U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-37

July 9, 2024

FINAL REPORT

Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

July 9, 2024

MEMORANDUM FOR: The Honorable Admiral Linda L. Fagan
Commandant
U.S. Coast Guard

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.07.09 16:01:57 -07'00'

SUBJECT: *Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks*

Attached for your action is our final report, *Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving Coast Guard's cyber readiness and precautions to secure the U.S. supply chain. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendations 2 and 3 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Further, based on information provided in your response to the draft report, we consider recommendations 1 and 4 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks

July 9, 2024

Why We Did This Audit

Coast Guard plays a lead role in securing and safeguarding the MTS, which facilitates the transport of nearly $5.4 trillion in commerce — representing about 25 percent of the U.S. gross domestic product. Our objective was to determine the extent to which Coast Guard has implemented cybersecurity readiness and precautions at U.S. ports and on U.S. waterways to protect the U.S. supply chain.

What We Recommend

We made four recommendations to improve Coast Guard's cyber readiness and precautions to secure the U.S. supply chain.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The United States Coast Guard (Coast Guard) took steps to enhance the cyber posture of the Marine Transportation System (MTS) but faces challenges fully implementing cybersecurity readiness efforts to protect the U.S. supply chain. Over the past 2 years, in accordance with its statutory requirements, Coast Guard established maritime cybersecurity teams to deter and respond to transportation cybersecurity incidents. In 2021, Coast Guard implemented Cyber Protection Teams to offer services that can help industry stakeholders prevent and target malicious cyberspace activities. However, private industry stakeholders have not fully adopted these services; stakeholders in only 36 percent of Coast Guard's sectors requested and received these services. Coast Guard faced these challenges because industry stakeholders are hesitant to use the cybersecurity services offered.

Coast Guard also conducts facility and vessel inspections, but these did not always address the full scope of potential cybersecurity threats. This occurred because Coast Guard does not have the authority or training to enforce private industry compliance with standard cybersecurity practices.

In addition, Coast Guard is not adequately staffed to provide cyber expertise for facility and vessel inspections or industry stakeholders due to the job series classification for a key cybersecurity position, which leads to hiring delays.

Overcoming these challenges will better enable Coast Guard to protect the MTS, which remains vulnerable to the exploitation, misuse, or failure of cyber systems. This continued cyber vulnerability may lead to injury or death, harm the marine environment, or disrupt vital trade activity.

DHS Response

The Department of Homeland Security concurred with all four recommendations.

Table of Contents

Abbreviations

C.F.R.	Code of Federal Regulations
CG Cyber Command	Coast Guard Cyber Command
CISA	Cybersecurity and Infrastructure Security Agency
CPT	Cyber Protection Team
MCRB	Maritime Cyber Readiness Branch
MTS	Marine Transportation System
MTSA	*Maritime Transportation Security Act of 2002*
MTSS-C	Marine Transportation Security Specialist–Cyber
OPM	U.S. Office of Personnel Management
VSA	Vessel Security Assessment

Background

The Marine Transportation System (MTS) is the backbone of the U.S. economy, as about 90 percent of U.S. imports and exports travel by ship. The waterways and ports that make up the MTS include 25,000 miles of coastal and inland waterways with 361 ports, 124 shipyards, and more than 3,500 maritime facilities. These critical assets connect U.S. highways, railways, airports, and pipelines to facilitate nearly $5.4 trillion in commerce — representing about 25 percent of the U.S. gross domestic product.

The MTS is a prime target for malicious actors who seek to disrupt our supply chain. The use of new technologies, such as those for navigation, communication, and security, benefit the supply chain. However, these technologies are increasingly vulnerable to exploitation, misuse, or simple failure, which could cause injury or death, harm the marine environment, or disrupt vital trade activity. For example, according to the United States Coast Guard (Coast Guard), vessels rely almost exclusively on networked Global Positioning System–based systems for navigation, while facilities often use the same technologies for cargo tracking and control.

Threats to maritime infrastructure and the supply chain continue to increase. For example, as of August 2021, Coast Guard estimated that hackers attacked the MTS every 39 seconds, for an average of 2,244 cyberattacks per day.[1] As discussed below, Congress and Coast Guard have taken steps to address these ever-increasing threats.

Coast Guard Responsibilities for Cybersecurity Protections for the Marine Transportation System

Coast Guard's mission is to ensure our Nation's maritime safety, security, and stewardship. In 2002, Congress implemented the *Maritime Transportation Security Act of 2002*[2] (MTSA) to protect the U.S. maritime industry, commerce, and the MTS. MTSA aims to prevent transportation security incidents that lead to loss of life, environmental damage, transportation system disruptions, and economic disruption. MTSA required Coast Guard to establish maritime security teams to further deter and respond to transportation security incidents. Then, in 2013, Coast Guard established its own Cyber Command (CG Cyber Command). Establishing CG Cyber Command also brought the component in line with other military organizations as a part of U.S. Cyber Command run by the U.S. Department of Defense.[3]

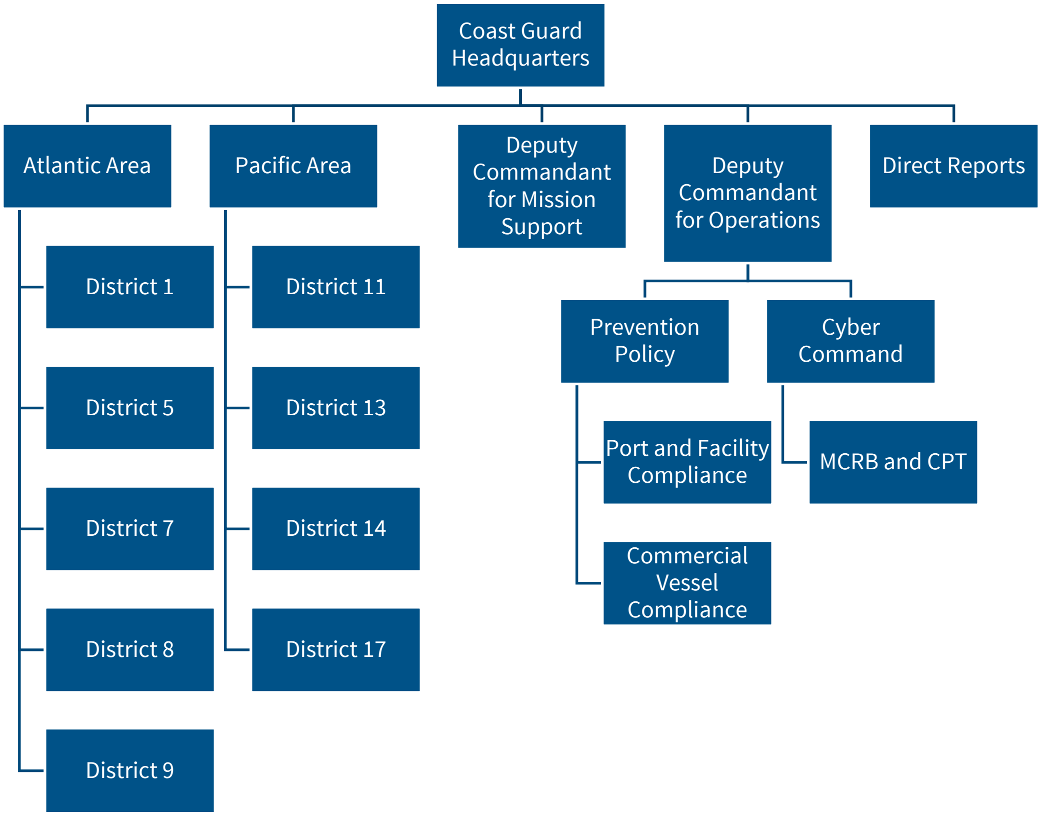
[1] Coast Guard, *Cyber Strategic Outlook* (August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.

[2] *Maritime Transportation Security Act of 2002*, Pub. L. No. 107-295, November 25, 2002, https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf.

[3] The U.S. Department of Defense's Cyber Command safeguards the Nation's maritime infrastructure and deploys units around the country to assess, prevent, respond to, and investigate cyber incidents.

Coast Guard works at the local, national, and international level to manage risk in the maritime domain. At the national level, in 2020, Coast Guard established a Maritime Cyber Readiness Branch (MCRB) within its Cyber Command unit. The MCRB is focused on raising cybersecurity readiness, resilience, and response capability throughout the MTS. The group provides outreach and engagements and shares information to increase cyber literacy at ports. When an industry stakeholder is compromised, CG Cyber Command takes steps to help mitigate damage by deploying a Cyber Protection Team (CPT). CG Cyber Command created CPTs [4] to enhance the resiliency of the MTS against cyber disruption by deploying to help prevent, detect, and respond to cyber events within the marine environment. As depicted in Figure 1, CG Cyber Command is a separate command from the area and district commands that oversee inspections.

Figure 1. Coast Guard Organizational Chart



Source: Department of Homeland Security Office of Inspector General generated based on Coast Guard documentation

[4] In October 2019, a memorandum from the U.S. Department of Defense outlined the benefits of creating CPTs as well as the structure of CPTs and mission-essential tasks for the teams.

Under current Maritime Security regulations[5] Coast Guard protects the MTS from physical and cyber threats.[6] According to these regulations and Coast Guard–issued guidance,[7] Coast Guard has the authority to require, review, and approve cybersecurity assessments[8] and plans for MTSA-regulated vessels and facilities. These assessments, completed locally in Coast Guard sectors, are separate from those conducted by CG Cyber Command and are completed by the stakeholders who own and operate vessels and maritime facilities.

