

# Where port security meets cyber security

4 August 2020 • 14:00-14:45 BST

## Presentation & sponsor documents:

Page 2: Scott Dickerson, Maritime Transportation System ISAC

Page 9: Dr Kimberly Tam, University of Plymouth

Page 14: Paul Ferrillo, McDermott, Will & Emery

Page 29: MTS ISAC company information

Part of  
**Maritime  
Cyber Security  
Webinar Week**

4-6 August 2020

In association with



MARITIME  
**OPTIMISATION**  
& COMMUNICATIONS

riviera )))

# Maritime Transportation System Information Sharing & Analysis Center

## Where Port Security Meets Cyber Security

August 4, 2020



*Scott Dickerson*

*Executive Director*

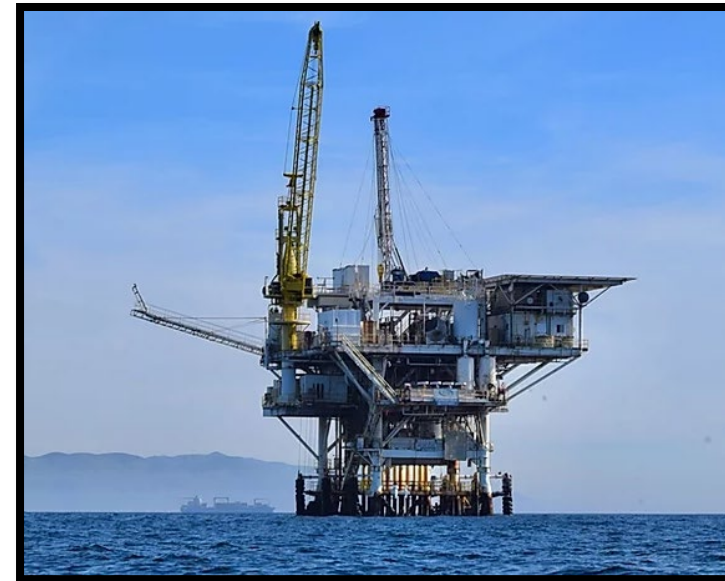
*C/CISO, CISSP, PMP, CNFA, C/EH, PCIP, TOGAF 9.1 Cert*

*M.S. Cybersecurity, Master of International Policy & Practice, M.B.A.*

# What is the MTS-ISAC?



- The MTS-ISAC is the **ONLY** information sharing organization formed and driven by **maritime port authorities and private sector owners and operators** based on their information sharing needs
- Unparalleled **relevant, actionable** and **contextualized threat information** for the maritime sector
- The MTS-ISAC is a member of the **National Council of ISACs**, which enables bi-directional information sharing with 23 ISACs and their sector specific agencies and DHS

