing each action.[84] Further, in April 2023, DHS and the Coast Guard developed a Maritime Security Plan as part of the Biennial National Strategy for Transportation

[82] As discussed above, in January 2025, the Coast Guard promulgated new cybersecurity regulations for most MTS owners and operators, which will be effective July 16, 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[83] U.S. Coast Guard, *Cyber Strategic Outlook* (August 2021).

[84] U.S. Coast Guard, *Cyber Strategic Outlook Implementation Plan* (October 2023).

Security, that includes risk-based priorities and activities to protect the MTS, including those related to cyber.[85]

National strategies are critical tools used to help address longstanding and emerging issues that affect national security and economic stability. In 2004, we identified a set of desirable characteristics for effective national strategies.[86] However, as presented in table 6, the *Cyber Strategic Outlook*, its implementation plan, and the *Maritime Security Plan* do not fully address all key characteristics needed for a national strategy.

Table 6: GAO Assessment of How Coast Guard's Strategy and Two Accompanying Plans Address the Key Characteristics of a National Strategy

Characteristic	Definition	GAO assessment
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	●
Problem definition and risk assessment	Addresses the particular national problems that the strategy is directed towards and assesses the risks to critical assets and operations—including the threats to, and vulnerabilities of, critical operations.	◑
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability.	◑
Resources and investments	Addresses what the strategy will cost, and the types of resources and investments needed.	◑
Roles, responsibilities, and coordination	Addresses who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts.	◑

Legend: ● Fully addresses all aspects of the characteristic. ◑ Partially addresses some but not all of the characteristic. ○ Does not address any aspects of the characteristic.

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

Collectively, the strategy and two accompanying plans fully addressed the key characteristic related to purpose, scope, and methodology, but did not fully address the other four characteristics. Specifically:

Purpose, scope, and methodology. Collectively, the strategy and two plans fully address the characteristic of outlining their purpose, scope, and methodology. For example, the strategy explains that it was produced to, among other things, ensure Coast Guard readiness for cyberspace missions and secure the maritime transportation sector. In

[85] Department of Homeland Security, *Appendix B: Maritime Security Plan: Biennial National Strategy for Transportation Security*, April 18, 2023.

[86] GAO-04-408T.

addition, the implementation plan explains that the Coast Guard held workshops with various cyberspace stakeholders to develop the plan's actions that fulfill activities within the strategy.

Problem definition and risk assessment. The strategy and two plans partially address the characteristic of defining the problem and performing a risk assessment. In particular, the strategy and two plans collectively identify the problems they were intended to address. For example, the strategy highlights cyberattacks on the MTS as a key problem that it is designed to address. Further, the strategy and two plans collectively assess several cybersecurity risks to the MTS. For example, the strategy recognizes that there are complex risks and vulnerabilities facing IT/OT networks in the MTS. As another example, the Maritime Security Plan highlights several cyber risks to the MTS, including unintentional incidents due to operator error or accidental software or hardware failures.

However, neither the strategy nor the two plans fully assessed relevant cybersecurity risks to the MTS. For example, neither the strategy nor the two plans analyzed the threat of a cyberattack involving the use of artificial intelligence. As previously mentioned, these types of cyberattacks pose an increasing risk to the MTS and may continue to evolve in sophistication and scope as the technology evolves. In addition, neither the strategy nor the two plans specifically assess the vulnerability of the MTS to a cyberattack specifically involving OT on a vessel, or attacks involving GPS such as jamming or spoofing.

Goals, subordinate objectives, activities, and performance measures. The strategy and two plans partially address the characteristic of outlining goals, subordinate objectives, activities, priorities, milestones, and performance measures. In particular, the strategy and two plans collectively outline the goals (e.g., lines of efforts), objectives (e.g., initiatives), activities (e.g., action items), priorities, milestones, and related performance measures for addressing cybersecurity risks facing the MTS.

However, the strategy and two plans did not always include milestones or performance measures with measurable targets for all its relevant goals, objectives, and activities. For example, the *Cyber Strategic Outlook* and implementation plan do not specify performance measures for its goals, objectives, and activities. Further, the *Maritime Security Plan* did not specify milestones for its goals, objectives, and activities. In addition, considering the previously identified gaps in the analysis of cybersecurity risks, it is unclear to what extent the stated plans' goals, objectives, and activities sufficiently address MTS cybersecurity risks.

Resources and investments. The strategy and two plans partially address the characteristic of describing resource and investment needs. Specifically, the strategy and two plans collectively identify high-level resources and investments needed to address the strategy overall. For example, the strategy highlights the need for the Coast Guard to sustain significant investments in their cyber workforce to continue to address cyber threats. However, the strategy and two plans do not fully identify resource and investment needs that are specific to carrying out specified goals, objectives, and activities. For example, the implementation plan includes an action item focused on establishing a mature cyber field support program; however, it does not describe the resources or investments needed to meet this action item.

Further, the strategy and two plans do not describe specific investment costs. For example, the implementation plan describes the need to develop training on cybersecurity fundamentals; however, it does not identify the specific costs associated with this investment. Further, given the previously discussed gaps in risk analysis, goals, and objectives, it is unclear to what extent the identified resource and investment needs are sufficient to address MTS cybersecurity risks.

Roles, responsibilities, and coordination. The strategy and two plans partially address the characteristic of describing roles, responsibilities, and coordination mechanisms for carrying out the goals, objectives, and activities. Specifically, the strategy and two plans collectively identify the responsible offices and their roles for implementing goals, objectives, and activities. For example, the implementation plan specifies responsibilities for the Assistant Commandant for Prevention Policy to lead efforts, with support from the Coast Guard Office of Port and Facility Compliance, to establish an information sharing channel with MTS owners and operators.

However, the strategy and two plans did not always identify the responsible offices and their roles for implementing all of its relevant goals, objectives, and activities. For example, the *Maritime Security Plan* did not identify the responsible offices and their roles for implementing its specified goals, objectives, and activities. Further, neither the strategy nor the two plans addressed specific mechanisms by which these offices will coordinate such as specific tools or processes they can use to coordinate internally.

Coast Guard officials acknowledged that their cyber strategy and plans did not address all the identified key characteristics. According to Coast Guard officials, one reason that the strategy and two accompanying plans did not fully address all characteristics was because the service believed their strategy and plans addressed the characteristics to the extent they could. For example, Coast Guard officials stated that there is a limit to how much the service can develop strategies and plans to address evolving and shifting cyber risks to the MTS.

As we previously reported in 2004, including the key characteristics of a national strategy helps to enhance the usefulness of strategies and plans as guidance for resource and policy decision-makers and better ensure accountability. Addressing all of the key characteristics of a national strategy would better position Coast Guard to ensure that its actions and its resources are addressing the highest cybersecurity risks.

Coast Guard Has Not Fully Addressed GAO Recommendations or Implemented Leading Practices on its Cyber Workforce

Coast Guard Has Not Fully Addressed Prior GAO Recommendations on Cyber Personnel Vacancy Challenges

The Coast Guard has taken steps to address vacancy gaps for key cyber personnel but faces continuing challenges fully staffing these positions. Specifically, in September 2022, we found that the Coast Guard had vacancy gaps for key cyber personnel—including personnel that help to mitigate risks in the MTS. We made four key recommendations aimed at addressing these vacancy issues.[87]

Although the Department of Homeland Security concurred with our recommendations from September 2022, the Coast Guard had not fully addressed them as of October 2024. Specifically, Coast Guard officials told us that they have taken several initial actions to address vacancy challenges. For example, as previously mentioned, the Coast Guard completed a Manpower Workforce Requirements Determination in September 2024 for its office of Cyber Command, but otherwise has not

[87] The four recommendations were for the Coast Guard to (1) assess and determine the staffing levels needed to meet its cyberspace mission demands; (2) establish a strategic workforce plan for its cyberspace workforce; (3) incorporate data from the Cyber Mission Specialist rating to inform its strategic workforce planning; and (4), develop metrics for recruitment of enlisted and all civilian cyberspace personnel. See GAO-22-105208.

implemented our recommendations and noted that they are in various stages of taking actions. According to Coast Guard policy, workforce requirements determinations help the service better understand the effects of existing, new, or modified mission or business processes on the workforce, including those to address cyber threats.

Nevertheless, the service continues to face vacancy gaps (see table 7). In particular, the Coast Guard identified a number of vacancies within its cybersecurity workforce, including eight vacant positions for its cybersecurity specialists and 23 vacant positions for its cyber protection teams—representing a 15 percent vacancy rate for each of the two positions.[88]

Table 7: Number of Coast Guard Authorized, Filled, and Vacant Cyber Workforce Positions as of October 2024

Cyber workforce	Authorized	Filled	Vacant	Vacancy rate
MTSS-C (cybersecurity specialists)[a]	55	47	8	15%
Cyber Protection Teams	156	133	23	15%

Source: GAO analysis of Coast Guard workforce data. | GAO-25-107244

[a]Maritime Transportation Security Specialist-Cyber

Until the Coast Guard addresses these recommendations, it will not be optimally positioned to recruit for difficult-to-fill cybersecurity positions and retain skilled personnel. Compounding these issues and as discussed in more detail later in this report, the Coast Guard has not consistently ensured that its personnel have the expertise needed to address all MTS cyber risks.