We conducted this audit to determine the extent to which Coast Guard has implemented cybersecurity readiness and precautions at U.S. ports and on U.S. waterways to protect the U.S. supply chain.

Results of Audit

Coast Guard took steps to enhance the cyber posture of the maritime environment but faces challenges implementing cybersecurity readiness measures and precautions at U.S. ports and on U.S. waterways. Specifically, Coast Guard implemented services to aid private industry stakeholders at U.S. ports and on U.S. waterways. However, in fiscal year 2022, private industry stakeholders in only 36 percent of Coast Guard's sectors requested and received services provided by Coast Guard's CPTs. Further, facility and vessel inspections did not always address cybersecurity, and Coast Guard is not adequately staffed to provide cyber expertise for these inspections.

These challenges occurred because industry stakeholders are hesitant to use Coast Guard's cybersecurity services, Coast Guard does not have the authority or training to enforce private

[5] See generally Title 33 of the Code of Federal Regulations (C.F.R.), Chapter I, Subchapter H, https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H, *Maritime Security*, November 1, 2022, which implements portions of the maritime security regime required by MTSA, as codified in 46 United States Code (U.S.C.) § 701.

[6] While there is no specific mention of cybersecurity in the regulations, 33 C.F.R. § 105.305(c)(1)(v) requires that the Facility Security Assessment for MTSA-regulated facilities include the analysis of "[m]easures to protect radio and telecommunication equipment, including computer systems and networks." See also 46 U.S.C. § 70102(b)(1)(C), which states, "the Secretary shall conduct a detailed vulnerability assessment of the facilities and vessels that may be involved in a transportation security incident. The vulnerability assessment shall include … [i]dentification of weaknesses in physical security, security against cybersecurity risks, passenger and cargo security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, contingency response, and other areas as determined by the Secretary."

[7] See *Navigation and Vessel Inspection Circular 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*.

[8] Cybersecurity assessments identify and assess radio and telecommunications equipment, including computer systems and networks, and address and mitigate any identified vulnerabilities. See *Navigation and Vessel Inspection Circular 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*. See also 33 C.F.R. §§ 105.305(c)(1)(v), 105.405(a)(17) for Facilities; and 33 C.F.R. §§ 106.305(c)(1)(v), 106.405(a)(16) for Outer Continental Shelf Facilities.

industry compliance with standard cybersecurity practices, and the job series classification for a key cybersecurity position leads to hiring delays.

Due to these challenges, Coast Guard cannot fully ensure compliance with cybersecurity measures intended to protect the MTS' ports and waterways or provide awareness, guidance, and expertise to safeguard private industry stakeholders' assets. Without these protective measures in place, the U.S. supply chain will remain vulnerable to the exploitation, misuse, or simple failure of cyber systems, which may lead to injury or death, harm the marine environment, or disrupt vital trade activity.

Coast Guard Has Taken Steps to Improve the Cyber Posture of the MTS, but Industry Stakeholders Were Reluctant to Use Coast Guard Cyber Services

CG Cyber Command created CPTs to help prevent, detect, and respond to cyber events within the marine environment. As of August 2023, CG Cyber Command had two fully staffed CPT units and was creating a third unit. A fully staffed CPT unit consists of 39 Federal civilians and active-duty military personnel serving in operational and support roles. These CPT personnel are organized, trained, and equipped to target malicious cyberspace activities. Each unit has three operational teams that deploy to perform technical work for industry stakeholders, including more than 2,900 MTSA-regulated facilities, as well as the companies supporting the 19,000 domestic vessels subject to Coast Guard inspection. The teams typically perform three types of missions:

- **Assessments:** CPT personnel conduct assessments to determine the overall risk and effectiveness of the industry stakeholder's cybersecurity controls. This Coast Guard assessment mission and the resulting report give industry stakeholders an outside perspective on their current technology systems. The assessment provides information that can help industry stakeholders take steps to correct identified problems and improve preparedness for future cyberattacks. According to Coast Guard documentation, the first CPT became fully operational in May 2021. From May 2021 through March 2023, CPTs conducted 27 assessments requested by industry stakeholders. It can take a CPT 8 weeks to complete an assessment; during 2 of those weeks the CPT engages the industry stakeholder remotely and in person.

- **Hunts:** CPT personnel scan the industry stakeholder's network to discover currently undetected adversaries before critical systems or services are compromised. As with assessments, hunts involve the use of state-of-the-art technology and may be conducted remotely or onsite. From May 2021 through March 2023, CPTs conducted 14 hunts requested by industry stakeholders.

- **Incident Response:** CPT personnel assist industry stakeholders who suspect they have a compromised system or need help recovering from a cyberattack. Coast Guard's response varies based on the needs of the industry stakeholder. Mitigating incident impacts and better preparing industry stakeholders for the future helps strengthen the MTS against cyberattacks. From May 2021 through September 2022,[9] CPT conducted five incident responses requested by industry stakeholders.

From May 2021 through March 2023, Coast Guard's CPT units performed 46 cybersecurity missions for industry stakeholders in various U.S. states and the U.S. Territory of Guam. Industry stakeholders request CPT assistance through their local Coast Guard Captain of the Port[10] who then forwards the request to CG Cyber Command in Washington, D.C., or the stakeholder can directly request CPT assistance from CG Cyber Command. Before industry stakeholders engage with a CPT remotely or in person, the CPT and the industry stakeholder sign a formal Request for Technical Assistance agreement. This agreement includes rules and boundaries, including which systems the CPT can review and assess.

As part of this audit, we analyzed 15 of the 30 (50 percent) assessments conducted by CPTs[11] to identify trends and common vulnerabilities or findings, and to further define the benefit the CPT assessments provided to industry stakeholders. As a result of these 15 assessments, CPTs reported 194 incidents involving 54 different and potentially exploitable vulnerabilities. These vulnerabilities included system deficiencies that could compromise access to industry stakeholders' facilities for the transfer of cargo or lead to cargo theft, a full stop of port operations, loss of life, or environmental threats (see Figure 2). CPTs groups vulnerabilities into five severity levels: Critical, High, Medium, Low, and Informational. CPTs categorized the 194 incidents as follows:

- CPTs categorized **59 percent** (or 114 individual incidents) as involving Critical or High vulnerabilities. Critical vulnerabilities pose immediate and severe risk due to the ease of exploitation and potential severity of impact. High vulnerabilities can lead to complete application, system, or network compromise. For example, an attacker could add security badges or turn off power to a system, which could impede operations within the MTS.

- CPTs categorized an additional **29 percent** (or 57 individual incidents) as involving Medium vulnerabilities. Medium vulnerabilities may result in unauthorized disclosure of sensitive customer information.

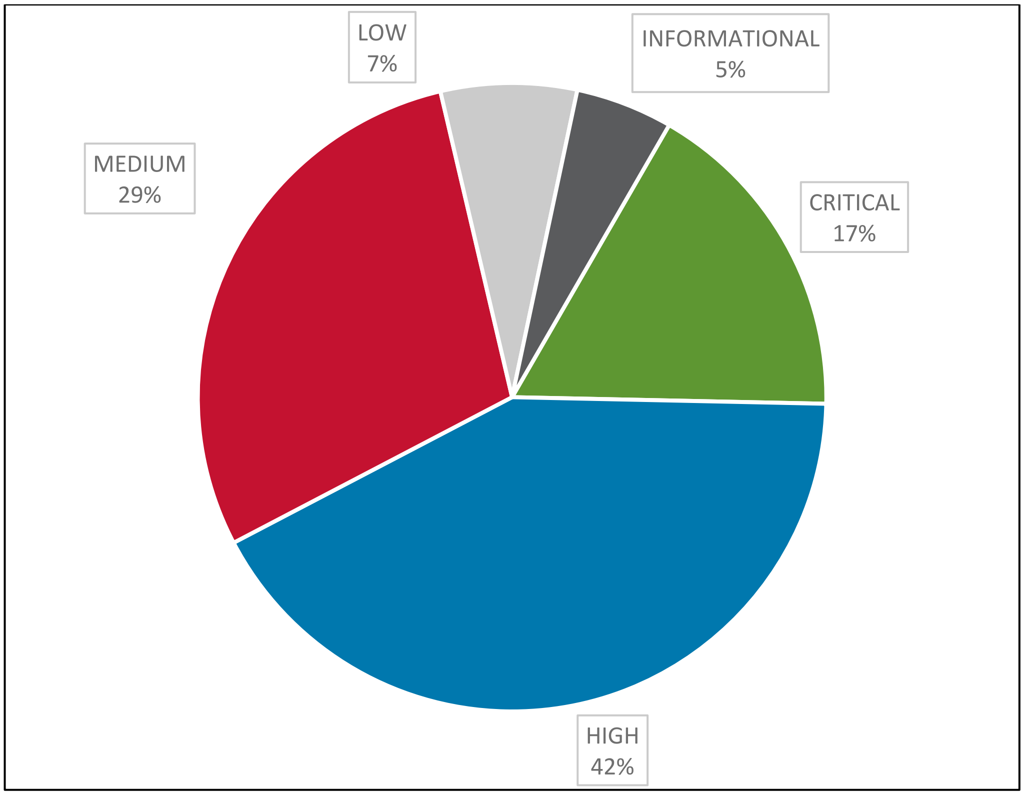
[9] Coast Guard data we received did not include any CPT incident responses for October 2022 through March 2023.

[10] A Coast Guard Captain of the Port has a unique, broad authority to oversee important aspects of safety and security in the MTS. Individuals in this role at different ports across the United States are in positions of high visibility.

[11] We requested 15 assessments for analysis; Coast Guard selected the assessments and then redacted company-specific or proprietary information from the files. The total number of 30 assessments includes 3 assessments performed before the first CPT became fully operational in March 2021.

