U.S. Department of Homeland Security

United States Coast Guard

The Evolution of Cyber Risk & Security in the Maritime Environment

Association of Terminal Operators, Stevedoring, and Shipping Companies of Micronesia (ATOSSCOM)

December 2022

Discussion Topics

- Marine Transportation System (MTS) Criticality
- Cyber Risk to the MTS
- Coast Guard Authorities
- Coast Guard Compliance Activities
- Reportable Cyber Incident Types & Cyber Incident Reporting
- Coast Guard Forces Micronesia – Sector Guam MTS Cyber Initiatives
- MTS Cyber Points of Contact

Marine Transportation System (MTS) Criticality

- The Marine Transportation System (MTS) is vital to national security and economic prosperity.
- 90% of world trade is conducted via the network of ports, vessels, and waterways which comprise the MTS.
- D14's AOR is extremely MTS dependent. Public health, safety, and well-being are inextricably linked to maritime enabled flow of goods and services.
- Any significant MTS disruption (cyber or otherwise) will have cascading and detrimental impacts across the region.

Cyber Risk to the MTS

- Cyber-attacks are a significant risk to the MTS, and will require an organized approach to detect, respond and recover.

- Notable cyber-attacks with a maritime nexus in recent years are:

  - MAERSK NotPetya ransomware attack costing over $300 million
  - South African ports and rails ransomware forcing declaration of force majeure
  - Colonial Pipeline ransomware attack crippling oil supply across the East Coast
  - External facing webserver compromise at District 8 based maritime facility

Coast Guard Authorities

- Presidential Policy Directive 21 designates the Coast Guard as the lead Sector Risk Management Agency (SRMA) for the Maritime Transportation Sector.

- SRMAs provide sector level feedback to DHS and enable assessment of national and cross-sector critical infrastructure protection and resilience programs.

- In short, SRMAs are tasked with building cyber-resilience and readiness across their assigned critical infrastructure sector.

Coast Guard Authorities

- Coast Guard has broad authority under Maritime Transportation Security Act (MTSA) to require physical and cyber security planning for facilities and vessels.
- Port and Waterways Safety Act requires hazardous condition reporting for all U.S. vessels in commercial service and all foreign vessels.
- 33 CFR 104, 105, 106 requires regulated facilities and vessels to address physical and cyber vulnerabilities within security assessments and plans.
- The International Maritime Organization also requires vessels subject to the International Safety Management Code to integrate cyber risk management within their Safety Management Systems.

Coast Guard Compliance Activities

- Coast Guard Prevention personnel are currently validating the integration of cyber into MTSA regulated vessel and facility security plans and safety management systems.

- The Coast Guard is also verifying compliance with International Maritime Organization requirements aboard applicable vessels.

- MTS Cyber Specialists at Coast Guard Districts and Sectors are working in concert with Port Security Specialists and the maritime industry to build cyber resilience.

Reportable Cyber Incident Types

- Transportation Security Incident (TSI): A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption of a particular area

- Breach of Security: A security incident not resulting in a TSI but in which security measures have been circumvented.

- Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

Cyber Incident Reporting

- 33 CFR 101.305 requires MTSA-regulated vessels and facilities to report TSIs, Breaches of Security, and Suspicious Activity to the Coast Guard and NRC without delay.

- CG-5P Policy Letter 08-16 provides additional guidance on these reporting requirements including specific examples of cyber incidents that must be reported e.g. ***intrusion or cyber compromise of telecom and computer networks linked to the MTS and vessel or facility security plan functions or safe operations.***

Cyber Incident Reporting

- Transportation Security Incidents must be reported to the local Captain of the Port without delay, with a follow-on notification to the National Response Center.

