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

ON
EVALUATING HIGH-RISK SECURITY VULNERABILITIES
AT OUR NATION'S PORTS

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

10 MAY 2023

Introduction

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. I am 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 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 a member of the U.S. Intelligence Community. We are uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

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 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. The MTS' complexity and consequence to the Nation cannot be overstated. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. 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 protects critical national security sealift capabilities, enabling U.S. Armed Forces to project and maintain power around the globe. We remain laser-focused on the safety and security of the MTS as an economic engine and strategic imperative, and we continue to serve as the Sentinels envisioned at our founding.

Evaluating Vulnerabilities – A Shared Responsibility

Safeguarding the MTS requires diligent assessment and remediation of vulnerabilities. The Coast Guard works across multiple levels of industry and government 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, diversity, and interconnectedness of the MTS.

Locally: Vessel and Facility Security Assessments

Security assessments in U.S. ports and waterways start with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) regulations in 33 CFR 104, 105, and 106 place specific requirements on regulated entities to conduct personalized security assessments, analyze the results, and prepare a security assessment report that is included in their security plans.

A completed security assessment report must be submitted to the Coast Guard as part of the plan approval process and include a description of how the on-scene survey was conducted, key facility operations to protect, each vulnerability found, security measures to address each vulnerability, and potential gaps in security policies and procedures.

In February 2020, the Coast Guard provided further guidance to the regulated industry on incorporating computer systems and networks into their required assessments and plans. During inspections to verify compliance, the industry sought more specific guidance on ways to integrate cyber into their existing security regime. The Coast Guard partnered with the Homeland Security Systems Engineering and Development Institute, a federally funded research and development center operated by the MITRE Corporation, and the National Maritime Security Advisory Committee (a Federal Advisory Committee) to develop the Maritime Cybersecurity Assessment and Annex Guide. This guide was released in January 2023 and provides a clear process for identifying and describing cybersecurity vulnerabilities, then addressing those vulnerabilities in mandated security plans.

For foreign ships operating in U.S. waters, the process is very similar to MTSA-regulated vessels and facilities. Per the International Ship and Port Facility Security Code (ISPS Code), each ship must conduct a Ship Security Assessment that identifies key shipboard operations to protect; threats to key shipboard operations; 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, and is verified by the Coast Guard during regular compliance examinations in U.S. ports.

Regionally: Area Maritime Security Assessments and Plans

At the regional level, Area Maritime Security Committees (AMSC) 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 serve as the primary regional body to jointly share threat information, evaluate risks, and coordinate risk mitigation activities. As the Federal Maritime Security Coordinator (FMSC), Coast Guard Captains of the Port (COTP) around the country direct their regional AMSC's activities.

The AMSC's 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 (TSI).

The COTP/FMSC and the AMSC ensure that a formal AMS Assessment for their entire Area of Responsibility (AOR) is conducted at least every five years. The AMS Assessment must also be evaluated at least annually to ensure its adequacy, accuracy, and consistency.

Nationally: Interagency Coordination and Assessment

As outlined in Presidential Policy Directive 21, along with the Department of Transportation, the Coast Guard is the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector. As a SRMA, the Coast Guard is responsible for coordinating risk management efforts with the Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner in all our risk management activities. CISA's technical expertise directly supports the 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. The relationship with CISA is strong and will continue to mature.

As a member of the U.S. Intelligence Community, the Coast Guard provides unique authorities, opportunities, and capabilities to collect, fuse, analyze, and share information and intelligence across domestic and international government and non-government stakeholders throughout the MTS. The Coast Guard's intelligence authorities allow for a collective understanding of factors and entities affecting the maritime domain, including physical security and cybersecurity. Threats, such as ransomware attacks, continue to mature in effectiveness and prevalence, requiring the Intelligence Community to align resources and integrate efforts that protect the safety and security of the MTS.

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

The Coast Guard serves as a partner to the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject matter expertise in maritime security. FEMA is responsible for the administration and management of the program, which includes designing and operating the administrative mechanisms and managing the distribution

and tracking of funds. The PSGP is designed to support AMSPs and facility security plans (FSPs) to protect critical port infrastructure from terrorism. All U.S. ports are eligible for PSGP funding. PSGP funds are intended to offset the costs for maritime security risk mitigation projects borne by maritime partners. To date (FY 2002 – FY 2022), the PSGP distributed over $3.73 billion to port stakeholders to make security improvements, including assisting facilities with capital investments for MTSA compliance.

Internationally: International Port Security Program

Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, and through the Coast Guard International Port Security (IPS) program, the Coast Guard conducts in-country foreign port assessments and applies the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to assess the effectiveness of security and anti-terrorism measures in foreign ports.

If the Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, we may impose Conditions of Entry (COE) that define additional security measures that vessels arriving to the United States from those ports must implement. COE may result in security verifications of vessels before they enter U.S. ports to verify that additional security measures were taken in foreign ports. The IPS program also conducts capacity building engagements to assist countries in implementing effective anti-terrorism measures.

The U.S. Coast Guard's Approach

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

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions. 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, 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, the Coast Guard operationalizes this framework at the port level. Coast Guard COTPs oversee MTSA-regulated vessels and facilities through their mandated Vessel or Facility Security Assessments and Plans. These plans set baseline activities to protect the MTS through personnel training, drills and exercises, communication, vessel interfaces, security systems, access control, cargo handling, delivery of stores, and restricted area monitoring.

The Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These new positions create a dedicated staff to build and maintain port level security-related relationships, facilitate information sharing across industry and government, advise Coast Guard and Unified Command decision-makers, and plan security exercises.

Response

Similar to the Prevention Concept of Operations, the 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 producing 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. The Service is not approaching this alone.

By regulation, MTSA-regulated vessels and facilities are required to report TSIs, breaches of security, and suspicious activity without delay. These reports enable operational commanders to rapidly notify other government agencies, evaluate associated risks, deploy resources, and unify the response.

For complex responses, the Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of prevention and response needs. These teams include specially trained law enforcement teams that can bolster physical security, pollution response teams for significant oil spills or hazardous material releases, and Cyber Protection Teams that can help local responders navigate the highly technical aspects of cyber incident assessment and response.

Through both prevention and response activities in the field, and engagements with industry, the Coast Guard captures lessons learned, recommendations, and best practices that strengthen the maritime industry's security posture and inform future policy, law, and regulations.

Future Focus

Working in close collaboration with CISA and other government partners, foreign allies, and industry, the Coast Guard will continue to leverage strong and established relationships across the maritime industry – at all levels – to assess and address security vulnerabilities.

The Coast Guard has secured and safeguarded the maritime environment for over 230 years and, during that time, has faced many complex challenges. We have honed our operating concepts, bolstered our capabilities, and strengthened our resolve. These same concepts and capabilities will secure and protect the Nation and maritime critical infrastructure from malicious activity in all domains. In addressing risks to ports and other components of the MTS, the Coast Guard's commitment is to address those risks 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 United States Coast Guard. I am pleased to answer your questions.