- Finally, CPTs categorized **7 percent** (or 14 individual incidents) as involving Low vulnerabilities and the remaining **5 percent** (or 9 individual incidents) as involving Informational vulnerabilities.[12] These findings represent areas that the industry stakeholder should be aware of, but that do not require immediate action.

Figure 2. Severity Levels of CPT-Identified Vulnerabilities



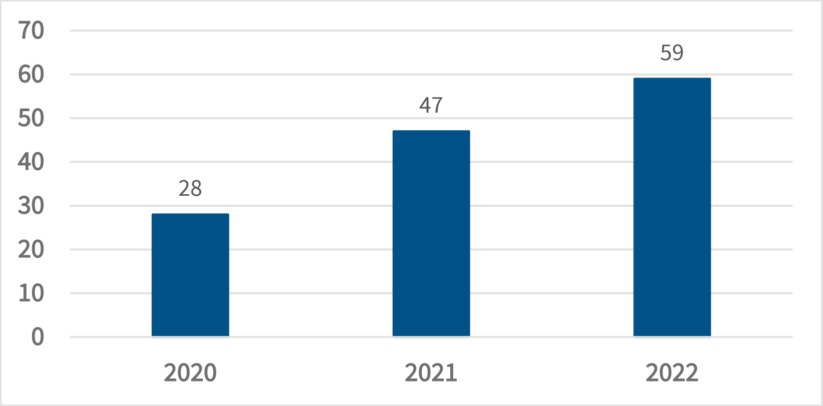
Source: DHS OIG analysis of CPT assessments

Over the past 3 years, the number of cyber incidents reported to and reviewed by Coast Guard increased by 111 percent, from 28 incidents in 2020 to 59 incidents in 2022, as shown in Figure 3. Although the number of cyber incidents reported[13] has increased each year, Coast Guard reported industry stakeholders in just 13 of its 36 sectors requested and received Coast Guard's free CPT services to help prevent or respond to cyberattacks.

[12] CPTs report any Low vulnerabilities as items of interest; they are normally not exploitable. Informational vulnerabilities are potential weaknesses within the system that also cannot be readily exploited.

[13] MTSA-regulated vessels and facilities must report cyber-related transportation security incidents, breaches of security, and suspicious activity to Coast Guard.

Figure 3. Cyber Incidents Reported to and Reviewed by Coast Guard from 2020 to 2022



Source: Coast Guard documentation[14]

Coast Guard Cybersecurity Guidance

Coast Guard has also instituted guidance for cybersecurity-related awareness and protections. In 2015, Coast Guard issued the *U.S. Coast Guard's Cyber Strategic Outlook*, establishing cyberspace as a new operational domain for Coast Guard. Then, in December of 2016, Coast Guard's Prevention Policy Branch provided guidance[15] on how cyber incidents relate to Coast Guard reporting requirements for breaches of security and suspicious activity. The 2016 policy document also outlines when and how to report a cyber incident. As cybersecurity threats continue to evolve, Coast Guard released an updated version of its Cyber Strategy in August 2021. The 2021 *Cyber Strategic Outlook*[16] updates the 2015 strategy, ensuring Coast Guard's readiness to conduct missions in contested cyberspace, protect the MTS, and identify and combat bad actors in cyberspace.

In February 2020, Coast Guard published *Navigation and Vessel Inspection Circular 01-20*,[17] requiring all MTSA-regulated facilities to conduct a cybersecurity vulnerability assessment. Coast Guard gave facility owners and operators 18 months to implement the new cybersecurity requirement.[18] In addition, starting on October 1, 2021, Coast Guard required facilities to submit

[14] Every year CG Cyber Command releases its *Cyber Trends and Insights in the Marine Environment*, which summarizes its findings from CPT assessments and provides recommended mitigations.
[15] Coast Guard Policy Letter No. 08-16, *Reporting Suspicious Activity and Breaches of Security,* December 14, 2016.
[16] Coast Guard, *Cyber Strategic Outlook* (August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.
[17] https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023.
[18] Coast Guard released a *Maritime Cybersecurity Assessment and Annex Guide* to help industry stakeholders identify and describe cybersecurity vulnerabilities as part of the Facility Security Assessment process.

a cybersecurity Facility Security Assessment and a subsequent Facility Security Plan addressing risks identified in the security assessments by October 1, 2022. These documents are submitted to Coast Guard for review and approval.[19]

Coast Guard also took steps to address cybersecurity risk for vessels. In October 2020, Coast Guard's Office of Commercial Vessel Compliance issued (CVC-WI-027(2)), *Vessel Cyber Risk Management Work Instruction,*[20] which contains guidance for assessing cyber risk on vessels to ensure vessels do not pose a risk to the MTS in the event of a cyberattack. On January 1, 2021, Coast Guard advised all U.S. vessels with a Safety Management System[21] to address cybersecurity risk. Similar to facilities, vessel security assessments are completed by industry stakeholders and incorporated into the vessel security plans submitted to Coast Guard for review and approval.

In September 2022, Coast Guard released the *Marine Transportation System Cyber Incident Response Playbook* for Coast Guard Captains of the Port; this playbook provides overarching cyber incident management policy, delineates responsibilities, and summarizes Coast Guard authorities for cyber incident response. More recently, in July 2023, Coast Guard released *Navigation and Vessel Inspection Circular 09-02*, Change 6, providing guidance to Area Maritime Security Committees for developing Area Maritime Security Plans that address cyber risks. This includes guidance for Area Maritime Security Assessments and a template for a Cybersecurity Risk Plan. Area Maritime Security Committees were established by MTSA to provide contingency planning, development, review, and update of Area Maritime Security Plans, and to enhance communication between port stakeholders within Federal, state, and local agencies, and in industry, to address maritime security issues.

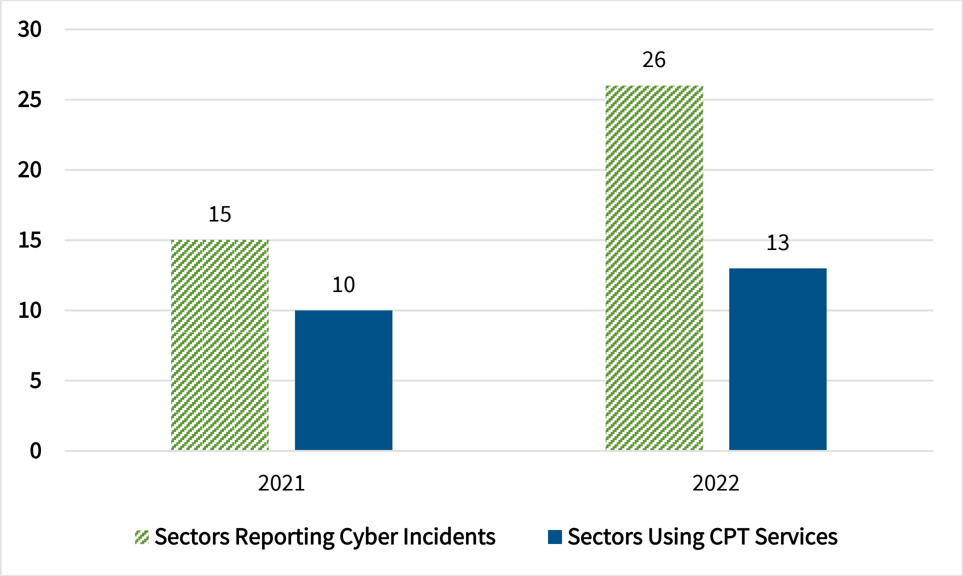
Industry Stakeholders Are Hesitant to Use CPT Services

Although industry stakeholders identify and report cyber events, they do not consistently request CPT's services to improve their cybersecurity posture. For example, none of the private industry stakeholders in the six sectors that make up Coast Guard's District 7[22] requested CPT services from 2021 through 2022 despite a confirmed ransomware and phishing/spoofing incident within the district. Figure 4 shows the number of Coast Guard sectors reporting cyber incidents during 2021 and 2022 compared to the number of sectors that used CPT services. As shown in Figure 4, in 2021, Coast Guard reported cyber incidents in 15 of its 36 sectors.[23] This

[19] See 33 C.F.R. §105.305, *Facility Security Assessment (FSA) Requirements*.
[20] https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf.
[21] A Safety Management System is a document catalog containing a vessel's certifications, maintenance records, training, security assessments, and plans, among other documents.
[22] District 7, which is located in the southeastern region of the United States, includes 6 of Coast Guard's 36 sectors: Sector Charleston, Sector Jacksonville, Sector Key West, Sector Miami, Sector San Juan, and Sector St. Petersburg.
[23] This includes 10 sectors experiencing phishing incidents (where information is obtained via a fake email prompting the user to provide data via social engineering) and 8 sectors experiencing ransomware incidents.

means that 42 percent of Coast Guard's sectors received notice of a cyber incident. However, industry stakeholders from only 10 of the 36 (28 percent) Coast Guard sectors received CPT services. Similarly, in 2022, Coast Guard reported cyber incidents in 26 of its 36 sectors (72 percent), but CPTs performed services in just 13 sectors for industry stakeholders (36 percent).

Figure 4. Number of Coast Guard Sectors Reporting Cyber Incidents Compared to Sectors Using CPT Services in 2021 and 2022.[24]



Source: DHS OIG based on Coast Guard documentation

Both Coast Guard and private industry stakeholders told us industry stakeholders are hesitant to request Coast Guard's CPT services, given Coast Guard's traditional role in regulating and enforcing laws. Coast Guard personnel said industry stakeholders are reluctant to seek CPT services due to concerns that CPT may issue fines if it identifies cyber deficiencies or instances of poor cyber hygiene. Further, according to Coast Guard personnel, industry stakeholders with very small operations are reluctant to use CPT services, in part, because they may not be able to afford enhancements to their already outdated or vulnerable information technology equipment.