[88] According to Coast Guard officials, there are 117 authorized positions, with 107 filled positions and 10 vacancies for its active duty cyber protection teams. In addition, there are 39 authorized positions, with 26 positions filled and 13 vacancies for its reserve cyber protection team. For the purposes of this report, we count the reserve and active duty positions under one cyber protection team header.

Coast Guard Personnel with Cyber Responsibilities Do Not Have Performance Competencies That Address All Cybersecurity Risks

The Coast Guard has taken steps to improve some cyber competencies for its personnel with MTS cyber responsibilities, including cyber mission specialists, cyber protection teams, facility inspectors, and vessel inspectors.[89] However, it has not fully implemented leading practices to assess cyber competencies that would help ensure these personnel are able to effectively carry out their duties and address all cybersecurity risks.

We have previously reported on leading practices that highlight the importance of ensuring that staff have the performance competencies needed to effectively carry out their role and address risk.[90] However, the Coast Guard has not fully addressed these leading practices for these personnel. See table 8 for the leading practices and the extent to which the Coast Guard has addressed them.

Table 8: GAO Assessment on How Coast Guard Addressed Leading Practices for Cybersecurity-Related Performance Competencies

Leading Practice	Definition	GAO Assessment
Develop competency requirements	An agency should develop a set of future competency requirements, such as defining position descriptions, for its cyber workforce including leadership positions.	◑
Assess gaps in competencies	An agency should periodically assess gaps between current competencies and future needs for its cyber workforce.	○
Address gaps in competencies	An agency should develop and implement plans to address competency gaps (e.g., plans for training).	○

Legend: ● Fully addresses all aspects of the leading practice. ◑ Partially addresses some but not all of the leading practice. ○ Does not address any aspects of the leading practice.

Source: GAO analysis of Coast Guard's workforce planning activities. | GAO-25-107244

[89] As previously mentioned, the Coast Guard relies on both cyber and non-cyber personnel to help mitigate maritime cyber risks. In particular, the Coast Guard relies on cyber specialists at the Captain of the Port level to advise MTS owners and operators on cybersecurity best practices and cyber protection teams from Coast Guard Cyber Command to provide direct technical assistance through assessment, threat hunting, and incident response. The Coast Guard also relies on non-cyber personnel within the agency to perform certain cybersecurity oversight responsibilities of MTS owners and operators. This includes vessel and facility inspection staff.

[90] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019). The eight key information technology workforce planning activities are (1) establish and maintain a workforce planning process; (2) develop competency and staffing requirements; (3) assess competency and staffing needs regularly; (4) assess gaps in competencies and staffing; (5) develop strategies and plans to address gaps in competencies and staffing such as training; (6) implement activities that address gaps; (7) monitor the agency's progress in addressing gaps; and (8) report to agency leadership on progress in addressing gaps.

- **Develop competency requirements.** Coast Guard partially addressed this practice for two of its personnel (cyber protection teams and cyberspecialists) and did not address this practice for the remaining two (facility and vessel inspectors). Specifically, Coast Guard developed performance competencies in its position descriptions for cyber protection teams and cyberspecialists that help address cyber risks to enterprise IT. However, the competencies listed in the position descriptions that we reviewed do not address all cyber risks—particularly those pertaining to OT and GPS. Further, the position descriptions for Coast Guard's facility and vessel inspectors do not include competencies related to mitigating cyber risks to the MTS.
- **Assess gaps in competencies.** Coast Guard did not assess gaps in competencies for all four of its personnel that address MTS cyber risks.[91] Specifically, Coast Guard has not assessed gaps in competencies for its cyber protection teams and cyber specialists. Further, Coast Guard has not assessed gaps in competencies for its facilities inspectors and its vessel inspectors.
- **Address gaps in competencies.** Coast Guard did not develop and implement plans for addressing gaps in competencies for all four of its personnel that address MTS cyber risks. Additionally, since the Coast Guard did not assess competency gaps for its cyber protection teams, cybersecurity specialists, and facility and vessel inspectors, the Coast Guard is not positioned to address any competency gaps that might exist for these personnel.

According to Coast Guard officials, the service has not addressed gaps in its workforce because it was waiting for the rulemaking on minimum cybersecurity requirements for MTS owners and operators to be

[91] The Coast Guard refers to the determination process as a Workforce Requirements Determination. According to the *Coast Guard's Manpower Requirements Manual* issued in November of 2020, it stated that the process starts with a workforce analysis (or assessment) that defines both the number of workers and the necessary mix of skills for the positions required. The determination used results from this analysis to identify the number and type of positions required to meet mission-based capability requirements. Currently, according to the *Coast Guard's Workforce Requirements Instruction* issued in August of 2024, the workforce requirements determination includes identifying the number and type of positions required to accomplish the Coast Guard's missions. Specifically, the instruction states that workforce requirements determinations provide a means for leadership to understand the effect on the workforce of existing, new, or modified missions or business processes. The determination process includes a workforce assessment, which determines and documents the required workforce or labor hours. The determination uses results from this assessment to identify the number and type of positions a unit (i.e., organized groups of Coast Guard personnel with a similar purpose) requires to meet mission-based capability requirements.

finalized.[92] Coast Guard officials said once requirements are in place, the service will work towards evaluating the tasks that personnel are expected to perform and determine the best training and performance support based on the tasks' difficulty, importance, and frequency. As the rule was finalized in January 2025 and will begin to take effect in July 2025, and in light of the significant cyber risks facing the MTS, it is important that Coast Guard address these weaknesses as soon as possible. Until the Coast Guard fully develops competency requirements for all its personnel with MTS cyber responsibilities and addresses any identified gaps, the service will not have assurance it is effectively mitigating cyber risks to the MTS.

Conclusions

The Coast Guard plays a vital role in protecting the nation's waterways, ports, and vessels. But the technology underpinning the MTS is vulnerable to highly damaging cyberattacks. However, the Coast Guard's lack of procedures for cataloguing cyber incidents has left the service without an accurate summary of such incidents. Implementing procedures to identify and track accurate cybersecurity incident information would help strengthen Coast Guard's ability to prevent or mitigate disruptions that could jeopardize billions in critical commerce.

Without the ability to readily access complete information on cybersecurity-related deficiencies identified during security inspections, the Coast Guard will be limited in its ability to oversee the extent to which MTS owners and operators comply with cybersecurity-related requirements, including cybersecurity requirements that will begin to take effect July 2025. By updating its case management system to provide ready access to complete information, the Coast Guard would be better positioned to fully understand the scope and type of cybersecurity risks MTS owners and operators have identified. Such information could also help the Coast Guard identify any patterns or trends to help inform future job aids and cybersecurity guidance it provides to owners and operators.

Additionally, without a cybersecurity strategy and plan that addresses all of the key characteristics needed to implement an effective national strategy, including a full assessment of cybersecurity risks to the MTS, the Coast Guard will not be positioned to fully confront these risks. Additionally, decision-makers will have limited guidance for allocating

[92] See Cybersecurity in the Marine Transportation System, 89 Fed. Reg. 13,404 (Feb. 22, 2024). Coast Guard officials provided us with this information in October 2024. The rule was finalized on January 17, 2025, and will take effect on July 16, 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

resources to priority risks. Moreover, updating its strategy and plan would help ensure accountability for efforts to address priority risks.

Finally, fully implementing leading workforce planning activities could help the Coast Guard ensure its personnel have the competencies to help manage key cyber risks to the MTS. Not having a comprehensive understanding of its cyber workforce competency needs limits the Coast Guard’s ability to make informed decisions and plan for staffing needs. Developing competency requirements for all its personnel with MTS cyber responsibilities and addressing any identified gaps could improve Coast Guard’s efforts to effectively manage cyber risks to the MTS.

Recommendations for Executive Action

We are making the following five recommendations to the Coast Guard:

The Commandant of the Coast Guard should develop and implement documented procedures to ensure the accuracy of cybersecurity incident information that the service identifies and tracks. (Recommendation 1)

The Commandant of the Coast Guard should ensure that its case management system for facility and vessel security inspections provides ready access to complete data on specific cybersecurity deficiencies identified during those inspections. (Recommendation 2)

The Commandant of the Coast Guard should 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. (Recommendation 3)

The Commandant of the Coast Guard should 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. (Recommendation 4)

The Commandant of the Coast Guard should, 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. (Recommendation 5)

Agency Comments

We provided a draft of this report to DHS and DOT for review and comment. In its comments, reproduced in appendix VI, DHS concurred with all five of our recommendations and described the Coast Guard’s planned actions to address them. DHS and DOT also provided technical comments, which we incorporated as appropriate.

Regarding our first recommendation that the Commandant of the Coast Guard develop and implement documented procedures to ensure the accuracy of cybersecurity incident information that the service identifies and tracks, DHS concurred. The Department stated that Coast Guard would review its existing cybersecurity incident procedures and determine what additional procedures are necessary to ensure the accuracy of tracked cybersecurity incident information, as appropriate.

