HEARING BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES SUBCOMMITTEES ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION (CIPI) AND TRANSPORTATION AND MARITIME SECURITY (TMS)

October 26, 2021

Testimony of Scott Dickerson, Executive Director Maritime Transportation System Information Sharing and Analysis Center Institute (MTS-ISAC)

I. Background

Ranking Member Garbarino, Ranking Member Gimenez, and Members of the Subcommittee: My name is Scott Dickerson and I serve as the Executive Director of the Maritime Transportation System Information Sharing and Analysis Center Institute (MTS-ISAC). Thank you for the opportunity to testify before the Committee today.

The Maritime Transportation System ISAC was formed as a nonprofit by a group of U.S. maritime critical infrastructure stakeholders. Our primary mission is to more effectively share information focused on cyber threats and cybersecurity best practices within a trusted community of stakeholders to help make the maritime community more resilient to cyber-attacks. Our stakeholders include port authorities, vessel owners and operators, terminal owners and operators, cruise lines, energy facilities, ferry operators, and other members of the public and private sector maritime critical infrastructure community. On a daily basis, our stakeholders are sharing actionable, timely, and relevant cyber threat information with their public and private sector peers. They formed the MTS-ISAC out of a need to quickly share relevant cyber threat information and have quickly shown how effective their ISAC model is working to do just that.

MTS-ISAC stakeholders exchange information every day about the attacks they are seeing. The MTS-ISAC provides anonymization of identities, which when combined with the Cybersecurity Information Sharing Act of 2015 (CISA 2015), fosters community trust and enables peer-to-peer collaboration. This peer-to-peer collaboration is extremely valuable because it allows stakeholders to better understand threats targeting the maritime sector and implement cybersecurity strategies more effectively to counter those attacks. This private sector sharing has resulted in more maritime industry focused cyber threat intelligence advisories being distributed to our stakeholders since our inception than those released by the more than 20 Federal government organizations with a responsibility for maritime security[1] combined. As an example, we have produced over 80 Cybersecurity Advisories this year and to our knowledge the US Coast Guard has released five cybersecurity threat reports. The MTS-ISAC has not received any cyber threat or incident reporting from MARAD, Department of Energy, TSA, USTRANSCOM, NOAA, ODNI's National Maritime Intelligence-Integration Office (NMIO), and or other maritime-focused governmental organizations. We have created over 500 Indicator Bulletins sourced from stakeholder shares, which I believe is roughly on par with the whole of CISA. We do this on a nonprofit budget that runs in the low six figures annually.

Our stakeholders believe that cybersecurity is a core element of risk management that allows their organizations to operate in a safe and secure manner. Because of the critical intermodal connections and relationships that ports, terminals, and a variety of facilities have, some of our stakeholders are subject to a variety of regulations and security directives, including the Maritime Transportation Security Act of 2002 as well as TSA's Pipeline and soon to be finalized Rail Security Directives. This is in addition to a

[1] National Maritime Cybersecurity Plan - https://www.hsdl.org/?abstract&did=848704

variety of other cybersecurity related requirements that can include safeguarding various types of information including HIPAA, PCI, PII and other cybersecurity frameworks and requirements. I say this not to be glib, but to say the maritime sector faces a highly complex intersection of requirements, and maritime companies understand how to operate in this environment. Cyber incidents need to be handled extremely delicately since they can have major impact across supply chains, for customers, stakeholders, and shareholders. Legal departments and auditors within an organization help work these details in closed door sessions to ensure compliance and legal issues are addressed properly. Additionally, those with cyber insurance coverage will be directed by their insurance how and with whom to share information. It would be beneficial for the Federal government to consult with stakeholders before new cybersecurity laws, security directives, or similar facets of oversight are finalized to fully understand the implications of drafts so that the desired risk management outcomes can be met in a manner appropriate for the complexities of this industry without creating undue burdens or unintended consequences.

In addition to sharing cyber threat information, our nonprofit is also working with numerous industry stakeholders to improve industry cybersecurity guidelines. We have provided inputs to drafts for updates to the International Association of Classification Societies' *Recommendations on Cyber Resilience*. The MTS-ISAC also contributed content to the following maritime industry cybersecurity references:

- The Guidelines on Cyber Security Onboard Ships (V4) and
- IAPH Cybersecurity Guidelines for Ports and Port Facilities (Version 1.0).