Two industry stakeholders we spoke with confirmed an initial hesitancy at having Coast Guard examine their systems and a concern about being fined if vulnerabilities were found.[25] These

Attacks like ransomware can impact a port's operating control systems, possibly leading to cargo theft or a full stop of port operations, resulting in financial losses and disruptions to the supply chain.

[24] CG Cyber Command's *2021* and *2022 Cyber Trends and Insights in the Marine Environment*.

[25] While Coast Guard can fine private industry stakeholders for vulnerabilities found during an inspection, CPTs do not fine industry stakeholders for vulnerabilities uncovered during assessments, hunts, and incident responses.

industry stakeholders described having to build a relationship of trust with Coast Guard before eventually benefitting from Coast Guard's services. For example, the Chief Security Officer of a private industry company explained how, despite early doubts, the company found the CPT assessment beneficial and used the resulting report to secure Federal Emergency Management Agency grant funding to enhance its cyber protections. The Chief Security Officer noted the company would like to use CPT services again in the future.

Coast Guard's Cybersecurity Inspections Are Limited by Its Lack of Authority and Expertise to Address Cybersecurity Vulnerabilities

In accordance with MTSA and the C.F.R., Coast Guard conducts vessel and facility inspections.[26] These vessel and facility inspections primarily focus on physical safety and security issues, such as whether firefighting equipment is functional, alarm systems are operational, and navigational systems work. Despite Coast Guard's internal instructions and job aids[27] implementing the inclusion of cybersecurity elements during vessel and facility inspections, eight of the nine inspections we observed[28] did not address cybersecurity on vessels and within facilities.[29] Reviewing cybersecurity elements includes looking at basic cyber hygiene (such as locked workstations or openly displayed passwords) or determining whether a cybersecurity event was a factor in the failure of an onboard system.

If inspections do include cybersecurity, the inspector[30] usually only checks whether the vessel or facility has completed cybersecurity paperwork. At one location, a facility supervisor stated that facility inspectors used a cyber job aid provided by the Coast Guard Office of Port and Facility Compliance to review cybersecurity during each inspection. Yet, when the audit team spoke separately with facility inspectors at that location, they admitted to not reviewing cybersecurity during the inspections and only focusing on physical safety.

During an inspection, when an inspector discovers a safety or security issue, the vessel or facility receives a written deficiency requiring resolution of the issue and possibly a monetary fine. Despite the audit team witnessing cybersecurity vulnerabilities[31] during our observation of

[26] Coast Guard performs inspections of domestic vessels and MTSA-regulated facilities. It performs examinations of foreign vessels. For ease of understanding, we will refer to examinations and inspections as inspections.

[27] CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction* (February 2021) and *Facility Inspector–Cyber Job Aid*, Rev 1 (March 2020).

[28] We observed inspections and examinations at port facilities, onboard international vessels moving cargo, vehicles, and sand, and on domestic ferries.

[29] At one of our site visits, cybersecurity was the focus of an added quarterly review, which required inspectors to complete a more in-depth look. Even at this inspection, inspectors only reviewed paperwork and told DHS OIG they did not really understand the information in the cybersecurity paperwork.

[30] Typically, Coast Guard inspectors perform inspections of domestic vessels and MTSA-regulated facilities while Marine Science Technicians perform examinations of foreign vessels. We will refer to both groups as inspectors.

[31] These vulnerabilities included unlocked, unattended workstations and passwords posted on or near workstations.

inspections, inspectors did not make any formal recommendations or issue any written deficiencies. We visited two sectors after Coast Guard's enhanced cybersecurity inspection quarter ended; inspectors in those two sectors were unaware of any prior vessel or facility deficiencies issued in relation to cybersecurity.

Further, the inspections personnel we spoke with expressed a limited understanding of how to address cybersecurity when conducting inspections. Personnel were not certain how to address cybersecurity risks detailed in Facility Security Plans or Vessel Safety Management Systems and did not understand the terminology used in these documents. They also did not feel confident reviewing cybersecurity as part of the inspection. For example, inspectors did not have the knowledge to determine the quality of cybersecurity precautions implemented on a vessel or in a facility. One supervisor further emphasized that inspectors were not well-equipped or comfortable asking cyber-related questions during inspections.

According to Coast Guard's 2021 *Cyber Trends and Insights in the Marine Environment*, Coast Guard will ensure the safety and security of the MTS by executing its authorities through a robust framework of prevention and response activities. With staff who are not equipped to fully assess the implementation of cybersecurity controls during an inspection, we are concerned Coast Guard may not be able to fully ensure the safety and security of the MTS. According to Coast Guard documentation, as evident by recent ransomware attacks such as the *NotPetya* attack,[32] the rapidly cascading nature of cyberattacks can impose unrecoverable losses to port operations, electronically stored information, national economic activity, and global supply chains.

Coast Guard Has Insufficient Authority to Address Vulnerabilities

Coast Guard's authority and responsibility to respond to cybersecurity vulnerabilities are not fully developed. Coast Guard requires both vessels and facilities to account for cybersecurity in security assessments and plans. As mentioned before, according to *Navigation and Vessel Inspection Circular 01-20* in conjunction with MTSA, Coast Guard must combat cyber threats within the MTS and has the authority to require, review, and approve cybersecurity assessments and plans for MTSA-regulated vessels and facilities. Vessels are required to document cybersecurity assessments and security plans,[33] and owners and operators of facilities must address cybersecurity in their security assessments and plans.[34] These assessments and plans are completed by the industry stakeholders and submitted to Coast Guard for review and approval.

[32] This attack in June 2017 originally targeted Ukraine but spread to more than 60 countries. The ransomware attack destroyed computer systems of thousands across those countries.

[33] 33 C.F.R. § 104.300 (d)(11); 33 C.F.R. § 104.305 (d)(2)(v); 33 C.F.R. § 104.400 (a)(3); and 33 C.F.R. § 104.405 (a)(17).

[34] 33 C.F.R. Chapter I, Subchapter H*,* https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H,Part 105, *Maritime Security Facilities*, and Part 106, *Marine Security: Outer Continental Shelf (OCS) Facilities,* November 1, 2022.

Despite its role in evaluating security assessments and plans for vessels and facilities, Coast Guard is limited in its ability to force facility owners and operators to comply with recommendations if a vulnerability is identified during review. MTSA gives vessel and facility owners and operators the discretion to determine how to best identify, assess, and address vulnerabilities in their computer systems and networks. This means Coast Guard can identify a vulnerability in a vessel or facility assessment or plan but cannot mandate how the vessel or facility resolves the issue.

Inspection-based Cyber Authority Is Also Limited

Similarly, inspectors conducting facility and vessel security inspections do not have regulations to support a written deficiency if they identify a cybersecurity vulnerability during the inspection process. During all three of our sector site visits, Coast Guard personnel acknowledged that, due to a lack of regulations, they cannot remedy cybersecurity vulnerabilities in the same way they would correct a physical safety or security violation.

Current regulations for facilities and vessels do not contain specifics about cybersecurity.

- **MTSA-regulated facilities:** Although 33 C.F.R.[35] briefly mentions computers and networks, it neither specifically addresses cybersecurity nor gives inspectors the authority to enforce compliance when deficiencies are found.[36] The lack of specificity within existing regulations allowed Coast Guard to interpret existing regulations to include cybersecurity. Specifically, *Navigation and Vessel Inspection Circular 01-20* expanded the interpretation of vulnerabilities to telecommunications to include cybersecurity, but the guidance still only includes two sentences:

  > *"Existing regulations require the owners and operators of MTSA-regulated facilities to analyze vulnerabilities associated with radio and telecommunication equipment, including computer systems and networks. Vulnerabilities in computer systems and networks are commonly referred to as cyber security vulnerabilities."*

- **Vessels:** Domestic and foreign vessels are governed by several varied regulations.

[35] According to 33 C.F.R. §105.305(c)(1)(v), the analysis for a Facility Security Assessment must consider "[m]easures to protect radio and telecommunication equipment, including computer systems and networks." See also 46 U.S.C. § 70102(b)(1)(C), which states, "… the Secretary shall conduct a detailed vulnerability assessment of the facilities and vessels that may be involved in a transportation security incident. The vulnerability assessment shall include … [i]dentification of weaknesses in physical security, security against cybersecurity risks, passenger and cargo security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, contingency response, and other areas as determined by the Secretary."

[36] According to 46 U.S.C. §§ 70102(b)(1)(A)-(C), the role of the Secretary is to "identify" vulnerabilities; no language is contained therein prescribing how the vulnerability findings should be addressed. 33 C.F.R. § 106.400(a)(3) indicates that it is the facility owner or operator who "must address each vulnerability identified in the Facility Security Assessment."

> Domestic and foreign vessels with a Safety Management System are subject to the International Maritime Organization's *Guidelines on Maritime Cyber Risk Management,*[37] which addresses requirements for basic cyber hygiene that domestic regulation currently lacks. Also, all U.S. vessels subject to MTSA regulations are required to develop a Vessel Security Assessment (VSA)[38] and incorporate cybersecurity. Vulnerabilities identified in the VSA must be addressed in the Vessel Security Plan.[39] Coast Guard Work Instruction (CVC-WI-027(2)) provides additional guidance for private industry stakeholders on incorporating cybersecurity into both the VSA and Vessel Security Plan.
>
> As with MTSA facilities, the current regulations lack specificity regarding cybersecurity requirements for domestic vessels, which makes enforcement of cybersecurity regulations difficult.