With respect to our second recommendation that the Commandant of the Coast Guard ensure that its case management system for facility and vessel security inspections provides ready access to complete data on specific cybersecurity deficiencies identified during those inspections, DHS concurred. The Department stated the Coast Guard's Office of Port and Facility Compliance will lead the service's efforts to update the MISLE database to ensure the system provides ready access to complete data on specific cybersecurity deficiencies identified during inspections. According to DHS, these efforts related to cybersecurity deficiency data include coordinating system enhancements with other stakeholders, as appropriate, to update MISLE data entry guidelines for vessel and facility inspections.

DHS also concurred with our third recommendation that the Commandant of the Coast Guard 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. The department noted that once the Maritime Transportation Sector-Risk Assessment and Management Plan is published (estimated completion date of July 2025), the Coast Guard's Office of Cyberspace Forces will follow this plan in the service's next iteration of the Coast Guard Cyber Strategic Outlook.

With respect to our fourth recommendation that the Commandant of the Coast Guard develop future competency needs for all its personnel with MTS cyber responsibilities for mitigating cyber risks to the MTS and analyze the gaps between current competencies and future needs, DHS concurred. The Department noted that the Coast Guard's Office of Port and Facility Compliance will establish a cross-program team to determine future competency needs for all personnel with MTS cyber responsibilities, analyze gaps between current competencies and future needs, and make recommendations on needed competencies, as appropriate.

DHS also concurred with our fifth recommendation that the Commandant of the Coast Guard, 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. DHS noted that the Coast Guard’s Office of Cyberspace Forces recognizes that any future or currently-needed competencies may require additional training and education. According to DHS, once the service makes recommendations regarding needed competencies in personnel with cyber responsibilities for mitigating cyber risks to the MTS, the Office of Cyberspace Forces will ensure these recommendations are reviewed by appropriate program offices and that they develop actions to address gaps, as needed.

We will continue to monitor the Coast Guard’s actions and the extent to which they address these recommendations.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Transportation, and the Secretary of Homeland Security. In addition, this report is available at no charge on the GAO website: https://www.gao.gov.

If you or your staff have any questions about this report, please contact Tina Won Sherman at (202) 512-8777, ShermanT@gao.gov; or Marisol Cruz Cain, (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VII.

Tina Won Sherman
Director, Homeland Security and Justice

Marisol Cruz Cain

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for us to conduct a study on cybersecurity threats to the Maritime Transportation System (MTS).[1] This report addresses (1) the cybersecurity threats and associated risks facing the MTS, and the extent to which Coast Guard has established procedures for maintaining incident information, (2) the extent to which the Coast Guard has taken action to assist and oversee MTS owners and operators in mitigating cybersecurity risks; (3) the extent to which the Coast Guard has conducted strategic planning to mitigate cybersecurity risks to the MTS, and (4) the extent to which Coast Guard has implemented leading practices for cyber workforce competency assessments, including addressing our prior cyber workforce staffing recommendations.

For all our objectives, we interviewed Coast Guard headquarters officials within the offices of Cyber Command, Port and Facility Compliance, Commercial Vessel Compliance, Waterways and Ocean Policy, and Human Resources. In addition, we selected a non-generalizable sample of four ports based on factors including volume of trade measured in tonnage, reported cybersecurity incidents, presence of ship-to-shore cranes, and geographic dispersion. We conducted in-person site visits with the New York and Houston/Galveston sectors, and virtual site visits with the Los Angeles/Long Beach and Ohio Valley sectors. At these site visits, we interviewed Coast Guard sector officials responsible for the selected ports to gather information and local perspectives on cybersecurity threats, oversight of MTS owner and operator compliance with cybersecurity statutory requirements and relevant regulations, cyber-

[1] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. K, tit. CXII, subtit. D, § 11230, 136 Stat. 2395, 4029 (2022).

related information sharing, and cyber workforce competencies, among other issues.[2]

During our in-person site visits, we observed facility security inspections in the Coast Guard New York sector and the Houston/Galveston sector. We also interviewed members of the Area Maritime Security Committee to better understand the unique perspectives of public and private MTS owners and operators. We discussed issues, such as coordinating with the Coast Guard to mitigate cybersecurity threats and associated risks facing the MTS, Coast Guard guidance, oversight, and information sharing efforts. The information that we gathered cannot be generalized to all ports and sectors across the United States. However, it can provide insight into cybersecurity threats, information sharing, cyber risk mitigation efforts, oversight, and workforce structure.

[2] We selected 3 large ports each with a high volume of trade, reported cybersecurity incidents, presence of ship-to-shore cranes, and geographic dispersion along various U.S. coasts: Port Houston, TX; the Port of New York, NY and New Jersey, NJ; and the Port of Long Beach. We selected one small port (Paducah, KY Marine Safety Unit within the Ohio Valley sector) with lower trade volume, no reported cyber incidents, no ship-to-shore cranes, and located inland; to better understand any unique factors or challenges a smaller port may face when mitigating cybersecurity risk to the MTS. A ship-to-shore crane, also known as a container crane, is a type of large dockside gantry crane found at container terminals for loading and unloading intermodal containers from container ships. Based on concerns that ship-to-shore cranes manufactured by companies in the People's Republic of China may be controlled, serviced, programmed from remote locations, and thus vulnerable to exploitation, in 2024 Coast Guard issued a Maritime Security Directive related to ship-to-shore cranes and cyber risks: U.S. Coast Guard, *MARSEC Directive 105-4: Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies,* (February 21, 2024). For each sector, we gathered information and local perspectives from the Captain of the Port, inspection staff, the Maritime Transportation System Specialist-Cyber (cyberspecialist), and Area Maritime Security Committee members. As local commander, a Coast Guard Captain of the Port oversees important aspects of security in the MTS and is responsible for local operations within each district. Each of the Coast Guard area commands, districts, and sectors is responsible for managing its assets and accomplishing missions within its geographic area of responsibility. The Coast Guard inspection staff conduct scheduled security inspections to assess MTS compliance with federal statutes and regulatory requirements. At the time of our review, some cybersecurity-related requirements existed in relevant statutes and regulations. See 46 U.S.C. § 70103(c)(3)(C)(v); 33 C.F.R. §§ 104.305(d)(vii)(2)(v), 105.305(c)(1)(v), 106.305(c)(1)(v). However, a final rule promulgating minimum cybersecurity requirements for maritime owners and operators was not issued until January 2025 and will not begin to take effect until July 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6298 (Jan. 17, 2025). Cyberspecialists advise Coast Guard commanders (e.g., Captain of the Port) and MTS owners and operators on cyber-related subject matter. The Coast Guard works through Area Maritime Security Committees to, among other things, identify critical maritime infrastructure and risks and communicate appropriate security information to maritime stakeholders.

For our first objective, we first developed a list of cyber threat actors that could pose a threat to the MTS, potential vulnerabilities in the infrastructure, cyber incidents that have been reported domestically, and reviewed the potential impacts of cyberattacks on MTS infrastructure. To develop the list of cyber threat actors, we reviewed our prior work on cyber-based threats facing other sectors,[3] as well as the threats identified by the 2024 *Annual Threat Assessment of the U.S. Intelligence Community*, Homeland Threat Assessment 2024, and *2023 Cyber Trends and Insights in the Marine Environment*.[4] Further, in addition to the Coast Guard and private sector representatives previously discussed, we interviewed officials from federal agencies and obtained the perspectives of select nonfederal stakeholders to confirm the accuracy of our cyber threat actor list.

- **Federal agencies**. We interviewed officials from four federal agencies (other than the Coast Guard) that we selected because of their responsibilities related to oversight of the MTS or critical infrastructure protection: Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), Department of the Interior's Bureau of Safety and Environmental Enforcement, Department of Justice's Federal Bureau of Investigation, and Department of Transportation's Maritime Administration.
- **Nonfederal stakeholders.** We contacted 13 nonfederal organizations that are members of, or represent a segment of, the MTS industry, or have been recognized by CISA as having expertise in OT.[5] We selected the 10 OT vendors who joined CISA's Joint Cyber Defense Collaborative in April 2022 when CISA expanded this group to focus on OT cyber issues. We also selected three other organizations that

[3] GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, GAO-23-105789 (Washington, D.C.: Oct. 26, 2022). *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, GAO-22-104256 (Washington, D.C.: June 21, 2022); *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021); *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024); Department of Homeland Security, *Office of Intelligence and Analysis, Homeland Threat Assessment 2024;* U.S. Coast Guard, Coast Guard Cyber Command, *2023 Cyber Trends and Insights in the Marine Environment*.