II. Current Challenges with Federal Cybersecurity Approaches

There are currently multiple cybersecurity challenges impacting critical infrastructure cyber resiliency. Of particular interest from an ISAC perspective are the following:

Overlapping Efforts	• Redundant, and sometimes conflicting cyber regulations and enforcement or interpretation differences across government roles and responsibilities. ○ Multiple agencies are involved with duplicative efforts. Redundant tracking, outreach, reporting, and mitigation efforts are a detriment to securing critical infrastructure as the time of limited resources is spent on redundant efforts. ○ Inconsistent standards often impact multiple sectors and cause confusion. • Federal government focus on "leading", rather than partnering to support private sector efforts. The private sector predominantly owns and operates critical infrastructure, and the Federal government should support effective solutions rather than lead ineffective solutions. ○ Private sector understands where the challenges lie; multiple governmental agencies try to "solve the problem" in silos rather than in partnership.
Information & Intelligence Sharing	• There is currently a Federal government focus on cyber incident reporting, rather than exchanging timely threat information that could minimize potential impacts. ○ Lack of consistent and clear definitions for suspicious activity, incidents, etc. – this needs to be remedied and should be in partnership with industry. • CISA should be the Federal agency hub for information sharing, and that needs to be reflected in all regulations, Security Directives, etc. Having a single touchpoint will streamline processes and should allow for more cross-sector critical infrastructure correlations to be made that are currently being missed. • Similarly, there are concerns with USCG being both a regulator and pushing for threat intel sharing outside of the required reporting mandates. Providing non-

	mandatory event reporting to a regulator is a cause for concern for some in the private sector. This should be voluntary (and based on trust), but again it would be better to have a single point of contact for all critical infrastructure sector reporting, which for maritime can then be provided to the 20+ Federal government organizations with a responsibility for maritime security. • Repeated misinformation that private sector does not share information with each other or with governmental agencies. • Greater Federal resource emphasis on granting security clearances to private sector stakeholders, who remain constrained on acting on classified information. • Agency and media inaccurate claims that certain sectors are better or worse in cybersecurity protections pit private industry as competitors, not collaborators.
Cybersecurity Resourcing	• Experienced cybersecurity specialists are in short supply in all sectors and across the public and private sectors. • Federal funding of cybersecurity efforts remains inconsistent across sectors and sometimes competes with private sector cybersecurity efforts, which confuses and frustrates maritime stakeholders.

In addition to these, there are numerous other cybersecurity challenges that also need addressing, but others that are notable include:

- Risks related to foreign investment and/or reliance within U.S. marine critical infrastructure;
- A heavy focus on check-box style types of regulation;
- Recent TSA Pipeline Security Directive did not include a mechanism for review and feedback from the stakeholders this will impact. As a result, some challenges may be arising that could have been avoided if some language was changed. For example, requiring to inform the government within seven days of personnel that will be designated to be available 24/7 to the government for any reason. There are several HR implications for this, including the potential need to reclassify positions, renegotiate contracts, etc. for the personnel in those roles; and
- Lack of funding for voluntary CISA cybersecurity programs, including CISA Risk and Vulnerability Assessments (RVA), Validated Architecture Design Reviews (VADR), and similar efforts within the Coast Guard, such as their outstanding Cyber Protection Team.

III. Recent Example of Post-Incident Response

A recent incident at a critical port is an example of a post incident response that highlights some of the above challenges and how the Federal government is currently handling critical infrastructure cybersecurity.

Summary

A port quickly identified and responded to a cyber-attack exploiting a zero-day vulnerability. The port confirmed the incident with their security vendor, who was able to identify other clients in other critical infrastructure sectors also experiencing the same attack. The port notified CISA, USCG, FBI and MTS-ISAC. The MTS-ISAC shared information with stakeholders and with other members of the National Council of ISACs the same day.

The Federal agencies worked with the vendor on a patch but stated they did not want vulnerability information shared broadly across critical infrastructure sectors until the patch was made available. Rather than engage in public-private partnership, these Federal agencies unilaterally decided to leave U.S.

critical infrastructure owners and operators with limited visibility and awareness to ongoing, active attacks exploiting a 0-day vulnerability. However, indicators that could have helped cyber defenders (for example hashes of files related to the attack) could have aided critical infrastructure to identify if they were under attack and take response actions. This could be done without leaking sensitive information that could lead to additional threat actors exploiting the vulnerability. Critical infrastructure protection and resiliency did not appear to be the priority for these agencies.

Finally, almost three weeks later, vulnerability and patch information was released as TLP:WHITE information along with a TLP:AMBER Joint Cybersecurity Advisory with information related to the attack. Then over a week later, similar information was released as TLP:WHITE. Then after another week went by, without coordinating or notifying the victim organization ahead of time, CISA personnel named the victim in a public Senate hearing and a USCG TLP:AMBER Technical Report was leaked to the press. During this time no Federal agency contacted or collaborated with the MTS-ISAC or other National Council of ISAC members. However, the MTS-ISAC regularly shares Cybersecurity Advisories with personnel at all three agencies and is a member of CISA's Cyber Information Sharing and Collaboration Program (CISCP).