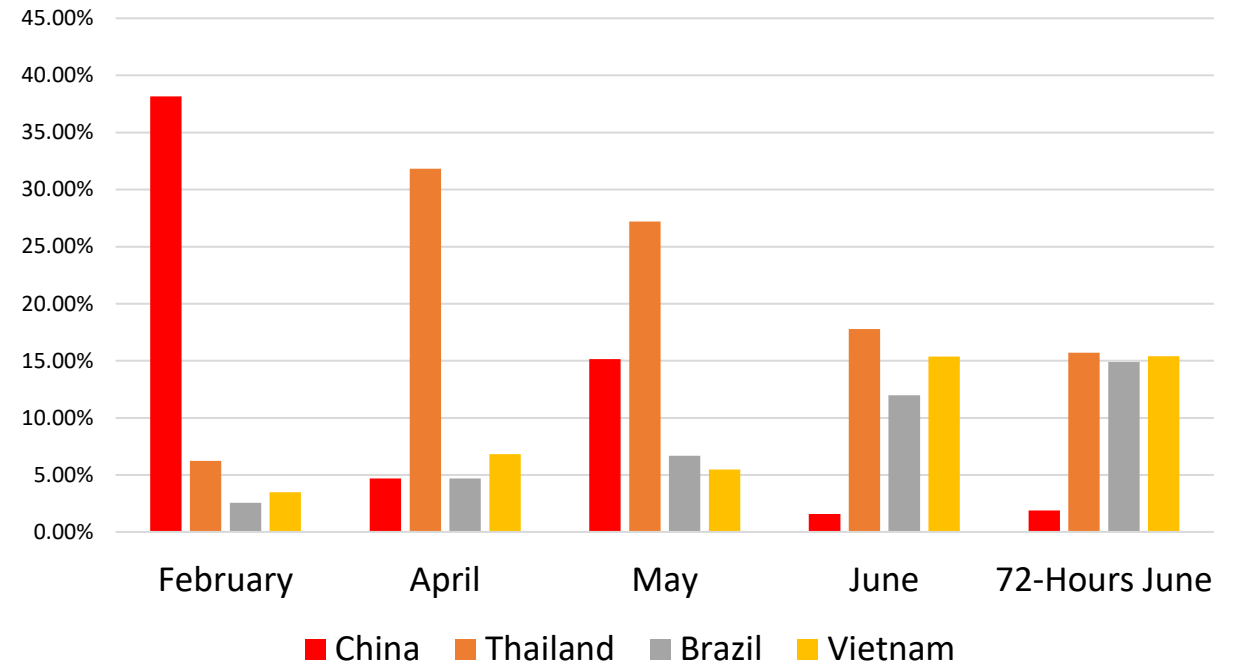


# Common 2020 Threat Trends



- **Phishing**
  - COVID-19
  - Financial
  - Vessel impersonation
- **Credential Stuffing**
  - O365
- **Scanning**
  - IT networks
  - RFID
  - Ports 21, 22, 25, 53, 80, 110, 443, 587, 993, 1433, 3306 and 3389

Failed O365 Login Attempts: % By Geolocation



Significant change in patterns for infrastructure launch points.

# Aim For Managing Risk

- **Cyber hygiene is critical**
- Example: email security
  - **People:** security awareness training using current, **real-world phishing examples**
  - **Processes:** Ensure personnel **understand how to handle links and attachments and report phishing emails** to security
  - **Technology:** apply principle of least privilege; limit the use of administrative accounts; leverage secure email features (DKIM, DMARC) and disable POP3, IMAP, and/or SMTP (e.g. O365 users); enable suspicious email activity logging and alerting; limit the ability to send PII; geo-blocking; etc.



**PHISHING!**  
DON'T TRUST THE BAIT!!!

Nothing tastes better than fresh phish...

> Avoid links and attachments – especially if they are asking for personal information

> Verify with the sender when you receive an unexpected request

1. **Check** if the address matches the sender.
2. **Beware** of non-personalized emails.
3. **Urgent action required** is a common phishing technique.
4. **Hover over the link** to see the real destination it will direct you to.



From: Package Delivery <david1234@gmail.com>  
Subject: Package Not Delivered  
Date: April 1, 2019

Dear Customer,

Unfortunately we were unable to deliver your package today. We will make two additional attempts in the **next 48 hours** before returning the package to the sender. Please verify your address is correct with the link below.

Order: 482637  
\*\*\*\*\*  
Shipping Tracking Information  
\*\*\*\*\*  
Tracking #: 1Z9Y623V085731294X  
Tracking Information:  
<https://www.fedex.com/tracking/1Z9Y623V085731294X>  
Shipped date: March 28, 2019

Thank you, <http://evilhacker.ru/phishedyou>

Please report suspicious emails to:



