Maritime Transportation System ISAC

Helping Build the Maritime Cybersecurity Community

Statistics for 2020 are alarming – it takes half a year to detect a data breach; 91% of attacks are launched with a phishing email; 1 business falls victim to a ransomware attack every 14 seconds.[1]

The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) was formed as a 501(c)(6) nonprofit in February 2020 by a group of U.S.-based maritime critical infrastructure stakeholders to promote cybersecurity information sharing throughout the community.

The Department of Homeland Security recognizes the Maritime Transportation System as one of the seven key subsectors within the Transportation Systems Sector.[2] This recognition, compounded by the fact that cargo activities at U.S. seaports account for 26 percent of the U.S. economy equaling $5.4 trillion in total economic activity with international freight transported to and from the U.S. with vessels moving 41.9 percent of the value and 70.7 percent of the weight of U.S. international trade in 2018, make the MTS worthy of cybersecurity protection.[3] [4] For over 20 years, sector-specific ISACs have been formed by owners and operators to share information. [5]

NIST Cybersecurity Framework: Identify – Protect – Detect – Respond – Recover

By working together as a community to identify, protect against, and detect threats targeting MTS networks, systems, and people, we can improve resilience against motivated cyber adversaries.

Actionable cybersecurity intelligence collated from trusted MTS private and public sector partners - and analyzed and enriched by the MTS-ISAC - could provide the early warning needed to protect your organization from incidents.

By correlating cybersecurity information and trending over time, the MTS can develop proactive cyber intelligence.

NIST 800-150: Guide to Cyber Threat Information Sharing

NIST encourages sharing of cyber threat information among organizations, both in acquiring threat information from other organizations and in providing internally generated threat information to other organizations. Threat information exchanged within communities organized around specific industries or sectors can be particularly beneficial because the member organizations often face threat actors that target the same types of systems and information. Cyber defense is most effective when organizations work together to deter and defend against well-organized, capable threat actors. Such collaboration helps to reduce risk and improve the organization's security posture. [6]

The recently released Cybersecurity Maturity Model Certification (CMMC) Version 1.0 includes a Situational Awareness (SA) category which assigns a Level 3 practice to C037 "Implement threat monitoring - receive and responding to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders."[7] Participation in the MTS-ISAC may be useful if your organization requires CMMC in support of defense contracts.

Furthermore, FEMA's 2020 Port Security Grant Program (PSGP) includes "Enhancing Cybersecurity" as a National Priority and identifies "Intelligence and Information Sharing" as a Core Capability.[8] MTS-ISAC Service is a PSGP fundable item and helps create a more resilient critical infrastructure sector.

[1] https://techjury.net/stats-about/cyber-security/#gref

[2] https://www.cisa.gov/transportation-systems-sector

[3] https://www.aapa-ports.org/advocating/content.aspx?ItemNumber=21150

[4] Port Performance Freight Statistics in 2018: Annual Report to Congress 2019 - https://rosap.ntl.bts.gov/view/dot/43525

[5] https://www.nationalisacs.org/about-isacs

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[7] https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

[8] https://www.fema.gov/media-library-data/1581615217999-123068487178bb6d65ae684a676ae46a/FY_2020_PSGP_NOFO_FINAL_508AB.pdf

To learn more, or for information about the MTS-ISAC's Services and pricing, email info@mtsisac.org.

Maritime Transportation System ISAC

Helping Build the Maritime Cybersecurity Community

MTS-ISAC Information Sharing Service

> *The MTS-ISAC recognizes that maritime critical infrastructure owners and operators work together - as a community - during times of emergency response (natural disasters and physical threats). Applying this same community-based approach to cybersecurity will help improve sector resiliency. Together, we can mitigate vulnerabilities being targeted across the maritime sector by cyber threat actors.*

The MTS-ISAC offers an Information Sharing Service for maritime critical infrastructure stakeholders. Three subscription levels are available. Each subscription level offers access to:
- Cyber threat intelligence, alerts, warnings, and vulnerability information cultivated from maritime stakeholders and public and private sector shares
- Open source intelligence
- Maritime cybersecurity news, event information, exercise and training opportunities
- Discounts on cybersecurity products and services from a growing list MTS-ISAC Partners

MTS-ISAC Service Subscription Levels

Organization	• Ideal for organizations wanting to connect with peer maritime stakeholders. • Receive actionable cyber threat intelligence and vulnerability information relevant to the MTS. • Training opportunities and best practices to improve the organization's cybersecurity resilience.
Community	• Up to 15 organizations, so ideal for working collaboratively with tenants, partners, and suppliers on cybersecurity concerns impacting a specific community. • Opportunity to receive and respond to more tailored cyber threat intelligence. • Exercise incident response plans, address vulnerabilities, and implement best practices across the community to ensure continuity of business operations.
Enterprise	• For States or MTS Associations wanting to bring cybersecurity resiliency to maritime organizations within their area of responsibility (AOR). • Opportunity for maritime organizations to operationalize critical cyber threat intelligence. • Advance cybersecurity awareness and resiliency across the AOR.

MTS-ISAC Cybersecurity Support Options

The MTS-ISAC offers several cybersecurity support options for an additional cost. The following list is subject to change as additional capabilities and partners come online.

- Cybersecurity Exercises
- Cybersecurity Training & eLearning
- Cybersecurity Policy Assessments
- Network Monitoring and Managed Security Services
- Paid Intelligence Feeds
- Cybersecurity Risk Assessments
- Penetration Testing
- Threat Hunting
- Grant Writing Support

To learn more, or for information about the MTS-ISAC's Services and pricing, email info@mtsisac.org.