U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL WAYNE R. ARGUIN
ASSISTANT COMMANDANT FOR PREVENTION POLICY

AND

REAR ADMIRAL JOHN C. VANN
COMMANDER, COAST GUARD CYBER COMMAND

ON

"PORT CYBERSECURITY: THE INSIDIOUS THREAT TO U.S. MARITIME PORTS"

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
TRANSPORTATION & MARITIME SECURITY SUBCOMMITTEE

29 FEB 2024

Introduction

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. We are honored to be here today to discuss a top priority for the U.S. Coast Guard: protecting the Marine Transportation System (MTS). At all times, the U.S. Coast Guard is a military service and branch of the U.S. Armed Forces, a Federal law enforcement agency, a regulatory body, a co-Sector Risk Management Agency, a first responder, and an element of the U.S. Intelligence Community (IC). The Service is uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

Since the early days of the Revenue Cutter Service, the Service has 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. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our workforce; and the breadth of our military, law enforcement, and civil partnerships to protect the Nation, its waterways, and all who operate on them.

The Criticality of the Marine Transportation System

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. It is difficult to overstate the complexity of the MTS and its consequence to the Nation. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. However, 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 supports the employment of more than 30 million Americans.

It supports critical national security sealift capabilities, enabling U.S. Armed Forces to project power around the globe. The U.S. Coast Guard remains laser-focused on the safety and security of this system as an economic engine and strategic imperative.

Port Security – A Shared Responsibility and Layered Approach

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

The U.S. Coast Guard works across multiple levels of government and industry to assess security vulnerabilities, determine risk, and develop mitigation strategies. This layered approach—from the local to the international level—is critical due to the size and interconnectedness of the MTS.

Locally: Vessel and Facility Security

Security in U.S. ports and waterways starts with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) and its implementing regulations place specific requirements on regulated entities to conduct security assessments, analyze the results, and incorporate their findings in U.S. Coast Guard-approved security plans.

These plans set baseline requirements that regulated U.S. vessels and facilities must follow to protect the MTS, including addressing access control, computer systems and networks, restricted area monitoring, communication, security systems, cargo handling, delivery of stores, personnel training, and drills and exercises. U.S. Coast Guard inspectors verify compliance with these plans during scheduled and unannounced inspections throughout a given year. Additionally, the Coast Guard released a proposed rulemaking leveraging the applicability of the MTSA regulations to further raise cybersecurity standards for vessels, facilities, and Outer Continental Shelf facilities.
For foreign-flagged vessels, the approach to security is very similar to that of MTSA-regulated domestic vessels. Per the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code, each foreign vessel must conduct a Ship Security Assessment that identifies: key shipboard operations that are important to protect; possible threats to key shipboard operations and likelihood of their occurrence; existing security measures and procedures; and potential weaknesses, including human factors, in security policies and procedures. This assessment then leads to the development of a Ship Security Plan, which must be approved by the ship's Flag Administration prior to a vessel being certificated as compliant with the ISPS Code. This certification is verified by the U.S. Coast Guard during regular compliance examinations when the vessel arrives in a U.S. port.

Regionally: Area Maritime Security Coordination

At the regional level, Area Maritime Security Committees (AMSC) are required by MTSA and its implementing regulations to serve an essential coordinating function during normal operations and emergency response. Comprised of government and maritime industry leaders, an AMSC serves as the primary regional body to jointly share threat information, evaluate risks, and coordinate risk

mitigation activities. As the Federal Maritime Security Coordinator (FMSC), U.S. Coast Guard Captains of the Port (COTP) direct their regional AMSC's activities.

AMSC input is vital to the development and continuous review of the Area Maritime Security (AMS) Assessment and Area Maritime Security Plan (AMSP). The AMS Assessment must include the critical MTS infrastructure and operations in the port; a threat assessment that identifies and evaluates each potential threat; consequence and vulnerability assessments; and a determination of the required security measures for the three Maritime Security levels.

These AMS assessments then lead to the collaborative development of AMSPs to ensure government and industry security measures are coordinated to deter, detect, disrupt, respond to, and recover from a threatened or actual Transportation Security Incident.

The U.S. Coast Guard COTP and AMSCs are also required by regulations to conduct or participate in an exercise once each calendar year to collectively assess the effectiveness of the AMSP in today's dynamic operating environment.

Nationally: Interagency Collaboration

The U.S. Coast Guard functions on behalf of the Department of Homeland Security as the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector along with the Department of Transportation. As an SRMA, the U.S. Coast Guard is responsible for coordinating risk management efforts with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner whose technical expertise supports the U.S. Coast Guard's ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA 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.