# Compliance Versus Risk Management



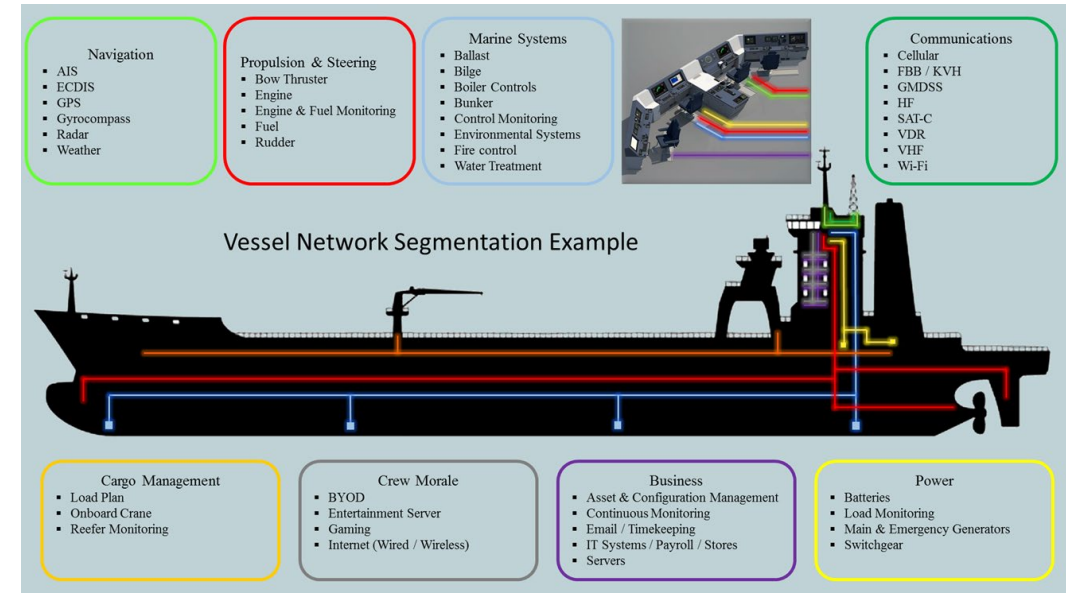
**Risk Management** builds the capacity to identify, protect, detect, respond and recover from cyber risk impacts

**“Compliance”** may satisfy an Inspector or Auditor, but is not reflective of the current cyber risk landscape

Compliance satisfies an audit and is a cost center, while risk management meets strategic organizational objectives, protects the organization, and can be a differentiator.

# Takeaways

- Cyber threat vectors are consistent, but are you **maintaining awareness of current threat campaigns** and how they are evolving?
- **Technology challenges can always be solved**, but how are you leveraging your **people and processes** to help you manage risk?
- **Risk management and compliance are separate, but overlapping efforts.** Does your organization have a strategic approach for these and managing the **actual risks** confronting the maritime sector on a daily basis?



# Questions or Comments?



# When Port Security Meets Cyber Security

## Riviera's Maritime Cyber Security Webinar Week 2020

Dr Kimberly Tam



# UNIVERSITY OF PLYMOUTH

Maritime Cyber Threats Research Group



# Wider University of Plymouth Context

- Founded in 1862 as the **School of Navigation**
- Home to globally leading **Maritime Cyber Threats Research Group**
- In November 2019 we were awarded funding from Research England for the new **Cyber-SHIP Lab (£3.2 million investment)** with 18 other partner organisations including shipping operators, ship builders and ships' equipment manufacturers, a class society, and supported by the UK Foreign and Commonwealth Office



# Our Research – The Big Picture

- We are researching into appropriate risk assessment for cyber & cyber-physical
  - **Ship to Port (but also beyond)**
  - **Looking at both IT and OT**
  - **Dynamic Risk Assessment (MaCRA)**

Aim is to give people information critical for cyber-safety and cyber-resilience in the sector





# Our Research – Case Studies

- **Cyber-MAR** – looking at specific case studies for cyber-security at ports (working with real ports)

- How plausible are some attacks?
- What do the *realistic* risks look like?
- What could a port cyber-attack cost?
- How do we train people to detect/mitigate these issues



 [www.Cyber-MAR.eu](http://www.Cyber-MAR.eu)