[5] Operational technology refers to programmable systems and devices that interact with the physical environment. As discussed in more detail later in this report, this technology is used by the MTS.

represent a segment of the MTS industry by reviewing our prior work on the issues and soliciting recommendations on organizations to interview from industry stakeholders. Of the 13 selected organizations, four—Bechtel, Dragos, Gary Kessler Associates, and the MTS Information Sharing and Analysis Center—provided responses to our questions by way of written responses or interviews.[6]

To identify cybersecurity vulnerabilities to MTS infrastructure, we reviewed reports developed by key federal and industry stakeholders, as well as our previous work on cybersecurity risks to critical infrastructure.[7] We also interviewed federal agencies and obtained the perspectives of nonfederal stakeholders to identify potential cybersecurity vulnerabilities and any related reports or assessments and to identify any reported incidents and potential impacts on MTS infrastructure. To assess the reliability of Coast Guard's data on cybersecurity incidents impacting the MTS from July 2019 through May 2024, we compared the data to the definition that the Coast Guard uses for a cybersecurity incident.[8] Control activities that respond to risks were significant to this objective, along with the related principle that management should implement control activities to include procedures that address related risks. Therefore, we assessed the extent to which Coast Guard established procedures for maintaining the incident data, consistent with *Standards for Internal Control in the Federal Government*.[9] We determined that Coast Guard's data were not sufficiently reliable for our purposes of describing the number of reported cybersecurity incidents impacting the MTS. For example, we found that the Coast Guard reported conflicting information about whether certain incidents impacted the MTS, as discussed in this report.

[6] The other nine—the Maritime Sector Coordinating Council and eight private sector companies—did not respond to interview requests.

[7] GAO-23-105789; GAO-22-104256; GAO-21-81; and GAO-19-332.

[8] Relevant regulations define a "cyber incident" as an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 33 C.F.R. § 6.01-8 (incorporating by reference the definition of "incident" in 44 U.S.C. § 3552(b)(2)); 101.615 (effective July 16, 2025, per Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025)).

[9] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

For our second objective, we reviewed Coast Guard guidance provided to MTS owners and operators on required and recommended cybersecurity practices. In addition, we reviewed relevant statutes and regulations, including the minimum cybersecurity regulatory requirements promulgated in January 2025. However, these minimum cybersecurity requirements do not begin to take effect until July 2025.[10] We also reviewed the Coast Guard's cyber threat information sharing methods, and we analyzed information on voluntary advisory services and direct technical assistance provided by the service to MTS owners and operators to help mitigate cybersecurity risks. We compared these advisory and technical assistance activities against cybersecurity-related requirements in federal regulations and various Coast Guard guidance documents related to cybersecurity in the MTS. We also compared documentation to our prior work on methods used by agencies to share cyber threat information with critical infrastructure owners and operators.

Additionally, we interviewed Coast Guard headquarters and sector officials within the offices and locations discussed above to confirm our understanding of applicable federal statutes and cybersecurity-related requirements, guidance provided to MTS owners and operators, the Coast Guard's efforts to share cyber threat information, and the service's facility and vessel security inspection processes.[11]

We also reviewed Coast Guard policy, procedures, and guidance provided to its staff responsible for overseeing MTS owner and operator compliance with relevant regulations, through the facility and vessel security inspection process. We observed how the Coast Guard records the results of its security inspections in its Marine Information for Safety and Law Enforcement (MISLE) case management system. We reviewed facility inspections data for cybersecurity-related deficiencies that occurred in fiscal year 2019 through June 2024. The Coast Guard

[10] See Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6,298 (Jan. 17, 2025).

[11] To address information sharing, we reviewed documentation on cyber threat information sharing methods. We reviewed documentation from and interviewed officials from the five previously mentioned federal agencies that are responsible for sharing cyber threat information with critical infrastructure owners and operators in the MTS. Specifically, we reviewed documentation and interviewed officials from the selected federal agencies regarding the methods they use to share cyber threat information (e.g., descriptions of the methods, types of information shared). We then aligned each method to one of 11 existing categories we identified in our prior work. GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, GAO-23-105468 (Washington, D.C.: Sept. 26, 2023).

provided this data based on its method for extracting cybersecurity-related information from MISLE using a key word search.[12] To obtain vessel inspection deficiency data for inspections that occurred during the same time-period, we reviewed publicly available data from the Coast Guard's web site. To identify vessel inspection cybersecurity-related deficiency data specifically, we selected data categories and reviewed each case deficiency description field in full to determine which data records were related to cybersecurity based on the content of the Coast Guard's description of each deficiency. We determined that a record was related to cybersecurity if the narrative description of the deficiency described gaps that would impact the cybersecurity of technology used on a vessel, such as protecting networks, devices, or data from unauthorized access or criminal use.

We selected Coast Guard MISLE data for fiscal year 2019, which was the first complete fiscal year following the inclusion of maritime cybersecurity requirements in the 2018 amendment to the Maritime Transportation Act of 2002 (MTSA).[13] To assess the reliability of the data, we reviewed available system documentation and interviewed agency officials responsible for managing the security inspection data. We determined that both facility and vessel data were sufficiently reliable for purposes of describing how the Coast Guard enters deficiency data into MISLE but not sufficiently complete for reporting the total number of cybersecurity-related inspection deficiencies that the Coast Guard has issued to MTS owners and operators, as discussed in this report.

For our third objective, we analyzed the service's efforts to develop approaches for implementing a cybersecurity strategy for the MTS

[12] Coast Guard queried its facility inspection deficiency data by searching a free-form text field (the case deficiency description field) using the key words "cyber", "computer", and "networks" to retrieve data records that contained at least one of these terms.

[13] See Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064. The Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, div. J, § 1805, 132 Stat. 3186, 3535 (amending MTSA). The 2018 amendment to the Maritime Transportation Security Act required, among other things, Maritime Transportation System owners and operators to assess, document, and address certain cybersecurity risks (in addition to vulnerabilities in their computer systems and networks). See id. at § 1805(d)(2)(D) (codified at 46 U.S.C. § 70103(c)(3)(C)(v)). In January 2025, Coast Guard promulgated new regulations implementing this requirement, which will go into effect on July 16, 2025. Cybersecurity in the Marine Transportation System, 90 Fed. Reg. 6298 (Jan. 17, 2025). Some new requirements go into effect on that date, while the rule allows regulated owners and operators 6 or 24 months from the time of publication to implement other requirements. Accordingly, the MISLE data for fiscal year 2019 which we reviewed does not reflect these implementing regulations.

subsector. Specifically, we compared the Coast Guard's MTS cybersecurity strategy and plans against leading practices we identified in prior work on key characteristics for a national strategy.[14]

For the fourth objective, we reviewed supporting documentation related to the service's competency efforts such as position descriptions, workforce analyses, and training efforts. We then compared these efforts against leading practices we identified in our prior work highlighting the importance of ensuring that staff are assigned the performance competencies to effectively carry out their duties.[15] We also interviewed Coast Guard officials on their efforts to develop competencies, assess competency gaps, and address identified gaps for the service's cyber workforce. To address the Coast Guard's efforts to address personnel vacancy challenges, we interviewed the service's officials on their initial actions to address vacancy challenges and current vacancy rates. Finally, we reviewed the Coast Guard's efforts to address recommendations from prior work on the service's efforts to improve the skills and vacancies of its cyber workforce.[16]

We conducted this performance audit from December 2023 to December 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[14] GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[15] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

[16] GAO, *Coast Guard: Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands*, GAO-22-105208 (Washington, D.C.: Sept. 27, 2022).

Appendix II: Applicability of Select Maritime Transportation Security Act Regulations

Table 9: Applicability of Certain Maritime Transportation Security Act Regulations by Facility and Vessel Type

Type	Citation	Regulation
Facility	33 C.F.R. parts 105-106 (containing security requirements, including security assessments and security plans to be reviewed by U.S. Coast Guard).	Subject to exceptions, 33 C.F.R. part 105 applies to the owner or operator of any U.S.: • Facility subject to 33 C.F.R. parts 126 (waterfront facilities handling packaged and bulk-solid dangerous cargo and to vessels at those facilities), 127 (waterfront facilities handling liquefied natural gas and liquefied hazardous gas), or 154 (certain facilities transferring oil or hazardous material in bulk). • Facility that receives vessels certificated to carry more than 150 passengers, except those vessels not carrying and not embarking or disembarking passengers at the facility. • Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, chapter XI. • Facility that receives foreign cargo vessels greater than 100 gross register tons. • Facility that receives U.S. cargo vessels, greater than 100 gross register tons, subject to 46 C.F.R. chapter I, subchapter I, except for those facilities that receive only commercial fishing vessels inspected under 46 C.F.R. part 105. • Barge fleeting facility that receives barges carrying, in bulk, cargoes regulated by 46 C.F.R. chapter I, subchapters D or O, or Certain Dangerous Cargoes. 33 C.F.R. part 106 applies to the owner or operator of any fixed or floating facility, including Mobile Offshore Drilling Units not subject to part 104 of this subchapter, operating on the Outer Continental Shelf of the United States for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N, that meet the following operating conditions: • Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more; • Produces greater than 100,000 barrels of oil per day; or • Produces greater than 200 million cubic feet of natural gas per day.