As an element of the IC, the U.S. Coast Guard possesses unique authorities, and has opportunity and capability to collect, analyze, and share information from domestic, international, and non-government stakeholders which operate throughout the MTS. This ability allows the U.S. Coast Guard to gain a collective understanding of threats and vulnerabilities facing the maritime domain, including physical security and cybersecurity.

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. The relationship between the U.S. Coast Guard and DoD ensures the Nation's surge capability and lines of communication will be secure and available during times of crisis. By sharing threat intelligence, developing interoperable capabilities, and leveraging DoD's expertise, the U.S. Coast Guard enables national security sealift capabilities and jointly supports our Nation's ability to project power around the globe.

The U.S. Coast Guard also supports the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject matter expertise in maritime security. The PSGP is designed to support and protect critical port infrastructure from terrorism. FEMA is responsible for the administration and management of the program, which has distributed more than $3.8 billion to MTS stakeholders since the program's inception in 2002.

Internationally: International Port Security Program

U.S. Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, including through the U.S. Coast Guard International Port Security (IPS) program, the U.S. Coast Guard conducts in-country foreign port assessments to assess compliance with the ISPS Code and the effectiveness of security and anti-terrorism measures in foreign ports. In addition, the IPS program conducts capacity building engagements to assist foreign ports in implementing effective anti-terrorism measures, where possible.

If the U.S. Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, the Service may impose additional security measures called Conditions of Entry (COE) on vessels arriving to the United States from those ports and may deny entry into the United States to any vessel that does not meet such conditions. Verification that a vessel took additional security measures when it was in foreign ports that lacked effective anti-terrorism measures may be required before the vessel is permitted to enter the United States.

The Growing Cyber Risks

Cyber-attacks can pose a significant threat to the economic prosperity and security of the MTS for which whole-of-government efforts are required. 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 cyber target. Terrorists, criminals, activists, adversary nation states and state-sponsored actors may view a significant MTS disruption as favorable to their interests. 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.

Cyber vulnerabilities pose a risk to the vast networks and system of the MTS. Cyber-attacks, such as ransomware attacks, can have devastating impacts on the operations of maritime critical infrastructure. A successful cyber-attack could disrupt global supply chains and impose unrecoverable losses to port operations, electronically stored information, and national economic activity. 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. 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.

Last week, the President signed an Executive Order which further enables our port security efforts by explicitly addressing cyber threats. It empowers the Coast Guard to prescribe conditions and restrictions for the safety of waterfront facilities and vessels in port and includes reporting requirements for actual or threatened cyber incidents. With this authority, the Coast Guard issued a directive requiring specific cyber risk management actions for all owners or operators of cranes manufactured by companies from the People's Republic of China. Our Captains of the Port around the country are working directly with crane owners and operators to ensure compliance and further mitigate the threats posed by these cranes.

The U.S. Coast Guard's Approach

In support of the whole-of-government effort, the U.S. Coast Guard applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces.

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions, including port security. It begins with establishing expectations in the MTS. Regulations and standards provide a set of baseline requirements and are critical to establishing effective and consistent governance regimes. With effective standards in place, vessel and facility inspectors verify systematic compliance activities to ensure 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.

In addition to vessel and facility inspectors, the U.S. Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These dedicated staffs build and maintain port level security-related relationships, facilitate information sharing across industry and government, advise U.S. Coast Guard and Unified Command decision-makers, and plan security exercises.

Response

The U.S. Coast Guard has a proven, scalable response framework that can be tailored for all hazards. Whether a cyber or physical security incident, our operational commanders immediately assess the risk, consider their authorities, and deploy assets or issue operational controls to mitigate risks. Depending on the incident's size and severity, commanders set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response.

For complex responses, the U.S. Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of needs and domains. These teams include specially trained law enforcement teams that can bolster physical security, and pollution response teams that can address significant oil spills or hazardous material releases.

In addition, the U.S. Coast Guard has established three Cyber Protection Teams as commands under U.S. Coast Guard Cyber Command. These units assist Captains of the Port with measuring cyber risk and are poised to deploy in support of time-critical or nationally significant cyber activities.

Future Focus

Given today's dynamic operational environment, the U.S. Coast Guard is ever vigilant and on watch to identify emerging threats, evaluate associated risk, and apply authorities and capabilities to protect the MTS. While the U.S. Coast Guard has a proven prevention and response framework that has been honed over many years, the Service is dedicated to continually assessing and enhancing the way we execute both enduring and emerging missions. The U.S. Coast Guard's commitment is to continue to lead with the same level of professionalism, efficiency, and effectiveness that the public has come to expect.

Thank you for the opportunity to testify today and thank you for your continued support of the U.S. Coast Guard. We look forward to answering your questions.