 Cyber\_MAR

 Cyber-MAR



*Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains*



**UNIVERSITY OF  
PLYMOUTH**




# Thank You



Dr Kimberly Tam

[kimberly.tam@plymouth.ac.uk](mailto:kimberly.tam@plymouth.ac.uk)

UoP Website 

<https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group>




[Newsletter sign-up](#)

## Some possible topics for the panel

- ◇ How do we measure Risk?
- ◇ How is Risk different for different ships/ports/organisations?
- ◇ How do we gather Data?
- ◇ How do we maintain/human involvement and safety?



The background features a dark blue gradient with a subtle pattern of white dots. Overlaid on this are several circular and semi-circular graphic elements in a lighter blue color. These include concentric circles, dashed lines, and arrows, some of which are arranged to form a scale or gauge. The scale is marked with numbers from 140 to 260 in increments of 10, with the numbers 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, and 260 visible. The overall aesthetic is technical and modern.

# STAYING OFF “THE ROCKS:” THE IMPORTANCE OF GOOD MARITIME CYBERSECURITY

PAUL FERRILLO

MCDERMOTT WILL & EMERY, LLP







**UNITED STATES COAST GUARD**  
U.S. Department of Homeland Security

***MARINE SAFETY ALERT***  
***Inspections and Compliance Directorate***

July 8, 2019  
Washington, D.C.

Safety Alert 06-19

***Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels***

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.

Prior to the incident, the security risk presented by the shipboard network was well known among the crew. Although most crewmembers didn't use onboard computers to check personal email, make online purchases or check their bank accounts, the same shipboard network was used for official business – to update electronic charts, manage cargo data and communicate with shore-side facilities, pilots, agents, and the Coast Guard.

<https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/C-G-5PC/INV/Alerts/0619.pdf>



YES, YOU ARE A TARGET, YES, YOU WILL BE HACKED. OR YOU HAVE BEEN HACKED ALREADY



PORT OF ANTWERP CYBERATTACK BY DRUG TRAFFICKERS





COSCO RANSOMWARE ATTACK HITS PORT OF LONG BEACH



## PORT OF SAN DIEGO RANSOMWARE ATTACK





## PORT OF BARCELONA CYBER ATTACK





## **CYBER-ATTACK AT A MAJOR PORT COULD COST \$1 BILLION PER DAY**

[https://www.gsnmagazine.com/article/39138/cyber\\_attack\\_major\\_port\\_could\\_cost\\_1\\_billion\\_day](https://www.gsnmagazine.com/article/39138/cyber_attack_major_port_could_cost_1_billion_day)

# THE THREATS AGAINST SHIPPING AND PORTS

- Nation states like Russia, China, Iran and North Korea – the Strait of Hormuz, the 2018 NATO WarGames, and the problems with GPS Spoofing commercial vessels in the Black Sea; recent GPS spoofing at the Port of Haifa;
- Cyber criminals – Ransomware attacks can be extremely costly and time punitive;
- The negligent or malicious insider – phishing, spearphishing, spoofing, #don'tclickonthelink
- Same threats – but potentially much bigger problems (including loss of life)



# CYBER REGULATIONS FOR THE MARITIME INDUSTRY – WHY THEY PROBABLY WON'T DO THE TRICK

- In the United States ports are critical infrastructure – The NIST Cybersecurity Framework applies – so do the United States Coast Guard Cyber regulations and cyber strategies which, for the most part, follow the NIST Framework.
- To the extent that there is PII involved, other federal and state laws may apply
- BIMCO "guidance" for ships and vessels
- IMO "guidance" on cyber risk management
- Guidance is "guidance," and not yet law - so no teeth
- No current enforcement mechanisms yet for USCG cyber regulations