Coast Guard's Office of Port and Facility Compliance told DHS OIG that Coast Guard is currently updating maritime security regulations to incorporate minimum cybersecurity requirements across MTSA-regulated facilities and vessels. This would establish a minimum cybersecurity requirement for domestic vessels and domestic facilities subject to MTSA. These draft regulations would not apply to any foreign vessels subject to 33 C.F.R. Part 104.[40] If approved, these regulatory updates would give Coast Guard greater enforcement authority, mandate cybersecurity requirements across domestic private industry, and establish cybersecurity officers across the MTS to maintain robust cybersecurity.[41]

[37] The International Maritime Organization addressed cybersecurity measures for foreign vessels through MSC/FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*, and Maritime Security Committee Resolution 428(98), *Maritime Cyber Risk Management in Safety Management Systems* (June 16, 2017), which recognized the urgent need to raise awareness of cyber risk and vulnerabilities. Coast Guard continues to use the process in CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction*, to ensure cybersecurity readiness on foreign vessels, which are exempt from Coast Guard's newly proposed updates to maritime security regulations.

[38] 33 C.F.R. §104.300, 104.305, and 104.310.

[39] 33 C.F.R. §104.400(a)(3).

[40] According to International Maritime Organization guidance, foreign vessels are required to incorporate cyber risk management into their mandated Safety Management Systems.

[41] On February 21, 2024, President Biden issued Executive Order 14116 on *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities in the United States* to further enable the protection and security of vessels, harbors, ports, and waterfront facilities by explicitly addressing cyber threats. This Executive Order allows the Captain of the Port additional powers to, among other things, respond to malicious cyber activity; inspect and search vessels and waterfront facilities, including cyber systems and networks; require facilities to correct unsatisfactory cyber conditions; and require reporting of cyber incidents (actual or threatened) that involve or endanger vessels, harbors, ports, or waterfront facilities to the Captain of the Port and other authorities. Because this Executive Order was published after our fieldwork period, we did not assess its impact on Coast Guard's ability to secure the MTS.

Coast Guard Inspections Personnel Lack Cybersecurity Subject Matter Expertise

Despite requirements to include cybersecurity elements during inspections, inspectors we observed did not perform cybersecurity checks. We attribute that in part to the fact that Coast Guard does not have standardized cyber training for inspectors to ensure they can identify when private industry fails to comply with standard cybersecurity practices. Inspectors from the three sectors we visited stated they receive little to no cybersecurity training outside of the annual DHS-wide cybersecurity training. Inspectors at one field office stated they would like more training, but that training needs to be based on enforceable regulations. A supervisor at another site noted the disadvantage to inspectors without regulations or training to guide them. A headquarters official confirmed that specific regulations are needed before training can be developed. Coast Guard also confirmed to us that it does not provide a formal cybersecurity training program for inspectors.

Although Coast Guard partners with an accredited educational institution to offer a specialized education course on maritime cybersecurity, funding restrictions limit the number of Coast Guard personnel who can attend. According to the institution providing the training, Coast Guard sends 80 personnel including officers, enlisted service members, and Coast Guard civilians to the course each fiscal year. According to institution officials, they would host more sessions throughout the year but are limited by the number of sessions Coast Guard can fund.

Without a formal training program, Coast Guard inspections personnel rely on written guidance. When we asked inspectors in the field what guidance they used, the inspectors showed us cybersecurity job aids that supplement their standard guidance. Our review of provided job aids determined that the steps in the guidance would be hard for an inspector to check or definitively confirm during their normal work, such as whether third party vendors are vetted before they connect to a facility or vessel’s network or whether access control systems and software are updated on a regular schedule. Coast Guard’s Office of Port and Facility Compliance confirmed that the component cannot create standard cybersecurity training for inspectors without an actual cybersecurity regulation that requires it.

Coast Guard Has Not Yet Fully Staffed Its Local Cybersecurity Expert Positions

In February 2021, Coast Guard developed a local position, the Marine Transportation Security Specialist–Cyber (MTSS-C), to work with Coast Guard districts and sectors and private industry stakeholders to improve the MTS’ cyber posture. According to the position description, an MTSS-C is responsible for implementing cybersecurity regulations, guidelines, and laws. MTSS-Cs also serve as liaisons between the Coast Guard Captain of the Port and port stakeholders. While they work with inspections teams, their obligations extend beyond facility and vessel inspections performed by Coast Guard. They also ensure Coast Guard districts and sectors are ready to help mitigate, respond to, recover from, and protect the MTS from cybersecurity incidents. Additionally, if cyberattacks occur, MTSS-Cs help state and local officials, along with Coast Guard personnel, understand the situation.

As of February 2023, 13 of 52 MTSS-C positions remained unfilled or took significant time and effort to fill. These 52 MTSS-C positions are allocated across Coast Guard's 6 marine safety units, 36 sectors, 9 districts, and 2 command areas. Although Coast Guard made some progress filling MTSS-C positions during our audit, as of May 2023, Coast Guard had not yet filled 8 of the 52 MTSS-C positions. The 8 unfilled positions consisted of 1 marine safety unit position and 7 sector-level positions.

Filling positions required considerable effort. At one location we visited, the MTSS-C position was vacant for more than 2 years. Another location had to post the position five times before hiring a qualified candidate, while a third location needed four listings to bring a qualified candidate on board. This extended timeframe does not comply with the 80-day timeframe suggested in the U.S. Office of Personnel Management's (OPM) *End-to-End Hiring RoadMap* and resulted in continued vacancies in these key cyber positions.

The Job Series Classification for MTSS-C Positions Leads to Hiring Challenges

The classification of the position creates a challenge in hiring qualified personnel. Coast Guard classified the MTSS-C position as GS-0301, which is the Miscellaneous Administration and Program series. Although GS-0301 jobs often do not require technical expertise, a February 2021 Concept of Operations for the MTSS-C position and current MTSS-C job postings both included technical cybersecurity-related duties among the position's responsibilities. Traditionally, positions in cybersecurity are listed under the GS-2210 series.[42] According to Coast Guard personnel, Coast Guard intentionally used a non-technical series to permit a broader range of applicants who may have cyber expertise or a background in MTS to apply for the position. The non-technical series may also result in qualified, technical applicants not seeing the job posting and thus not applying. As a result, the selected series may cause Coast Guard to miss out on more technically proficient applicants.

The use of a GS-0301 job series classification for the MTSS-C position also makes it difficult to use direct hire authority,[43] which would allow local Coast Guard districts and sectors to fill the position more quickly with a qualified candidate. Use of this authority expedites hiring as it allows organizations to appoint a specific person to a role if they meet all necessary requirements. The Cybersecurity and Infrastructure Security Agency (CISA), another DHS

[42] GS-2210 is the Information Technology Management series.

[43] OPM approves direct hire authority, which allows certain Executive agencies with delegated examining authority to fill vacancies when a critical hiring need or severe shortage of candidates exists. See 5 C.F.R. Part 337, Subpart B.

component, uses this authority to fill its cyber positions. According to OPM guidelines,[44] Coast Guard would be permitted to use direct hire authority for GS-2210 positions.

Conclusion

With $5.4 trillion and 90 percent of U.S. imports and exports flowing through the marine environment annually, the MTS is a consistent target for adversarial nation states and cyber criminals. The CG Cyber Command observed attacks targeted at companies providing logistics or technology services with the ability to impact a number of organizations simultaneously. Such attacks could affect industry software, such as ship management software that could impact a large portion of the MTS at once.

Coast Guard is taking steps that may improve the cyber posture of the MTS by offering complimentary cybersecurity services, such as assessments, hunts, and incident response, and by hiring sector-level MTSS-Cs. These efforts mitigated the impact of cyberattacks on the MTS and better prepared industry stakeholders for the future, ultimately strengthening the MTS against cyberattacks and protecting the supply chain, U.S. ports, and U.S. waterways. However, despite a promising increase in voluntary reporting of cyberattacks and incidents, Coast Guard acknowledged many organizations remain reluctant to report or share information with the component.

Without regulations providing the authority to better govern cybersecurity, Coast Guard will remain unable to enforce industry stakeholder compliance with cybersecurity measures intended to protect the MTS. Additionally, without trained cyber personnel in the districts and sectors to work with industry stakeholders, understanding of cyber vulnerabilities and the use of Coast Guard–provided cybersecurity services will not spread quickly. Limited regulatory authority and inadequate training and subject matter expertise across Coast Guard sectors impede Coast Guard's ability to carry out its responsibilities for securing the MTS against cyber threats.

Recommendations

Recommendation 1: We recommend that Coast Guard's Cyber Command and Office of Port and Facility Compliance develop and implement a plan of action with established benchmarks for the Cyber Protection Team and the Maritime Cyber Readiness Branch to work with Marine Transportation Security Specialists–Cyber to enhance coordination and to build working relationships with private industry stakeholders.

[44] 5 C.F.R. Part 337, Subpart B, Subsections 337.204, *Severe shortage of candidates*, and 337.205, *Critical hiring needs*.

Recommendation 2: We recommend that Coast Guard's Assistant Commandant for Prevention Policy complete and publish cybersecurity-specific regulations providing enforcement authority for facility and vessel inspections.

Recommendation 3: We recommend that Coast Guard's Office of Port and Facility Compliance establish standardized cybersecurity training on enforceable authorities.

Recommendation 4: We recommend that Coast Guard's Office of Port and Facility Compliance review and determine whether the Marine Transportation Security Specialist–Cyber position description and job series is the correct designation based on the needs of the position.

