U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

**TESTIMONY OF**
**REAR ADMIRAL JOHN W. MAUGER**
**ASSISTANT COMMANDANT FOR PREVENTION POLICY**

**ON**
**THE EVOLVING CYBERSECURITY LANDSCAPE:**
**FEDERAL PERSPECTIVES ON SECURING THE NATION'S INFRASTRUCTURE**

**BEFORE THE**
**HOUSE COMMITTEE ON TRANSPORTATION & INFRASTRUCTURE**

**2 DECEMBER 2021**

## Introduction

Good morning Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee. I am honored to be here to discuss a top priority for the U.S. Coast Guard: cybersecurity in the marine transportation system (MTS). Since the early days of the Revenue Cutter Service, we have protected our Nation's waters, harbors, and ports. While much has changed over the centuries - with our missions expanding from sea, air, and land into cyberspace - our ethos and operational doctrine remain steadfast. We employ a risk-based approach to protect the Nation from threats in the maritime environment. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our people; and the breadth of our civil, military, and law enforcement partnerships to protect the Nation, its waterways, and those who operate on them.

I recognize that protecting the MTS from cyber threats is also a top priority for Congress. The Coast Guard thanks Congress for Fiscal Year 2021 appropriations that will deliver more cyber risk management capability for the nation and build a more resilient MTS. The Coast Guard is committed to maximizing the return on this important investment and we look forward to the continued dialog with Congress on such a critical issue for our country.

## The Criticality of the Marine Transportation System

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. One of the challenges with protecting the MTS is that it can be difficult to quantify. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. But it is more than ports and waterways. It is cargo and cruise ships, passenger ferries, waterfront terminals, offshore facilities, buoys and beacons, bridges, and more. The MTS supports $5.4 trillion of economic activity each year and accounts for the employment of more than 30 million Americans. It also enables critical national security sealift capabilities, enabling U.S. Armed Forces to project and maintain power around the globe.

The maritime transportation of cargo is considered the most economical, environmentally friendly, and efficient mode of freight transport. As the economic lifeblood of the global economy and critical to U.S. national interests, the MTS connects America's consumers, producers, manufacturers, and farmers to domestic and global markets. Any significant disruption to the MTS, whether man-made or natural, has the potential to cause cascading and devastating impact to our domestic and global supply chain and, consequently, America's economy and national security.

**The Growing Cyber Risks**

Cyber attacks are a significant threat to the economic prosperity and security of the MTS, and will require a whole of nation effort to address the threat. The MTS's complex, interconnected network of information, sensors, and infrastructure continually evolves to promote the efficient transport of goods and services around the world. The information technology and operational technology networks vital to increasing the efficiency and transparency of the MTS also create complicated interdependencies, vulnerabilities, and risks.

The size, complexity, and importance of the MTS make it an attractive target. Terrorists, criminals, activists, adversary nation states and state-sponsored actors may view a significant MTS disruption as favorable to their interests. The diversity of potential malicious actors and their increasing levels of sophistication present substantial challenges to government agencies and stakeholders focused on protecting the MTS from constantly evolving cyber threats.

Recent destructive cyber activities highlight the risk posed to the vast networks and system of the MTS. Cyber attacks, such as ransomware attacks, can have a devastating impact on the operations of maritime critical infrastructure. A successful cyber attack could impose unrecoverable losses to port operations, electronically-stored information, national economic activity, and disruption to global supply chains. The increased use of automated systems in shipping, offshore platforms, and port and cargo facilities creates enormous efficiencies, but also introduces additional attack vectors for malicious cyber actors. This growing reliance on cyber-physical systems and technologies requires a comprehensive approach by all MTS stakeholders to manage cyber risks and ensure the safety and security of the MTS.

**Shared Responsibility**

The U.S. Coast Guard is the Nation's lead federal agency for safeguarding the MTS. We apply a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. Our authorities and capabilities cut across threat vectors, allowing operational commanders at the port level to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

Just like the other risks we manage, the maritime industry has a vital role in cyber risk management—Cyber risk management is a shared responsibility. In a number of forums and industry engagements, I hear the consistent message that cybersecurity does not have a one-size-fits-all solution. I agree with that assessment. However, the building blocks of sound cyber risk management practices have common threads across the maritime industry and other critical infrastructure sectors.