Type	Citation	Regulation
Vessel	33 C.F.R. part 104 (containing security requirements, including security assessments and security plans to be reviewed by U.S. Coast Guard).	Subject to exceptions, 33 C.F.R. part 104 applies to the owner or operator of any • Mobile Offshore Drilling Unit, cargo, or passenger vessel subject to the International Convention for Safety of Life at Sea, 1974, Chapter XI–1 or Chapter XI–2. • Foreign cargo vessel greater than 100 gross register tons. • Self-propelled U.S. cargo vessel greater than 100 gross register tons subject to 46 C.F.R. subchapter I, except commercial fishing vessels inspected under 46 C.F.R. part 105. • Vessel subject to 46 C.F.R. chapter I, subchapter L. • Passenger vessel subject to 46 C.F.R. chapter I, subchapter H. • Passenger vessel certificated to carry more than 150 passengers. • Other passenger vessel carrying more than 12 passengers, including at least one passenger-for-hire, that is engaged on an international voyage. • Barge subject to 46 C.F.R. chapter I, subchapters D or O. • Barge carrying certain dangerous cargo in bulk or barge that is subject to 46 C.F.R. chapter I, subchapter I, that is engaged on an international voyage. • Tankship subject to 46 C.F.R. chapter I, subchapters D or O. • Towing vessel greater than eight meters in registered length that is engaged in towing a barge or barges subject to this part, except a towing vessel that—(i) Temporarily assists another vessel engaged in towing a barge or barges subject to this part; (ii) Shifts a barge or barges subject to this part at a facility or within a fleeting facility; (iii) Assists sections of a tow through a lock; or (iv) Provides emergency assistance.

Source: GAO analysis of U.S. Code of Federal Regulations. | GAO-25-107244

Appendix III: Cyberattack Tactics and Techniques Associated with Enterprise IT and Operational Technology Systems

Attackers may use various tactics, such as gaining an initial foothold on target systems, running malicious code, and moving through various systems, to exploit vulnerabilities and position themselves to achieve their ultimate goals (see table 10).

Table 10: Summary of Cyberattack Tactics and Techniques Associated with Enterprise IT and Operational Technology Systems

Technology	Summary of cyberattack tactics and techniques[a]
Enterprise IT systems	Attackers often begin cyberattacks on enterprise systems by • performing reconnaissance, such as scanning for vulnerabilities in target hosts or applications; then, • establishing resources that can be used to support their operations, such as developing malicious software. • Subsequently, attackers will seek to gain initial access to a target network by • using spear phishing emails (i.e., emails sent in a targeted attempt to trick a specific person into revealing confidential information) or • exploiting weaknesses on public-facing web servers. After gaining an initial foothold, attackers will often use a variety of tactics and techniques to achieve their objectives, such as • running malicious code, • stealing account names and passwords to gain higher-level permissions, and • moving throughout a network to find and gain access to their target. Attackers may achieve a level of access to allow further actions on objectives within the enterprise system, such as • collecting, exfiltrating, or destroying data from targeted information systems; • establishing and maintaining persistent and undetected command and control access for future operations; and • reducing the productivity and revenue of the targeted entity by denying availability to IT systems and the data on those systems, compromising the confidentiality or integrity of data, or committing financial theft.

Technology	Summary of cyberattack tactics and techniques[a]
Operational technology (OT) systems	Attackers can gain initial access to OT systems by • exploiting internet-accessible system devices; • compromising the supply chain of the system by manipulating products (such as hardware or software) or delivery mechanisms before receipt by the end consumer;[b] or • gaining access to enterprise IT systems, then leveraging this access to target OT systems. After gaining initial access to OT systems, attackers may use other tactics to position themselves to achieve their goals, such as • running malicious code, • avoiding detection, and • moving throughout the industrial control systems environment. Attackers will then attempt to manipulate or interrupt operations of OT systems to achieve their goals, including by • damaging or destroying infrastructure, equipment, and the surrounding environment; • preventing operators from controlling industrial operations, even after the malicious interference has subsided; and • reducing productivity and revenue by disrupting or damaging the availability and integrity of control system operations, devices, and related processes.

Source: Prior GAO reports and GAO analysis of MITRE ATT&CK® Matrix for Enterprise and Matrix for Industrial Control Systems. | GAO-25-107244

[a] MITRE ATT&CK® Matrix for Enterprise, MITRE Corporation accessed on April 25, 2022, https://attack.mitre.org/matrices/enterprise/ and MITRE ATT&CK® Matrix for Industrial Control Systems, MITRE Corporation, accessed on April 25, 2022, https://attack.mitre.org/matrices/ics/. The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. MITRE has done extensive research for the federal government on cybersecurity issues.

[b] The supply chain is a linked set of resources and processes that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

Appendix IV: Coast Guard Guidance for Cybersecurity for Facility Owners and Operators

As shown below in table 11, the Coast Guard's *Maritime Cybersecurity Assessment and Annex Guide* recommends that facility owners and operators identify a cybersecurity officer, define cybersecurity vulnerabilities and protections based on the National Institute of Standards and Technology Cybersecurity Framework, and identify all necessary cybersecurity vulnerabilities to safeguard physical assets.[1] The annex guide also states that a cybersecurity officer should have a thorough understanding of the systems that affect facility security, the networks those systems are connected to, the threats that affect those systems and networks, and the cyber protections available to the facility. Overall, the annex guide states that credible protection for relevant cybersecurity vulnerabilities can only be achieved if the facility's network meets or exceeds a minimum level of cyber hygiene.[2]

Table 11: Coast Guard's Maritime Cybersecurity Assessment and Annex Guide on Functions, Categories, and Subcategories

Function	Category	Example of subcategory
Identify	Asset Management: Data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried
	Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, in normal operations).
	Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
	Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Asset vulnerabilities are identified and documented.
	Risk Management: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by organizational stakeholders.
	Supply Chain Risk Management: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

[1] U.S. Coast Guard, *Maritime Cybersecurity Assessment and Annex Guide* (January 2023).

[2] Cyber hygiene is a set of routine practices for using basic security capabilities to mitigate cyber risks due to common or pervasive threats.

Function	Category	Example of subcategory
Protect	Identify Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
	Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	All users are informed and trained.
	Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Protections against data leaks are implemented.
	Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
	Maintenance: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and repair of organizational assets are performed and logged with approved and controlled tools.
	Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Removable media is protected, and its use is restricted according to policy.
Detect	Anomalies and Events: Anomalous activity is detected, and the potential impact of events is understood.	A baseline of network operations and expected data flows for users and systems is established and managed.
	Security Continuous Monitoring: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The network is monitored to detect potential cybersecurity events.
	Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Roles and responsibilities for detection are well defined to ensure accountability.
Respond	Response Planning: Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	A response plan is executed during or after an incident.
	Communications: Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	Incidents are reported consistent with established criteria.
	Analysis: Analysis is conducted to ensure effective response and support recovery activities.	Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
	Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Newly identified vulnerabilities are mitigated or documented as accepted risks.
	Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans incorporate lessons learned.

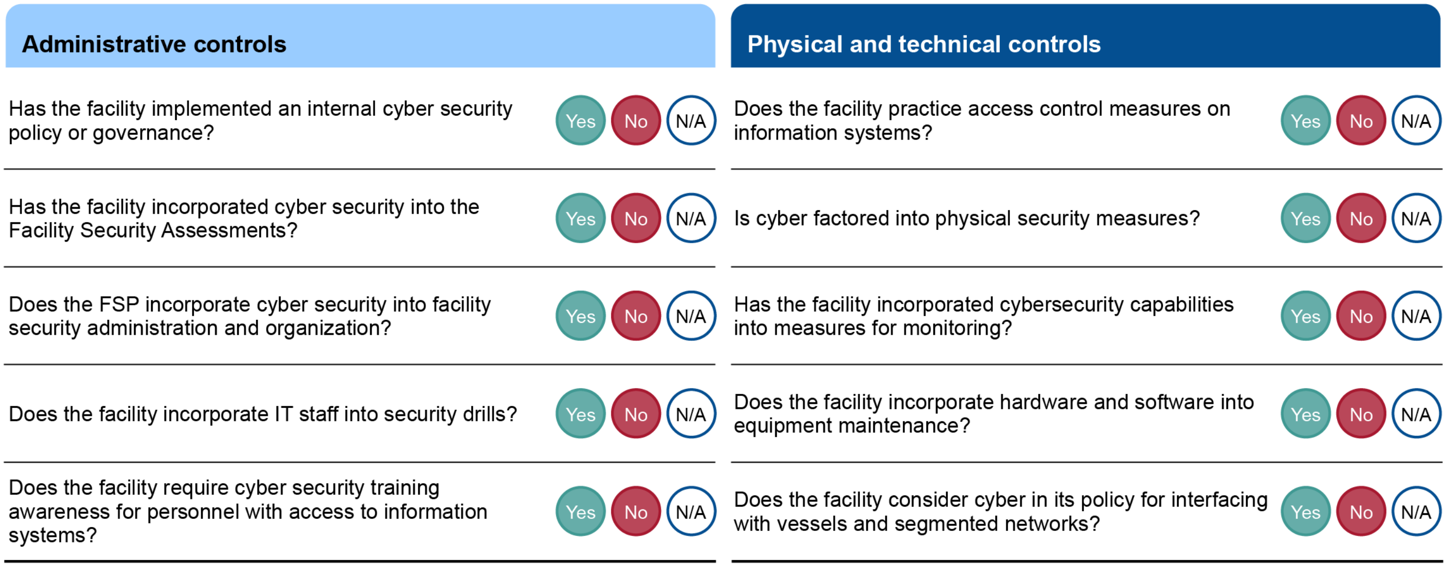
Function	Category	Example of subcategory
Recover	Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	A recovery plan is executed during or after a cybersecurity incident.
	Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned.
	Communications: Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors).	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

Source: Coast Guard. | GAO-25-107244

Appendix V: Coast Guard Job Aid on Recommended Questions for Facility Inspections

The facility inspection job aid involving cybersecurity is available on Coast Guard's web site and recommends that facilities' cybersecurity staff participate in Coast Guard's security inspections, to encourage interaction and to address any cybersecurity-related questions. This includes any physical observations made by inspectors. As shown in figure 4, the facility job aid includes suggested, cybersecurity-related questions for inspectors to ask when inspecting a facility. The job aid states that that it is not to be used as a regulatory compliance tool, but to address general cybersecurity practices.