Management Comments and OIG Analysis

DHS provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments from the Department on the draft report, and we revised the report as appropriate. DHS concurred with all four recommendations. Recommendations 1 and 4 are open and resolved, and recommendations 2 and 3 are open and unresolved. A summary of DHS' response and our analysis follows.

OIG Response to General Comments

We appreciate the Department's positive comments about our draft report. The Department was pleased to note our recognition of the efforts of the Coast Guard Cyber Protection Teams to enhance cyber posture and protect the MTS from cyber disruptions. Additionally, the Department emphasized Coast Guard's continued commitment to strengthening internal cyber readiness and aiding private industry partners in efforts to prevent, detect, and respond to cyber events in the maritime environment. However, the Department and CISA expressed concern over our statement regarding CISA's participation in our audit fieldwork. We appreciate the assistance that CISA provided during this audit, but we stand by our statement that CISA declined to schedule a meeting with relevant personnel and provide timely access to requested documents and information on numerous occasions throughout the audit.

Additionally, Coast Guard addressed concerns about the accuracy of the information in our report. Coast Guard noted sending DHS OIG technical comments under separate cover. As a part of our standard audit process, we provide the Department with a draft so that they can review the report to ensure its findings are accurate. We reviewed Coast Guard's technical edits and comments and accepted their suggested revisions as appropriate and supported by audit evidence. We appreciate Coast Guard's efforts over the course of the audit to provide information and context for our report. We offered the Department a chance to review and revise their statements about the accuracy of our reporting, but it did not respond.

DHS Response to Recommendation 1: Concur. CG Cyber Command, the Office of Port and Facility Compliance, and the Office of Cyberspace Forces regularly collaborate with each other and the MTSS-Cs on cyber risk management activities. In May 2024, Coast Guard hosted a workshop with MTSS-Cs that included cyber risk management on the agenda. The workshop also initiated a plan of action to further build industry relationships. DHS estimates these actions will be completed by April 30, 2025.

OIG Analysis: We believe the development of a plan of action to further build industry relationships is in line with our recommendation. We will close this recommendation once we are able to review this plan and learn more about the planned implementation, the work with CPTs, and the benchmarks for completion. This recommendation is open and resolved.

DHS Response to Recommendation 2: Concur. On February 22, 2024, Coast Guard published a Notice of Proposed Rulemaking entitled "Cybersecurity in the Marine Transportation System." Coast Guard used the Notice of Proposed Rulemaking to seek public comment on proposed regulations specifically focused on establishing minimum cybersecurity requirements for U.S. flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to MTSA regulations. The public comment period ended on May 22, 2024. Coast Guard is currently reviewing public comment results to determine next steps. DHS did not provide an estimated date of completion.

OIG Analysis: We believe the Notice of Proposed Rulemaking adheres to the intent of our recommendation. Finalization and publication of this new set of regulations will help Coast Guard with its cybersecurity enforcement authorities. We will close this recommendation once we review the finalized, published regulations to ensure alignment with the recommendation. Because there is no estimated completion date, this recommendation is open and unresolved.

DHS Response to Recommendation 3: Concur. Coast Guard's Force Readiness Command is actively developing a Marine Safety Personnel Cyber Training e-Learning course with input from other Coast Guard entities. However, formal training for Coast Guard's workforce on the compliance and enforcement activities of Coast Guard cyber security regulations requires the publication of a final rule on cyber risk management regulations. DHS did not provide an estimated completion date.

OIG Analysis: We believe this new training, when brought in line with the proposed new regulations, will provide much-needed instruction to Coast Guard personnel. We will close this recommendation when we review course materials and Coast Guard provides information on how this training will be disseminated to appropriate personnel. Because there is no estimated completion date, this recommendation is open and unresolved.

DHS Response to Recommendation 4: Concur. The Office of Port and Facility Compliance and the Office of Cyberspace Forces are reviewing the existing position description and job series and comparing each against MTSS-C expectations and experiences in the field. This was also a topic of discussion during the May 2024 MTSS-C workshop mentioned in recommendation 1. Feedback from this workshop is under evaluation and will be included in the final determination as to whether the MTSS-C position description and job series are correct and whether any further actions are appropriate. DHS estimates completion of this work by April 30, 2025.

OIG Analysis: We believe a multi-faceted review of the MTSS-C position will provide Coast Guard leadership with important information to evaluate the position description and job series. We will close this recommendation once we review workshop feedback and the overall evaluation and determination documentation as Coast Guard works through this process. This recommendation is open and resolved.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent to which Coast Guard has implemented cybersecurity readiness and precautions at U.S. ports and on U.S. waterways to protect the U.S. supply chain.

To conduct this audit, we held nearly 50 in-person meetings and virtual interviews with Coast Guard personnel to learn about Coast Guard's implementation of cybersecurity readiness and precautions at U.S. ports and on U.S. waterways. At Coast Guard Headquarters, we interviewed representatives from CG Cyber Command, including the MCRB and CPTs. We also met with Coast Guard subject matter experts at the Office of Port and Facility Compliance, Office of Cyberspace Forces, Office of Commercial Vessel Compliance, Office of Inspections and Compliance, and Human Resources Command. Our team conducted three site visits to Coast Guard sectors (Jacksonville, Florida; New York, New York; and San Francisco, California) as well as a site visit to Washington, D.C. During our site visits, we met with Coast Guard personnel from the Prevention Department, including individuals responsible for training, domestic vessel inspection, foreign vessel inspection, and facility inspection. We also met with intelligence personnel, Captains of the Port, and MTSS-Cs. Additionally, we met with private industry stakeholders for context. Finally, we observed a total of nine vessel and facility inspections, as well as a CPT assessment mission, including a demonstration of the standard tool kit CPT personnel use to do their work.

We also interviewed officials from CISA's National Risk Management Center and the Infrastructure Security Division, as well as two CISA Regional Protective Security Advisors. We tried to meet with personnel from CISA's Cybersecurity Division during this audit, but the Cybersecurity Division did not set up a meeting with relevant personnel. CISA also did not provide documents we requested by the end of our fieldwork period. This limited access to information pertinent to our scope resulted in an audit risk and a scope limitation. Our team made every effort to reduce this limitation. However, this lack of information resulted in our report focusing solely on Coast Guard's efforts. While CISA is a partner in reducing cyber risk, Coast Guard was the primary focus of our audit, and our team was still able to answer our objective. We are unable to include information on the services CISA provides or the benefit those services yield.

We requested and reviewed approximately 250 documents and files from Coast Guard. These files include current and draft authorities, job aids, work instructions, policies, and standards related to our audit objective. Additionally, our team requested, received, and analyzed 15 cyber assessments performed by CPTs. Coast Guard selected our sample (50 percent of the prior years' assessments) and redacted company-specific or proprietary information. Our planned analysis was not impacted by the removal of company or proprietary information.

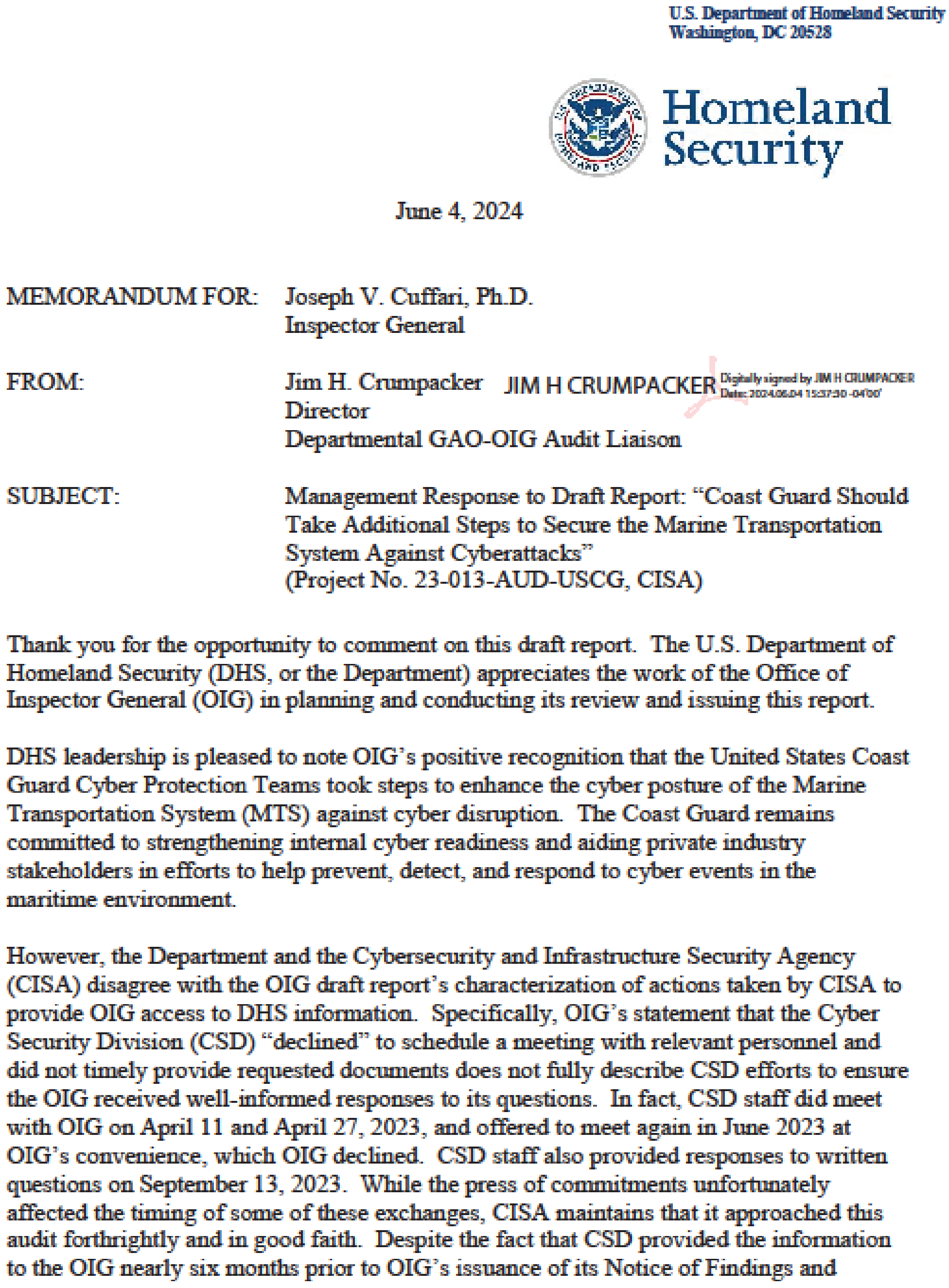
Our review also included an assessment of the 17 internal control principles relevant to the audit objective. During audit fieldwork, we identified weaknesses related to conducting cyber assessments at port facilities and onboard vessels traversing U.S. waterways, as discussed in this report. Because our review was limited to internal controls, components, and underlying principles relevant to the audit objective, this report may not disclose all control deficiencies that may have existed in Coast Guard at the time of this audit.