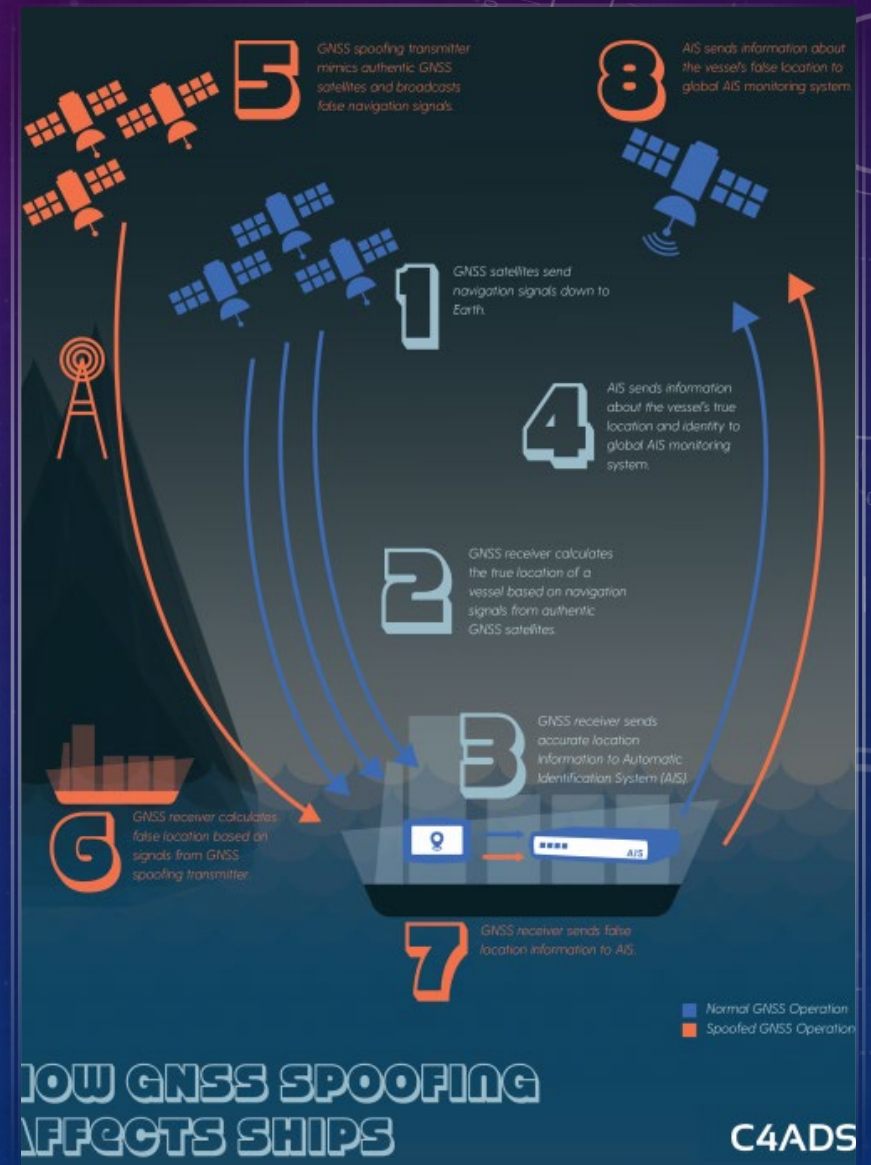
GPS SPOOFING IS DANGEROUS AND A GROWING THREAT



# GPS SPOOFING IS THE REAL DEAL

GPS spoofing tech works by manipulating Global Navigation Satellite Systems (GNSS) into believing they are located elsewhere. GNSS is a catch-all term for satellite-based navigation systems, including: GPS, the Russian GLONASS, Europe's Galileo and China's Beidou.

