Serenity

Maritime & Port Security
Information Sharing & Analysis Organization

Identify – Protect – Detect – Respond - Recover
Ensuring the Cyber Resilience of our Nation’s Critical Maritime Sector

Critical infrastructure represents the assets, systems and networks (physical or virtual), so vital that incapacitation or destruction would have debilitating and catastrophic cascading impacts within and across sectors. Cyber threats and attacks continue to increase in frequency, severity, and sophistication.

The Nation’s security and prosperity depends upon a safe, secure and resilient Maritime Critical Infrastructure moving people, manufactured and agricultural goods, healthcare products, bulk energy, and retail products throughout the Maritime ecosystem handling $1.3 trillion in annual cargo…all dependent upon cyber resilience.

Cyber technology and computer systems are essential to the operation and efficient functioning of Maritime operations. Cyber attacks and vulnerability exploits can have potentially catastrophic cascading impacts to GPS-based and e-navigation (ECDIS or AIS) systems, pumps, machinery, vessel propulsion and navigation systems; monitoring and control of safety and environmental systems; operation of security cameras and gates; tracking and controlling container cargo movements; and enabling vessel operators to control ballast water and ship stability systems with precision and safety.

Moving from a reactive to a proactive stance requires addressing cybersecurity from a risk-based approach, assessing maritime-specific cyber risks and interdependencies, expanding beyond physical aspects of security and safety, and greater information exchange and sharing solutions to enable and ensure systems protection, accessibility, reliability and resiliency.

Maritime Cyber Resilience protection efforts require:

- Cooperation, coordination and a sustainable collaborative infrastructure connecting public/private sector and cross-sector stakeholders …breaking down existing silos and boundaries.
- Incorporating the real-time availability of “actionable” threat intelligence, analysis, coordinated response, best practice adoption, and role-based workforce education.

To advance Maritime Cyber Resilience, a strategic collaborative public/private partnership has established the:

The Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO)

The MPS-ISAO provides the Maritime Critical Infrastructure with a trusted and secure public/private collaborative infrastructure:

- **The National Maritime & Port Security Cyber Threat Intelligence Platform** –
  - Automated Threat “Actionable Intelligence” - Bi-directional information sharing of Threat Indicators, Incidents, Observables, Threat Actors, TTPs, Exploit Targets, Campaigns – Supported by Daily Alerts & Advisories
  - Automated Threat Sighting Detection - Managed platform and network appliance to automate detection of community-shared threats and to support participation in the sharing community.

- **The National Maritime & Port Security Cyber Response Communications and Control Platform** – Unified real-time communications management (secure response planning, exercising, and incident response) via landline, cell, text, email, secure voice, secure video, mobile app two-way radio communications

- **The Global Incident Analysis and Analytics Repository** – Advancing Cyber Risk Management - Identifying top risks, tactics/techniques/ procedures (TTPs), effective controls, sector differentiation, forecasting, trending, and modeling.

- **Global Cyber Range** – Cyber Risk Assessments (Certification/Accreditation), cyber resilience independent testing, modeling and simulation, cybersecurity education, customizable virtual range to exercise skills, and resources to support development of role-based education.
The Maritime Critical Infrastructure faces tremendous cybersecurity risks requiring Ports, Port Terminals and public/private Maritime stakeholders to dedicate more resources in support of:

- **Defending Cyberspace**
  Managing Risk, Integrating Cybersecurity into System Planning & Acquisition, Optimizing Intelligence-Driven Cyber Defense, Increasing Operational Resilience, Incorporating Cybersecurity Enterprise-wide

- **Enabling Operations**
  Recognizing Cyberspace as an Operational Domain, Integrating Cyber Resilience into Mission Planning and Execution, Increasing Awareness/Capability, Intelligence to Support Cyber Operations, Cyber Support to Operations

- **Protecting Infrastructure**
  Promoting Cyber Risk Awareness and Management, Improving Risk Assessment Tools, Methodologies, and Real-Time Information Sharing, Reducing Vulnerabilities, Incorporating Cybersecurity Role-Based Training

Operationalizing cyber resilience is dependent upon opportunities to participate and leverage investments in developing Maritime-specific cyber operational guidance, and benefit from collaborative partnerships to build knowledge, resource capacity, and to provide sustainable training to enable a well-trained cyber workforce.

**MARITIME & PORT SECURITY CYBER RESILIENCE ACTION PLAN – OPERATIONAL GUIDANCE**

The Maritime and Port Security ISAO (MPS-ISAO) is advancing Maritime Cyber Resilience by:

- Strengthening resilience by strategically focusing on people, process and technology
- Aligning with the Business Mission providing a common lexicon, and enabling organizations to easily adopt and adapt guidance into existing policies, processes and procedures.
- Leveraging the U.S. Coast Guard Cyber Strategy (June 2015), the NIST Framework for Improving Critical Infrastructure Cybersecurity, the Department of Defense Service Management Framework, IT Service Management (ITSM), additional best practices, lessons learned, and Maritime security and compliance requirements
- Supporting adoption and adaption with tools, templates, resources, technologies, and role-based cyber resilience workforce education (foundational and practitioner)

*To engage as a Leading Member of the MPS-ISAO, contact...*

**The Maritime & Port Security ISAO**
Global Situational Awareness Center (GSAC)
NASA/Kennedy Space Center, FL 32899
Direct: 904-476-7858
info@mpsisao.org