We conducted this audit from January through August 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to 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.

DHS OIG's Access to DHS Information

During this audit, Coast Guard provided timely responses to our requests for information and did not delay or deny access to Coast Guard information we requested. However, throughout our audit, we attempted to meet with members of CISA's Cybersecurity Division. The Cybersecurity Division declined to schedule a meeting with relevant personnel and did not provide documents we requested by the end of our fieldwork period.

Appendix B:
DHS Comments on the Draft Report



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

Homeland Security

June 4, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

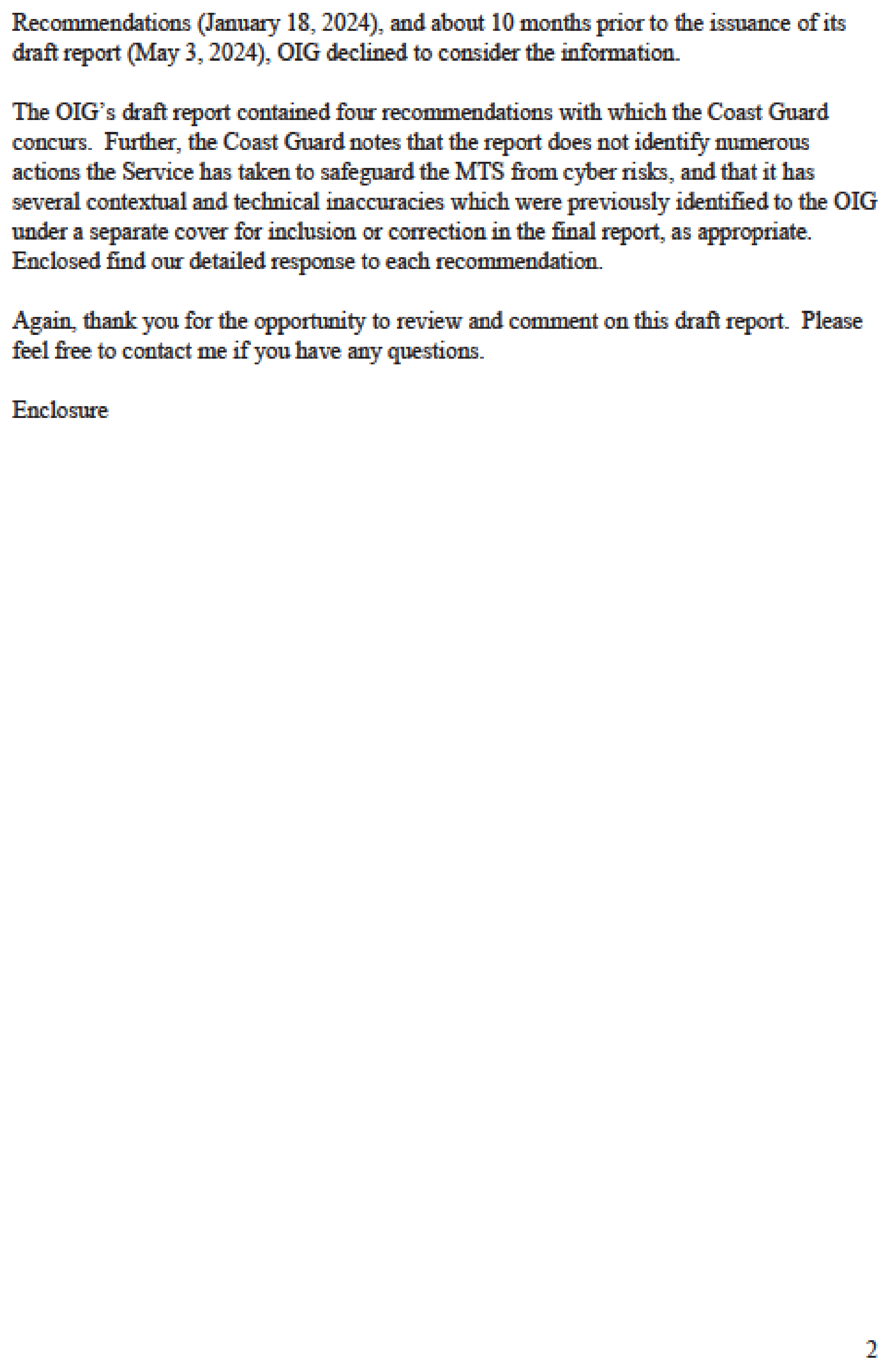
FROM: Jim H. Crumpacker JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2024.06.04 15:37:30 -04'00'
Director
Departmental GAO-OIG Audit Liaison

SUBJECT: Management Response to Draft Report: "Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks"
(Project No. 23-013-AUD-USCG, CISA)

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

DHS leadership is pleased to note OIG's positive recognition that the United States Coast Guard Cyber Protection Teams took steps to enhance the cyber posture of the Marine Transportation System (MTS) against cyber disruption. The Coast Guard remains committed to strengthening internal cyber readiness and aiding private industry stakeholders in efforts to help prevent, detect, and respond to cyber events in the maritime environment.

However, the Department and the Cybersecurity and Infrastructure Security Agency (CISA) disagree with the OIG draft report's characterization of actions taken by CISA to provide OIG access to DHS information. Specifically, OIG's statement that the Cyber Security Division (CSD) "declined" to schedule a meeting with relevant personnel and did not timely provide requested documents does not fully describe CSD efforts to ensure the OIG received well-informed responses to its questions. In fact, CSD staff did meet with OIG on April 11 and April 27, 2023, and offered to meet again in June 2023 at OIG's convenience, which OIG declined. CSD staff also provided responses to written questions on September 13, 2023. While the press of commitments unfortunately affected the timing of some of these exchanges, CISA maintains that it approached this audit forthrightly and in good faith. Despite the fact that CSD provided the information to the OIG nearly six months prior to OIG's issuance of its Notice of Findings and