Figure 4: Coast Guard Job Aid on Recommended Questions for Facility Inspections

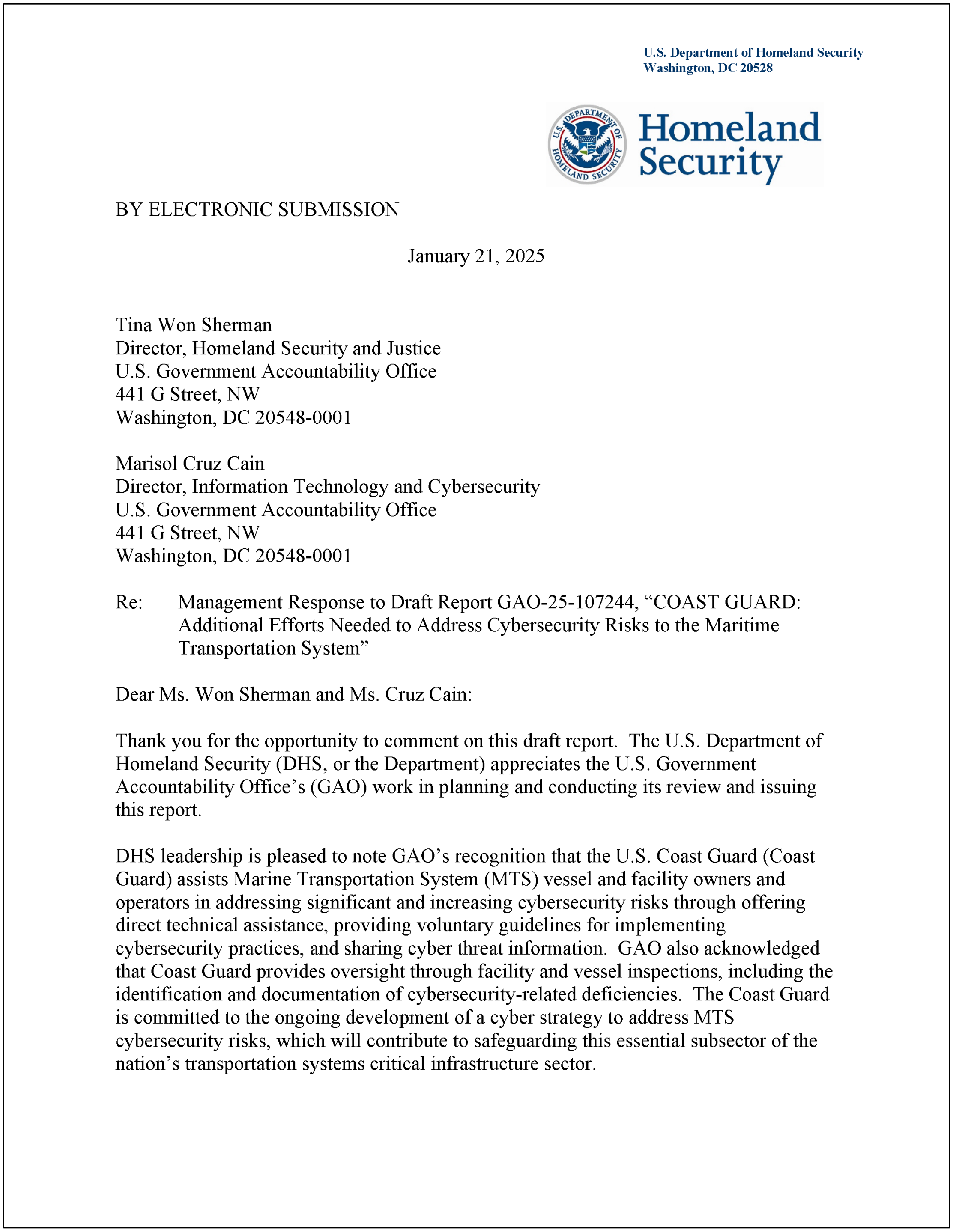


Administrative controls		Physical and technical controls	
Has the facility implemented an internal cyber security policy or governance?	Yes No N/A	Does the facility practice access control measures on information systems?	Yes No N/A
Has the facility incorporated cyber security into the Facility Security Assessments?	Yes No N/A	Is cyber factored into physical security measures?	Yes No N/A
Does the FSP incorporate cyber security into facility security administration and organization?	Yes No N/A	Has the facility incorporated cybersecurity capabilities into measures for monitoring?	Yes No N/A
Does the facility incorporate IT staff into security drills?	Yes No N/A	Does the facility incorporate hardware and software into equipment maintenance?	Yes No N/A
Does the facility require cyber security training awareness for personnel with access to information systems?	Yes No N/A	Does the facility consider cyber in its policy for interfacing with vessels and segmented networks?	Yes No N/A

N/A Not applicable

Source: U.S. Coast Guard. | GAO-25-107244

Appendix VI: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

BY ELECTRONIC SUBMISSION

January 21, 2025

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

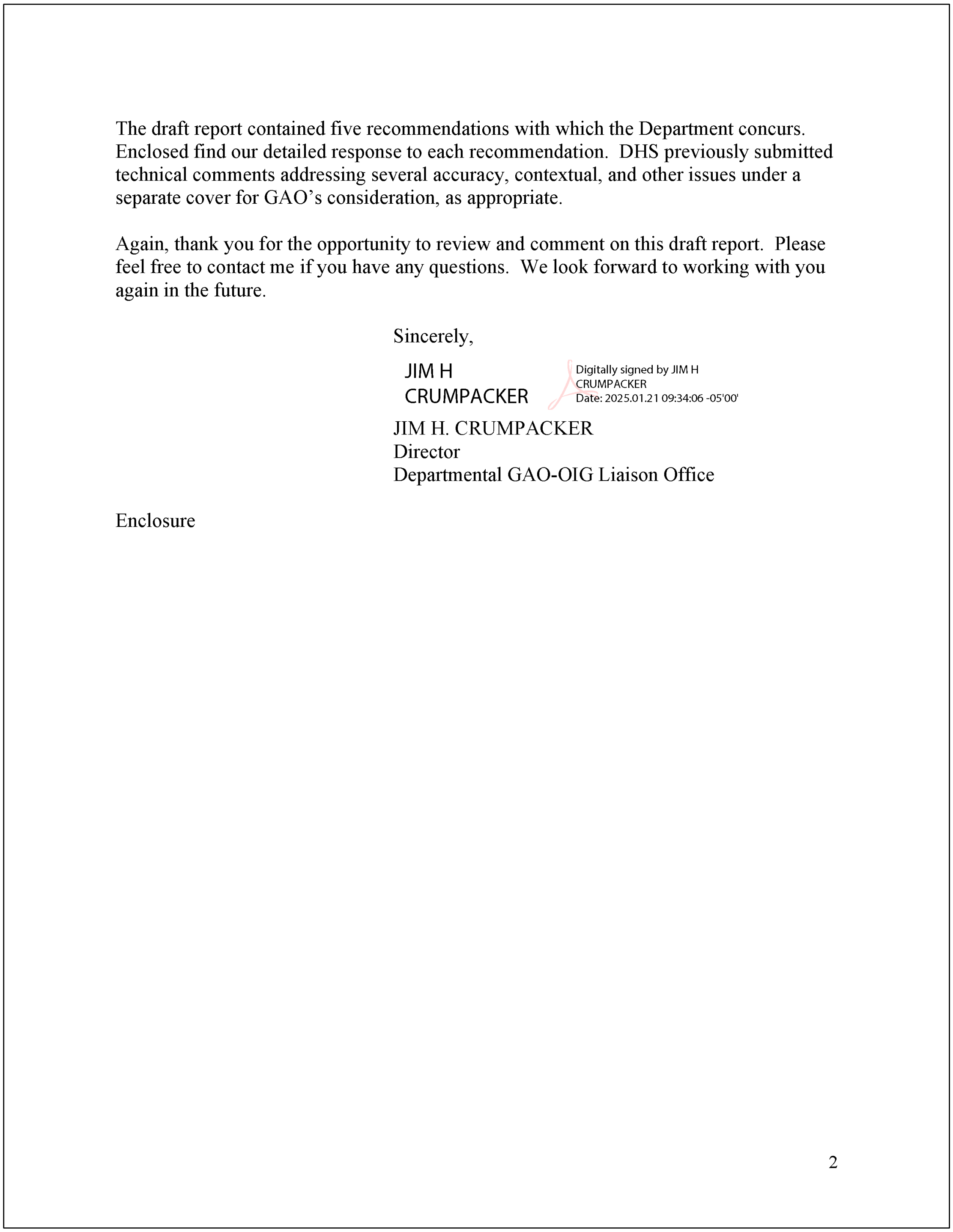
Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-25-107244, "COAST GUARD: Additional Efforts Needed to Address Cybersecurity Risks to the Maritime Transportation System"