It starts with accountability and focus. First, companies need to identify and empower a responsible person with the authority and resources to address the cyber challenge. Then, companies need to have a plan. This includes conducting vulnerability assessments, identifying gaps, and working to close them. Third, companies need to exercise their plan, so cybersecurity is ingrained in all of the work they do. Lastly, companies need to report cyber incidents—reporting of cybersecurity incidents is absolutely critical because it enables a coordinated response, and more importantly, can help to inform other companies and critical infrastructure to take action and mitigate risk.

Information sharing is clearly an essential component of our shared responsibility, and we have heard from industry that it must happen at the "speed of cyber" to spur meaningful prevention and response activities. While we have existing information sharing networks – within the Coast Guard and across government – we must deliver specific, timely information with appropriate levels of privacy protection in order to build trust and confidence in the system. Without that trust, we will lose the massive benefit of the industry's perspectives, experiences, and trends.

## The U.S. Coast Guard's Approach

For the U.S. Coast Guard, protecting the MTS from threats is not new, and we will continue to leverage our foundational operational concepts and strong relationships to strengthen the cyber resiliency of the MTS. In August of 2021, we released a new Coast Guard Cyber Strategic Outlook that outlines our strategic direction for facing cyber threat. One of the three primary Lines of Effort is to "Protect the Marine Transportation System," and a fundamental element for this effort is applying our proven prevention and response framework.

### *Prevention*

The Prevention Concept of Operations - Standards, Compliance, and Assessment - guides all of our prevention missions including our cyber risk management activities. It begins with establishing expectations in the MTS. Regulations and standards provide a set of minimum requirements, and are critical to establishing effective and consistent governance regimes. With effective standards in place, compliance activities systematically verify that the governance regime is working. This part of the system is vital in identifying and correcting potential risks before they advance further and negatively impact the MTS. Effective assessment is paramount to continuous improvement. It provides process feedback and facilitates the identification of system failures so that corrective actions can be taken to improve standards and compliance activities.

Importantly, we are operationalizing this framework at the port-level. U.S. Coast Guard Captains of the Port are overseeing Maritime Transportation Security Act (MTSA)-regulated facilities as they incorporate cybersecurity into their mandated Facility Security Assessments and Facility Security Plans. We have provided the industry with detailed guidance on ways to meet the regulatory requirements related to computer systems and networks, including personnel training, drills and exercises, communication, vessel interfaces, security systems, access control, cargo handling, delivery of stores, and restricted area monitoring. On October 1, 2021, Coast Guard field units began reviewing these Facility Security Assessments and Facility Security Plans to validate that cybersecurity is satisfactorily addressed, and all MTSA-regulated facilities will be inspected for compliance by September 30, 2022.

The U.S. Coast Guard worked closely with the International Maritime Organization on guidelines for commercial vessels operating internationally to integrate cyber risk management into mandated safety management systems. During regular inspections, the U.S. Coast Guard is verifying that foreign vessels operating in U.S. waters are complying with these requirements.

The U.S. Coast Guard is hiring Cybersecurity Advisors at each Area, District, and Captain of the Port Zone. These new positions create a dedicated staff to build and maintain port level cyber-related relationships, facilitate information sharing across industry and government, advise Coast Guard and Unified Command decision-makers, and plan cyber-related security exercises.

Finally, Coast Guard Cyber Command's (CGCYBER) Maritime Cyber Readiness Branch is assessing technology employed in the MTS, evaluating known or potential threats, and sharing information across industry and government. Their Cyber Protection Teams (CPTs) are conducting detailed vulnerability assessments of maritime critical infrastructure when requested to help the industry identify and close gaps in their cybersecurity systems.