<https://www.wired.co.uk/article/russia-gps-spoofing>



## RUSSIA JAMMED GPS DURING MAJOR NATO MILITARY EXERCISE WITH US TROOPS

Norway has determined that Russia was responsible for jamming GPS signals in the Kola Peninsula during Exercise Trident Juncture. Finland has expressed concern over possible jamming in Lapland," NATO spokesperson Oana Lungescu told CNN Wednesday."In view of the civilian usage of GPS, jamming of this sort is dangerous, disruptive and irresponsible," she added.  
<https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html>



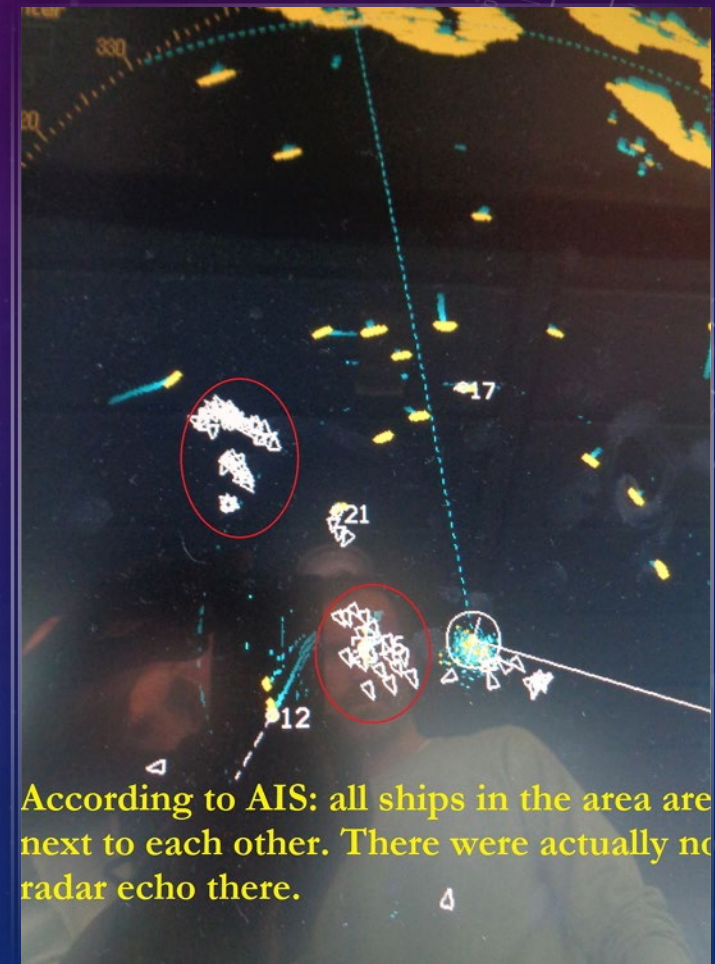


## IS GPS SPOOFING BEING DONE IN THE CIVILIAN ENVIRONMENT?

Russia spoofing civilian vessels in the Black Sea — It looks like a sophisticated attack, by somebody who knew what they were doing and were just testing the system,...it "strongly" looks like a spoofing incident. Fire Eye agreed, saying the activity looked intentional and...[was] purposely disrupted

Russia and Iran Spoofing Military and Civilian Aircraft in the Middle East

We don't know the true extent of GPS spoofing but it is certainly far more prevalent than reported.



# WHAT IS THE HOLY GRAIL OF MARITIME CYBERSECURITY?

- AI and machine learning at ports and on ships for visibility in IT and OT networks
- NIST cybersecurity framework should be made mandatory for ports and vessels
- Attention to architecture – Windows XP ain't going to cut it
- Comprehensive vulnerability and compromise assessments – every 3-6 months
- #patchit, #backitup, #thebasicsmatter
- Training and education of employees, deckhands, captains and crew
- Cybersecurity insurance may drive other improvements





# 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.<sup>1</sup>**

**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.<sup>2</sup> 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.<sup>3 4</sup> For over 20 years, sector-specific ISACs have been formed by owners and operators to share information.<sup>5</sup>

*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 - can provide the early warning needed to protect your organization from incidents.