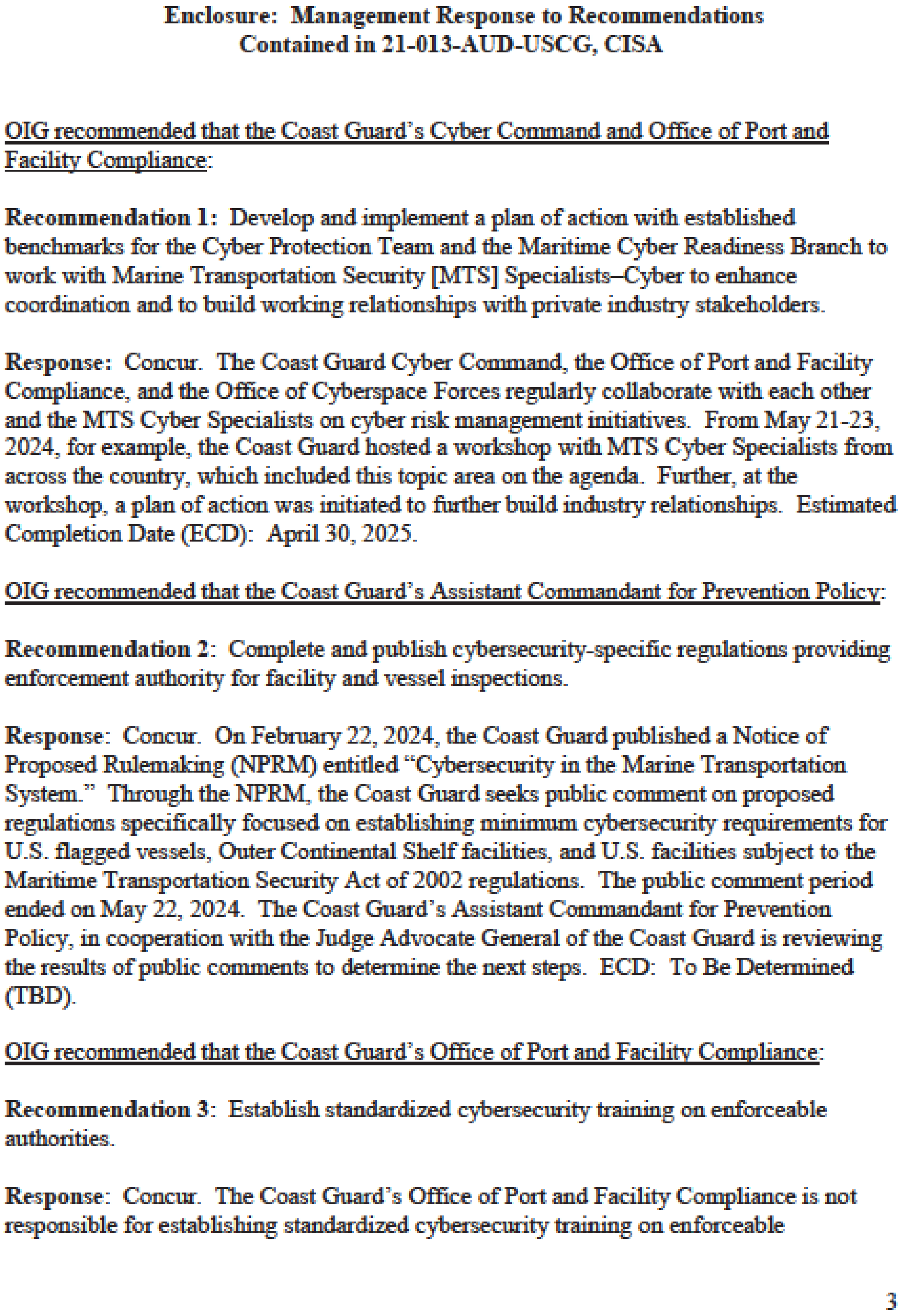


Recommendations (January 18, 2024), and about 10 months prior to the issuance of its draft report (May 3, 2024), OIG declined to consider the information.

The OIG's draft report contained four recommendations with which the Coast Guard concurs. Further, the Coast Guard notes that the report does not identify numerous actions the Service has taken to safeguard the MTS from cyber risks, and that it has several contextual and technical inaccuracies which were previously identified to the OIG under a separate cover for inclusion or correction in the final report, as appropriate. Enclosed find our detailed response to each recommendation.

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.

Enclosure



Enclosure: Management Response to Recommendations Contained in 21-013-AUD-USCG, CISA

OIG recommended that the Coast Guard's Cyber Command and Office of Port and Facility Compliance:

Recommendation 1: Develop and implement a plan of action with established benchmarks for the Cyber Protection Team and the Maritime Cyber Readiness Branch to work with Marine Transportation Security [MTS] Specialists–Cyber to enhance coordination and to build working relationships with private industry stakeholders.

Response: Concur. The Coast Guard Cyber Command, the Office of Port and Facility Compliance, and the Office of Cyberspace Forces regularly collaborate with each other and the MTS Cyber Specialists on cyber risk management initiatives. From May 21-23, 2024, for example, the Coast Guard hosted a workshop with MTS Cyber Specialists from across the country, which included this topic area on the agenda. Further, at the workshop, a plan of action was initiated to further build industry relationships. Estimated Completion Date (ECD): April 30, 2025.

OIG recommended that the Coast Guard's Assistant Commandant for Prevention Policy:

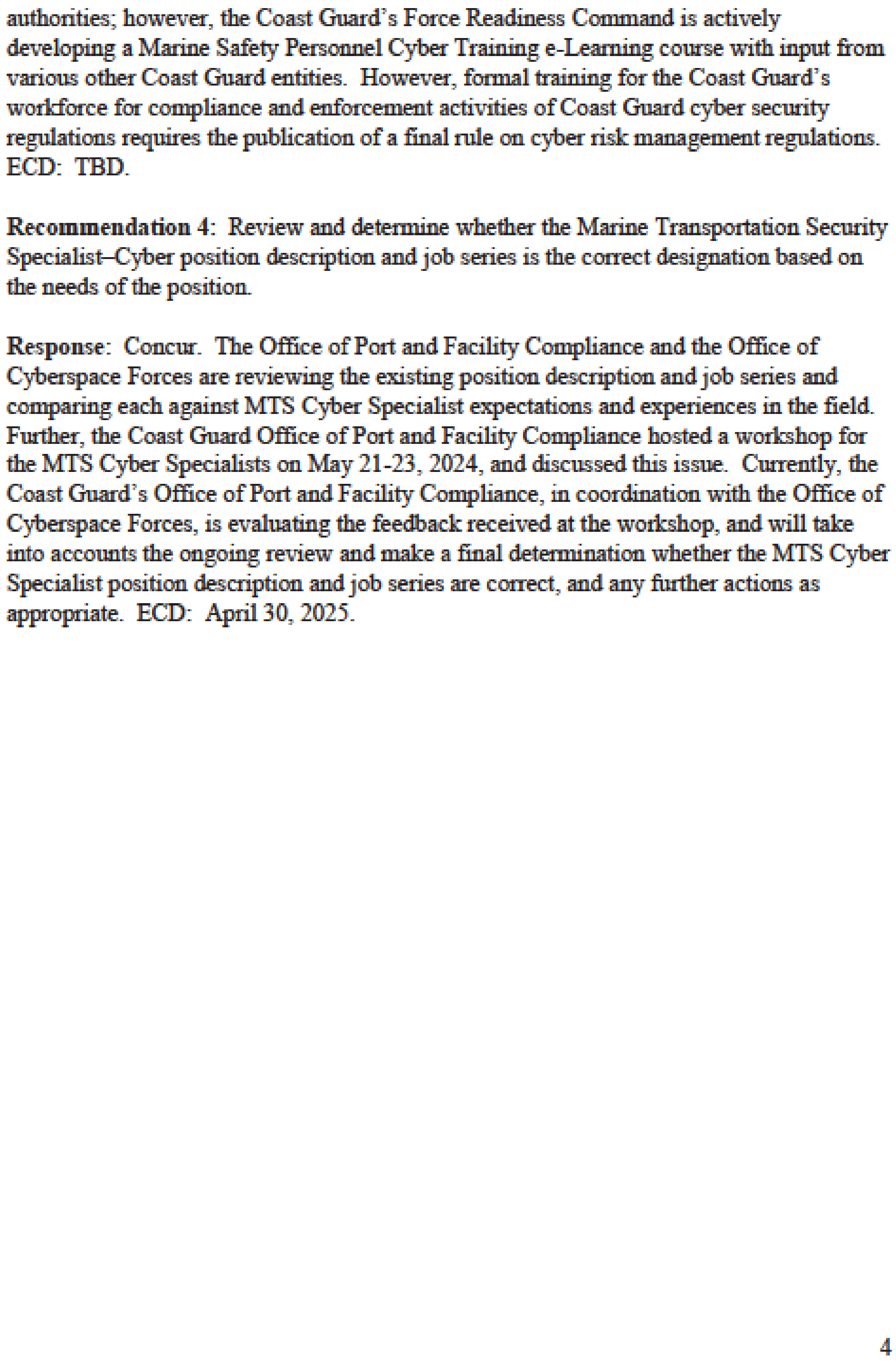
Recommendation 2: Complete and publish cybersecurity-specific regulations providing enforcement authority for facility and vessel inspections.

Response: Concur. On February 22, 2024, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) entitled "Cybersecurity in the Marine Transportation System." Through the NPRM, the Coast Guard seeks public comment on proposed regulations specifically focused on establishing minimum cybersecurity requirements for U.S. flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to the Maritime Transportation Security Act of 2002 regulations. The public comment period ended on May 22, 2024. The Coast Guard's Assistant Commandant for Prevention Policy, in cooperation with the Judge Advocate General of the Coast Guard is reviewing the results of public comments to determine the next steps. ECD: To Be Determined (TBD).

OIG recommended that the Coast Guard's Office of Port and Facility Compliance:

Recommendation 3: Establish standardized cybersecurity training on enforceable authorities.

Response: Concur. The Coast Guard's Office of Port and Facility Compliance is not responsible for establishing standardized cybersecurity training on enforceable



authorities; however, the Coast Guard's Force Readiness Command is actively developing a Marine Safety Personnel Cyber Training e-Learning course with input from various other Coast Guard entities. However, formal training for the Coast Guard's workforce for compliance and enforcement activities of Coast Guard cyber security regulations requires the publication of a final rule on cyber risk management regulations. ECD: TBD.

Recommendation 4: Review and determine whether the Marine Transportation Security Specialist–Cyber position description and job series is the correct designation based on the needs of the position.

Response: Concur. The Office of Port and Facility Compliance and the Office of Cyberspace Forces are reviewing the existing position description and job series and comparing each against MTS Cyber Specialist expectations and experiences in the field. Further, the Coast Guard Office of Port and Facility Compliance hosted a workshop for the MTS Cyber Specialists on May 21-23, 2024, and discussed this issue. Currently, the Coast Guard's Office of Port and Facility Compliance, in coordination with the Office of Cyberspace Forces, is evaluating the feedback received at the workshop, and will take into accounts the ongoing review and make a final determination whether the MTS Cyber Specialist position description and job series are correct, and any further actions as appropriate. ECD: April 30, 2025.

Appendix C:
Office of Audits Major Contributors to This Report

Craig Adelman, Director
Anna Hamlin, Audit Manager
Saajan Paul, Auditor-in-Charge
Nadine F. Ramjohn, Auditor
Jessica Garcia, Auditor
Uroosa Malik, Auditor
Jean Apedo, IT Specialist
Maria Romstedt, Communications Analyst
Lauren Bullis, Independent Referencer

Appendix D:
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commandant, United States Coast Guard
Coast Guard Liaison
Director, Cybersecurity and Infrastructure Security Agency
Cybersecurity and Infrastructure Security Agency Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305