Dear Ms. Won Sherman and Ms. Cruz Cain:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition that the U.S. Coast Guard (Coast Guard) assists Marine Transportation System (MTS) vessel and facility owners and operators in addressing significant and increasing cybersecurity risks through offering direct technical assistance, providing voluntary guidelines for implementing cybersecurity practices, and sharing cyber threat information. GAO also acknowledged that Coast Guard provides oversight through facility and vessel inspections, including the identification and documentation of cybersecurity-related deficiencies. The Coast Guard is committed to the ongoing development of a cyber strategy to address MTS cybersecurity risks, which will contribute to safeguarding this essential subsector of the nation's transportation systems critical infrastructure sector.



The draft report contained five recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

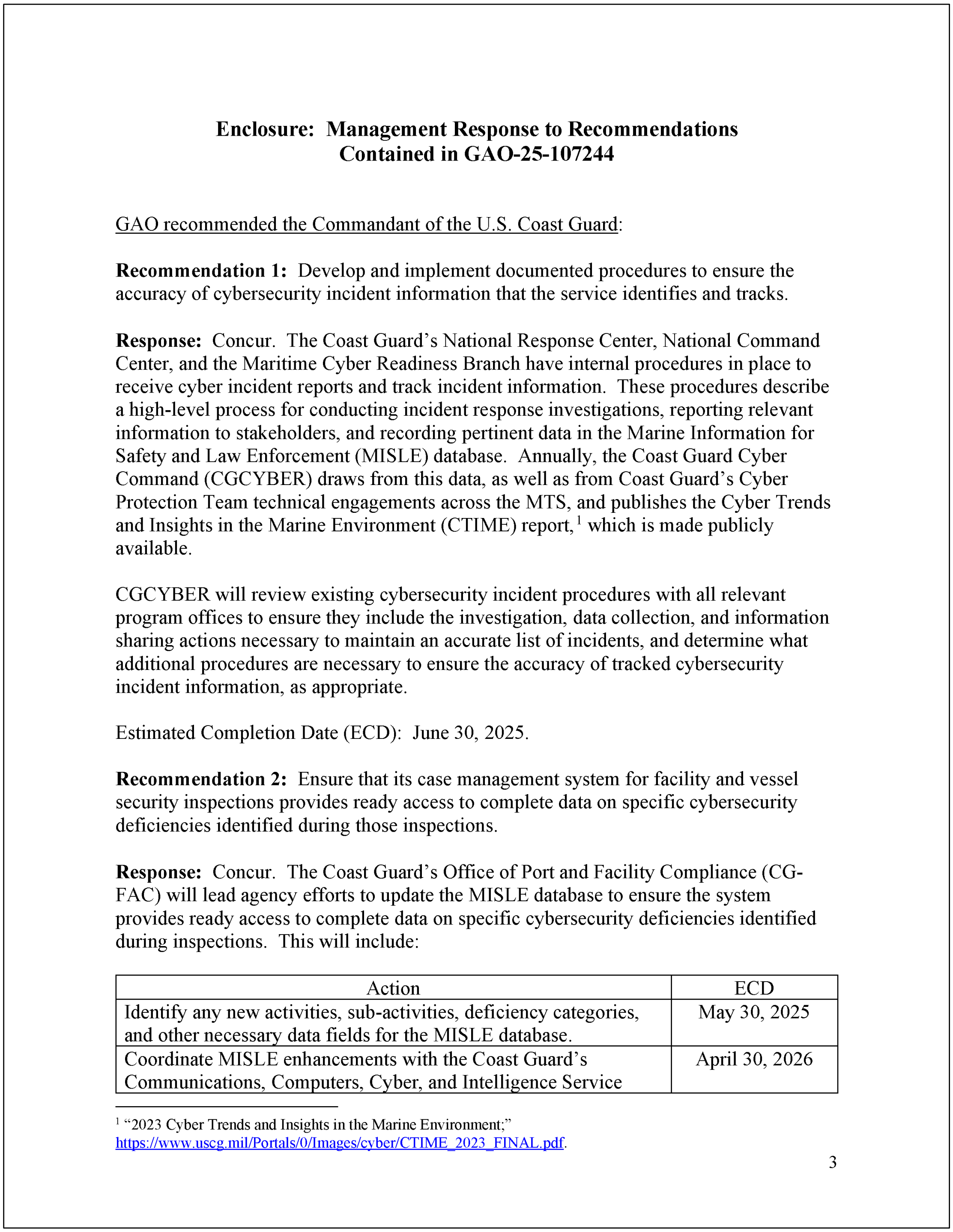
Sincerely,

JIM H
CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2025.01.21 09:34:06 -05'00'

JIM H. CRUMPACKER
Director
Departmental GAO-OIG Liaison Office

Enclosure



Enclosure: Management Response to Recommendations Contained in GAO-25-107244

GAO recommended the Commandant of the U.S. Coast Guard:

Recommendation 1: Develop and implement documented procedures to ensure the accuracy of cybersecurity incident information that the service identifies and tracks.

Response: Concur. The Coast Guard's National Response Center, National Command Center, and the Maritime Cyber Readiness Branch have internal procedures in place to receive cyber incident reports and track incident information. These procedures describe a high-level process for conducting incident response investigations, reporting relevant information to stakeholders, and recording pertinent data in the Marine Information for Safety and Law Enforcement (MISLE) database. Annually, the Coast Guard Cyber Command (CGCYBER) draws from this data, as well as from Coast Guard's Cyber Protection Team technical engagements across the MTS, and publishes the Cyber Trends and Insights in the Marine Environment (CTIME) report,[1] which is made publicly available.

CGCYBER will review existing cybersecurity incident procedures with all relevant program offices to ensure they include the investigation, data collection, and information sharing actions necessary to maintain an accurate list of incidents, and determine what additional procedures are necessary to ensure the accuracy of tracked cybersecurity incident information, as appropriate.

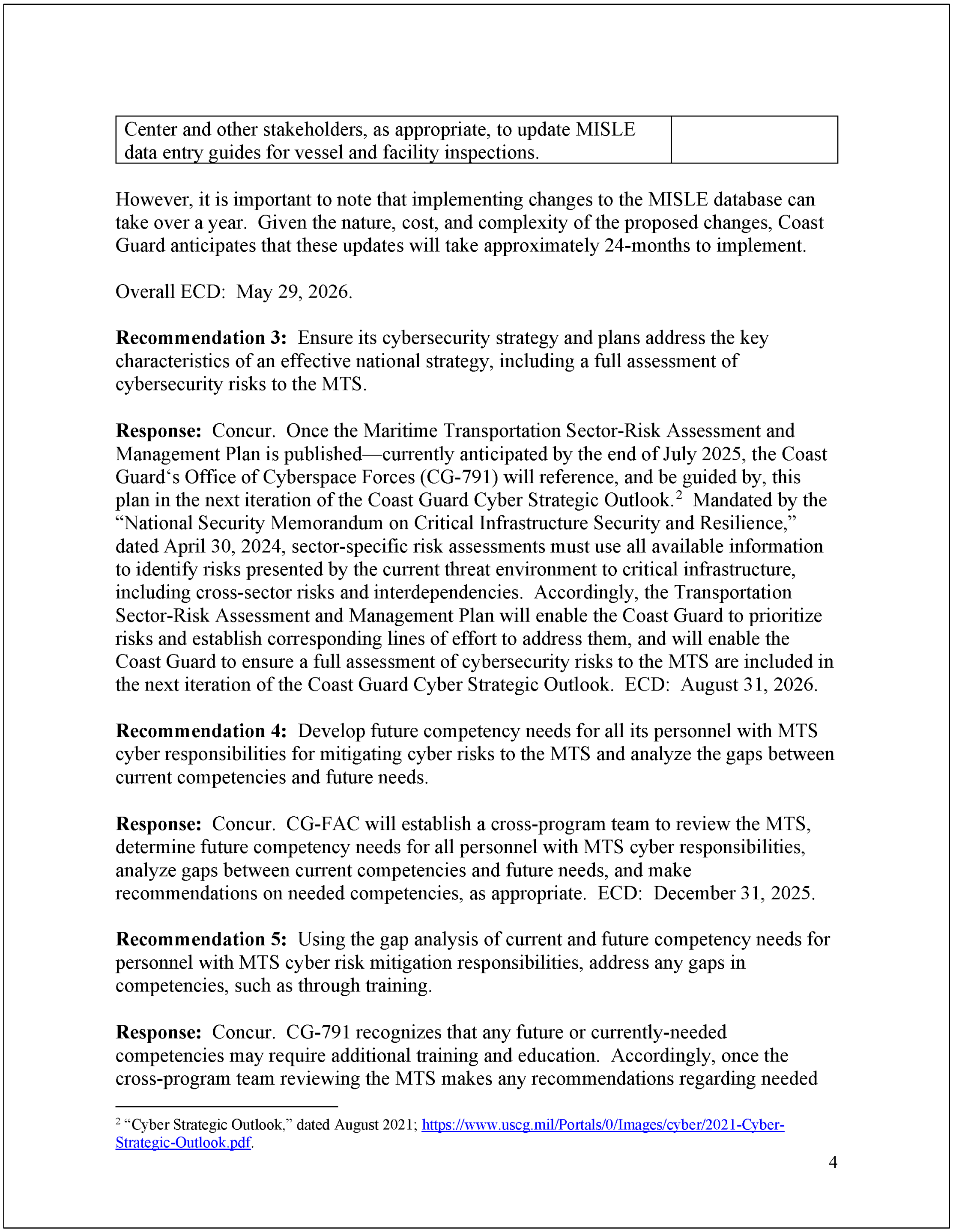
Estimated Completion Date (ECD): June 30, 2025.