*Response*

Similar to our Prevention Concept of Operations, the U.S. Coast Guard has a proven, scalable response framework that can be tailored for all-hazards. This is especially important as cyber incidents can quickly transition to physical impact requiring operational commanders to immediately deploy assets to mitigate risks. Depending on the incident's size and severity, commanders will set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response. We are not approaching this alone.

By regulation, MTSA-regulated vessels and facilities are required to report Transportation Security Incidents, breaches of security, and suspicious activity without delay. We have provided additional guidance on reporting requirements specifically related to cyber incidents. These reports enable our operational commanders to rapidly notify other government agencies, evaluate associated risks, deploy resources, and unify the response.

CGCYBER is also bringing specialized operational capability to MTS cyber response. These teams will support maritime critical infrastructure owners and operators after a cyber attack and provide extensive technical expertise for post-incident investigation, response, and recovery. Their cyber skills are unprecedented for our Service.

While we are converting our strategy into action, we know our work is not done. Through all of these prevention and response activities in the field and engagements with industry, the U.S. Coast Guard will capture lessons learned, recommendations, and best practices that strengthen the maritime industry's cybersecurity posture and inform future policy, law, and regulations.

**Partnerships**

MTS cyber risk management requires a whole-of-government effort to protect America's critical infrastructure. As the Federal Maritime Security Coordinator, the U.S. Coast Guard Captain of the Port directs Area Maritime Security Committee (AMSC) activities. AMSCs are required by federal regulations and serve an essential coordinating function during normal operations and

emergency response. They are comprised of government agency and maritime industry leaders, and have adapted to the cyber threat, serving as the primary local means to jointly evaluate cyber risks, share threat information, and participate in cyber preparedness exercises.

In addition to being the federal government's lead regulator for the MTS, we are also the co-Sector Risk Management Agency (SRMA), along with the Department of Transportation for the Maritime Transportation Subsector, as outlined in Presidential Policy Directive 21. As an SRMA, we are responsible for coordinating risk management efforts, including cyber, with DHS, the Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders. We also provide, support, and facilitate technical assistance for the MTS to address vulnerabilities and develop processes and procedures to mitigate risk.

CISA is a key partner in all of our cyber risk management activities. CISA's technical expertise directly supports our ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA provides technical expertise, integrates a whole-of-government response, analyzes broader immediate and long-term impacts, and facilitates information sharing across transportation sectors. Our relationship with CISA is strong and will continue to mature.

Our enduring relationship with the Department of Defense (DoD) is also crucial to safeguarding the MTS. In many cases, DoD's ability to surge forces from domestic to allied seaports depends on the same commercial maritime infrastructure as the MTS. We must ensure our surge capability and sea lines of communication will be secure and available during times of crisis. By sharing intelligence on cyber threats, developing interoperable capabilities like Cyber Protection Teams, and using DoD's expertise to protect our own cyber networks, we enable national security sealift capabilities and jointly support our nation's ability to project power around the globe.

**Future Focus**

Recent cyber incidents, including attacks on multiple segments of maritime critical infrastructure only reinforce that cyberspace is a contested domain. Working in close collaboration with the Department of Homeland Security, CISA, and our other government partners, foreign allies, and the maritime industry, we will continue to leverage strong and established relationships across the maritime industry – at the international, national, and port levels – to build confidence and establish trust through cyber prevention and response activities.

We have secured and safeguarded the maritime environment for over 230 years. During that time we have faced many complex challenges. These trials have honed our operating concepts, bolstered our capabilities, and strengthened our resolve. We will employ these same concepts and capabilities to secure and protect our Nation and maritime critical infrastructure from malicious cyber activity and cyber attacks. In addressing cyber risks to ports and other aspects of the maritime industry, our commitment is to address those risks with the same level of professionalism, efficiency, and effectiveness that the public has come to expect. The Coast Guard will continue to adapt, as it has done over the last two centuries, to the challenges and opportunities that accompany technological advancements in our operating environment.

Thank you for the opportunity to testify today, and thank you for your continued support of the United States Coast Guard. I am pleased to answer your questions.