## **Member of the National Council of ISACs (NCI) and DHS' Cyber Information Sharing and Collaboration Program (CISCP)**

MTS-ISAC's membership in the NCI and CISCP connects maritime critical infrastructure stakeholders with the NCI's 20+ ISACs, further expanding the ability of critical infrastructure stakeholders to share cyber threat information to better protect facilities, personnel, and customers and reduce risk. In addition, MTS-ISAC is part of DHS CISA's CISCP, providing additional valuable opportunities for analyst-to-analyst collaboration, operational analysis, and information exchange. As a result, MTS-ISAC stakeholders receive an unparalleled level of integration into critical infrastructure cybersecurity protection efforts.

By correlating cybersecurity information and trending over time, the MTS-ISAC is able to detect trends in cyber threats, which enables us to provide actionable recommendations on cybersecurity strategies.

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."<sup>6</sup> 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) included "Enhancing Cybersecurity" as a National Priority and identifies "Intelligence and Information Sharing" as a Core Capability.<sup>7</sup> MTS-ISAC Service is a PSGP fundable item and helps create a more resilient critical infrastructure sector.

<sup>1</sup> <https://techjury.net/stats-about/cyber-security/#gref>

<sup>2</sup> <https://www.cisa.gov/transportation-systems-sector>

<sup>3</sup> <https://www.aapa-ports.org/advocating/content.aspx?ItemNumber=21150>

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

<sup>5</sup> <https://www.nationalisacs.org/about-isacs>

<sup>6</sup> [https://www.acq.osd.mil/cmmc/docs/CMMC\\_Model\\_Appendices\\_20200203.pdf](https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf)

<sup>7</sup> [https://www.fema.gov/media-library-data/1581615217999-](https://www.fema.gov/media-library-data/1581615217999-123068487178bb6d65ae684a676ae46a/FY_2020_PSGP_NOFO_FINAL_508AB.pdf)

[123068487178bb6d65ae684a676ae46a/FY\\_2020\\_PSGP\\_NOFO\\_FINAL\\_508AB.pdf](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](mailto:info@mtsisac.org).



# Maritime Transportation System ISAC

Helping Build the Maritime Cybersecurity Community

*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 cyber 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 focused webinars, event information, exercise and training opportunities
- Discounts on cybersecurity products and services from a growing list of MTS-ISAC Trusted Partners

## MTS-ISAC Subscription Levels

<b>Organization</b>	<ul style="list-style-type: none"><li>• Ideal for organizations wanting to connect with peer maritime stakeholders.</li><li>• Receive actionable cyber threat intelligence and vulnerability information relevant specifically to maritime stakeholders.</li><li>• Training opportunities and information on best practices to improve the organization's cybersecurity resilience.</li></ul>
<b>Community</b>	<ul style="list-style-type: none"><li>• Up to 15 organizations - ideal for working collaboratively with tenants, partners, and suppliers on cybersecurity concerns impacting a specific community.</li><li>• Opportunity to receive and respond to more tailored cyber threat intelligence.</li><li>• Exercise incident response plans, address vulnerabilities, and implement best practices across the community to ensure continuity of business operations.</li></ul>
<b>Enterprise</b>	<ul style="list-style-type: none"><li>• For Federal Agencies, States or MTS Associations wanting to bring cybersecurity resiliency to maritime organizations within their area of responsibility (AOR).</li><li>• Opportunity for maritime organizations to operationalize critical cyber threat intelligence and receive insights on maritime cyber threat activity and trending.</li><li>• Advance cybersecurity awareness and resiliency across the AOR.</li></ul>

## 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
- Network Monitoring and Managed Security Services
- Cybersecurity Policy Assessments
- Cybersecurity Risk Assessments
- Paid Intelligence Feeds
- Penetration Testing and Threat Hunting
- Incident Response and Forensics Support
- Grant Writing Support

To learn more, or for information about the MTS-ISAC's Services and pricing, email [info@mtsisac.org](mailto:info@mtsisac.org).