Recommendation 2: Ensure that its case management system for facility and vessel security inspections provides ready access to complete data on specific cybersecurity deficiencies identified during those inspections.

Response: Concur. The Coast Guard's Office of Port and Facility Compliance (CG-FAC) will lead agency efforts to update the MISLE database to ensure the system provides ready access to complete data on specific cybersecurity deficiencies identified during inspections. This will include:

Action	ECD
Identify any new activities, sub-activities, deficiency categories, and other necessary data fields for the MISLE database.	May 30, 2025
Coordinate MISLE enhancements with the Coast Guard's Communications, Computers, Cyber, and Intelligence Service	April 30, 2026

[1] "2023 Cyber Trends and Insights in the Marine Environment;" https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf.



Center and other stakeholders, as appropriate, to update MISLE data entry guides for vessel and facility inspections.	

However, it is important to note that implementing changes to the MISLE database can take over a year. Given the nature, cost, and complexity of the proposed changes, Coast Guard anticipates that these updates will take approximately 24-months to implement.

Overall ECD: May 29, 2026.

Recommendation 3: 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.

Response: Concur. Once the Maritime Transportation Sector-Risk Assessment and Management Plan is published—currently anticipated by the end of July 2025, the Coast Guard‘s Office of Cyberspace Forces (CG-791) will reference, and be guided by, this plan in the next iteration of the Coast Guard Cyber Strategic Outlook.[2] Mandated by the "National Security Memorandum on Critical Infrastructure Security and Resilience," dated April 30, 2024, sector-specific risk assessments must use all available information to identify risks presented by the current threat environment to critical infrastructure, including cross-sector risks and interdependencies. Accordingly, the Transportation Sector-Risk Assessment and Management Plan will enable the Coast Guard to prioritize risks and establish corresponding lines of effort to address them, and will enable the Coast Guard to ensure a full assessment of cybersecurity risks to the MTS are included in the next iteration of the Coast Guard Cyber Strategic Outlook. ECD: August 31, 2026.

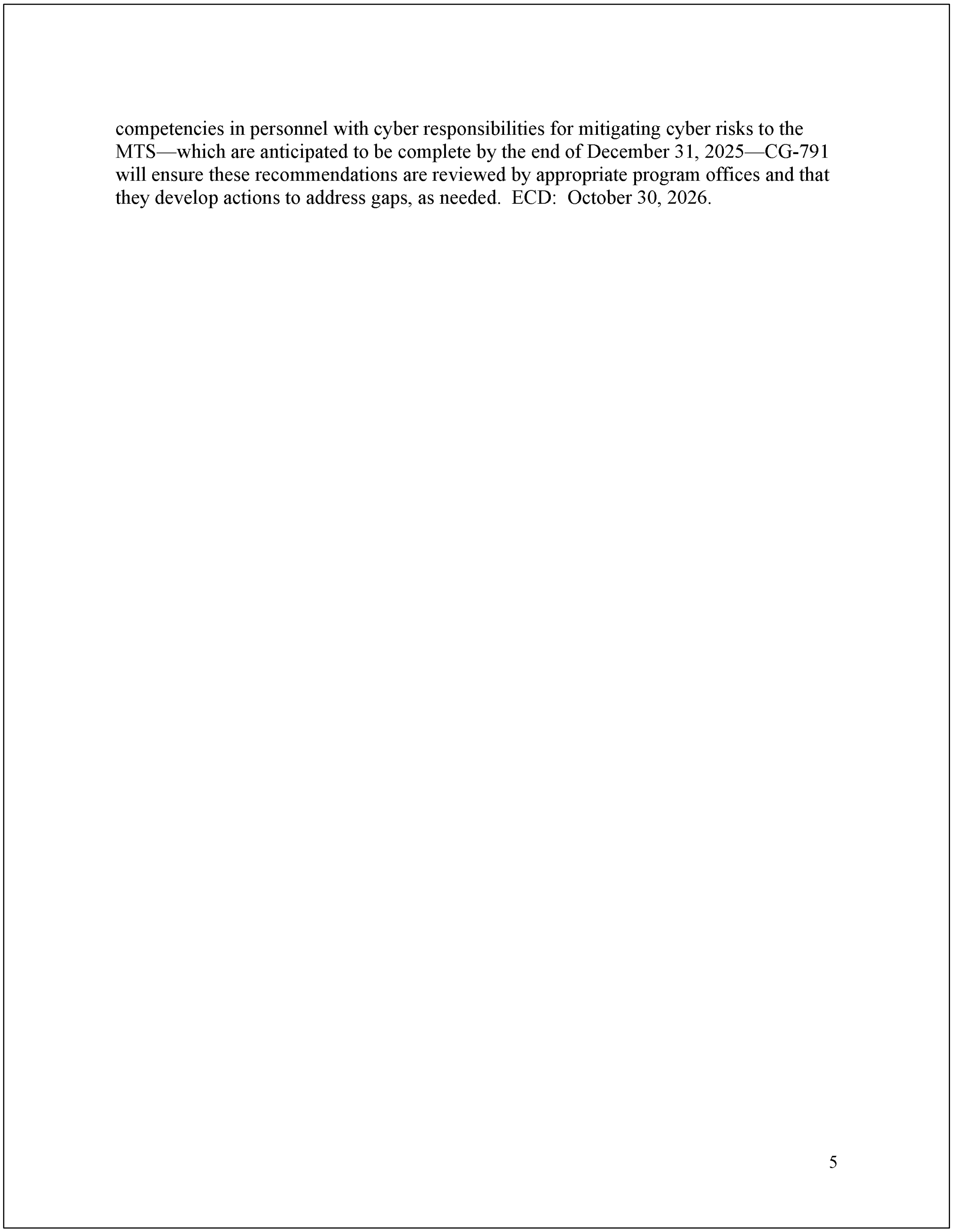
Recommendation 4: Develop future competency needs for all its personnel with MTS cyber responsibilities for mitigating cyber risks to the MTS and analyze the gaps between current competencies and future needs.

Response: Concur. CG-FAC will establish a cross-program team to review the MTS, determine future competency needs for all personnel with MTS cyber responsibilities, analyze gaps between current competencies and future needs, and make recommendations on needed competencies, as appropriate. ECD: December 31, 2025.

Recommendation 5: 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.

Response: Concur. CG-791 recognizes that any future or currently-needed competencies may require additional training and education. Accordingly, once the cross-program team reviewing the MTS makes any recommendations regarding needed

[2] "Cyber Strategic Outlook," dated August 2021; https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.



competencies in personnel with cyber responsibilities for mitigating cyber risks to the MTS—which are anticipated to be complete by the end of December 31, 2025—CG-791 will ensure these recommendations are reviewed by appropriate program offices and that they develop actions to address gaps, as needed. ECD: October 30, 2026.

Appendix VII: GAO Contacts and Staff Acknowledgments

GAO Contact

Tina Won Sherman, (202) 512-8777 or shermant@gao.gov or Marisol Cruz Cain, (202) 512-5017 or cruzcainm@gao.gov.

Staff Acknowledgments

In addition to the contacts above, Chris Ferencik (Assistant Director), Kaelin Kuhn (Assistant Director), Mike Tropauer (Analyst-in-Charge), Amanda Andrade, Lauri Barnes, Eric Hauswirth, Amanda Miller, Mary Offutt-Reagin, Sukhjoot Singh, Filip Stojkovski, and Jason Stonehocker made contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, X, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548