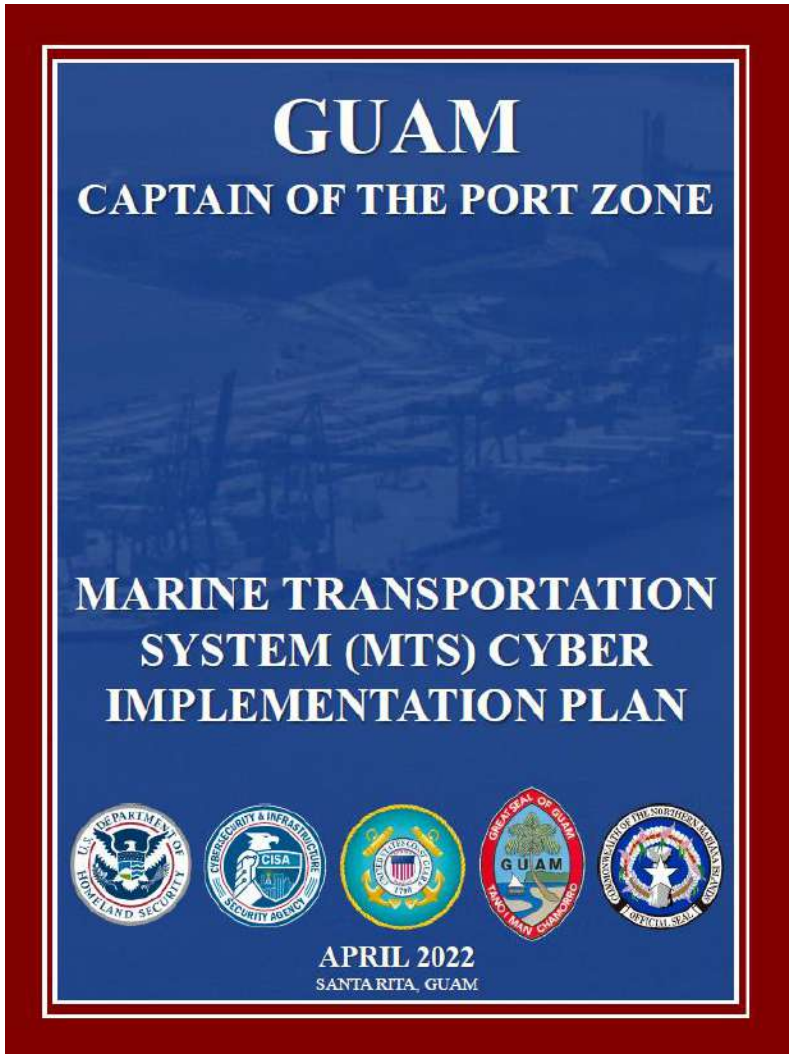
- Breaches of Security and Suspicious Activity must be reported to the National Response Center without delay.

CG Forces Micronesia – Sector Guam MTS Cyber Initiatives

- Joint outreach to port community with D14 MTS Cyber Specialist, Sector Interim MTS Cyber Specialist & GovGuam Office of Technology
- Solicitation/Hiring/On-Boarding of Sector MTS Cyber Specialist
- Re-Establishment of Area Maritime Security Committee (AMSC) Cyber Subcommittee
- Mandatory development of Cyber annex to Area Maritime Security Plan (Guam & CNMI) in 2023/2024

CG Forces Micronesia – Sector Guam MTS Cyber Initiatives

- Release of Guam Captain of the Port Zone Marine Transportation System Cyber Implementation Plan
- Promulgated to Guam and CNMI AMSC membership April 2022
- Electronic copies can be requested by contacting joshua.n.blocker@uscg.mil



U.S. Department of Homeland Security

United States Coast Guard

CG Forces Micronesia – Sector Guam MTS Cyber Initiatives

- Prevention Department (Facilities) in review of regulated facilities' Facility Security Plans – Cyber Annexes
- Integration of cyber incidents into Area Maritime Security Training & Exercise Program (AMSTEP)
- Coast Guard Headquarters Office of Cyber Forces (CG-791) & Office of Port & Facility Compliance (CG-FAC) outreach and training
- Partner agency capacity building & technical assistance

CG Cyber Protection Team

- Cyber Protection Team Overview
  - Based in Washington, D.C.
  - Support local Captains of the Port in cyber missions
  - Two CPTs (39 Members Each)
    - Six Deployable Elements
    - Intelligence and mission support
  - Teams comprised of Active Duty Coast Guard Officers and Enlisted & Government Civilians with:
    - Wide range of industry standard training and certifications
    - 8-12+ months of Department of Defense cyber training
    - Previous positions at CISA, US CYBER, and NSA

CG Cyber Protection Team

- Cyber Protection Team Roles in the MTS
  - Assess
    - Identify vulnerabilities and weaknesses in Critical Infrastructure before exploitation causes a major incident
    - Guidance and recommendations to secure and protect MTS networks
    - Provide situational awareness to Coast Guard leadership on cybersecurity risk posture of U.S. MTS Infrastructure
  - Hunt
    - Identify adversary on MTS networks
    - Analyze malicious tactics, techniques and procedures
  - Incident Response
    - Advise on remediation steps and best practices
    - Forensic artifact analysis
    - Assistance with integration of FBI,CISA & other agencies.

CG Cyber Protection Team

- Cyber Protection Team Engagements in the AOR
  - Completed CPT Missions
    - Guam Waterworks Authority
  - Pending CPT Missions (RTAs/Scheduling/Deployment Logistics)
    - Guam Power Authority
    - Cabras Marine
    - Port Authority of Guam
      - In conjunction with DHS CISA RRAP
    - Commonwealth Port Authority
      - In conjunction with DHS CISA RRAP

MTS Cyber Points of Contact

- **Prevention Department (Facilities)**
  - LT Gaylord Amores
    - Gaylord.C.Amores@uscg.mil
- **Interim MTS Cyber Specialist**
  - Mr. Joshua Blocker, Port Security Specialist (AMS)
    - Joshua.N.Blocker@uscg.mil
- **National Response Center**
  - MTS Cyber Incident Reporting
    - 800.424.8802
- **CG Forces Micronesia – Sector Guam Command Center**
  - MTS Cyber Incident Reporting
    - 671.355.4824
    - rccguam@uscg.mil


Questions