Trust is critical when fostering collaboration and information sharing, which we absolutely need to create a more cyber resilient critical infrastructure community. The maritime community's trust in Federal agencies was shaken following this incident because:

1. Immediately following the incident, the Federal government delayed information sharing for three weeks while the critical infrastructure community was ready to share this information immediately.
2. CISA released the name of the victim which may have been in violation of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and perhaps the Federal government should research whether this should lead to sanctions. "*Section 1504(a)(3)(C)(ii) requires that procedures ensure there are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under CISA 2015 in an unauthorized manner*."[2]
3. A USCG For Official Use Only Technical Report with details surrounding the incident was leaked to the press. The MTS-ISAC did not receive this report nor did other maritime stakeholders. If the report was intended solely for the victim, then how did the press receive it? Some industry stakeholders are wondering if this was "leaked" as part of a political agenda. No matter how or why, several stakeholders have expressed concerns with reporting incidents to the government as a result.

To be honest, the most common refrain I hear from private sector stakeholders when it comes to information sharing with the Federal government can be boiled down to a lack of trust in how the government will handle the information. I hate to hear this having served on active duty and as a Federal government civilian, but there are some legitimate concerns that should be recognized. I thought about whether to bring this challenge up in my testimony, but *nothing* will improve by not bringing this up. At some point conversations about how Federal government actions are undermining the trust of the critical infrastructure community would be healthy, in my opinion.

IV. Opportunities for Improvement

There are opportunities for the Federal government to effectively partner with the MTS-ISAC and public and private sector maritime stakeholders:

[2] https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

Improve Efficiencies	• Leverage ISACs and other forums to reduce redundant efforts and join private sector stakeholders in their chosen collaboration mechanisms. The MTS-ISAC has nonvoting seats for CISA, Coast Guard, and the Department of Energy representatives which remain unfilled by these agencies. ○ Support private sector stakeholder solutions that already address Federal governmental needs and have proven effective for critical infrastructure. • A great example is also the Information Exchanges being created that include port authorities, USCG, CISA, other agencies and public and private local Maritime stakeholders working with the MTS-ISAC at a community level to define and foster trust while sharing actionable, relevant, and timely threat information.
Information & Intelligence Sharing	• CISA 2015 remains significantly underutilized. Although it has been implemented, there remains resistance to fully trusting and using the provisions of the legislation by both Federal and private partnership programs. • Prioritize ongoing bi-directional exchange of unclassified threat information between the public and private sectors, not just incident reporting. ○ Holistic sharing of threat information, best practices, and lessons learned is more beneficial for improving cyber resilience than focused incident reporting. • Improve training of government personnel on proper information classification procedures and how to more effectively mark information to allow for sharing. • Focus additional Federal resources toward information declassification efforts.
Resource Investments	• Ensure requirements are in place to raise awareness of Federal employees of cybersecurity funding opportunities that align with agency mission sets.[3] • Review opportunities for partnering with ISACs for hands on cybersecurity training, internships, and educational opportunities. • CISA should consider funding ISAC analyst positions at CISA Central to better facilitate the bi-directional flow of information across critical infrastructure. • Multiple maritime stakeholders are partnering with Computer Science, Cybersecurity or other closely related college programs to provide students with real-world experiences that they might not otherwise have exposure to for several years. These programs would benefit from further support and resourcing. • Increase funding for voluntary programs such as RVAs, VADR, and CPTs; waitlists and backlogs for these efforts should not be reaching 18+ months as they have in the past. The Coast Guard has an outstanding Cyber Protection Team, but there is a need for regional cyber incident response teams. There are not enough to adequately provide assistance should there be even a mild demand. CISA was not able to respond in a timely manner to produce meaningful input to a recent attack on a port authority.

[3] As an example, cybersecurity was the highest stated priority for FEMA's 2020 Port Security Grant Program. Yet many stakeholder requests for cybersecurity investments were turned down by USCG Captains of the Port in favor of physical security efforts, resulting in only roughly $12 million out of the $100 million program being invested in the highest priority area.

V. Conclusion

The MTS-ISAC is hopeful that the maritime critical infrastructure community and the Federal government can more effectively partner with each other to safeguard our national interests. Sharing cyber threat information is a key element to improving our resiliency, and that will work best if industry and ISACs are engaged as envisioned by CISA 2015. Whether it is related to incident response or proactive threat information sharing, we need true collaboration between the Federal government and other public and private sector organizations. Currently this is not an effective system of public-private partnership and collaboration. It feels like industry is being threatened with additional regulation and security directives rather than being treated as the partners who own and operate the vast majority of critical infrastructure. I kindly request you consider the beneficial role that ISACs play daily in facilitating trusted, anonymous, information sharing for the improved resiliency of critical infrastructure across our country in the face of ongoing cyber-attacks. Please include, and protect the mechanisms safeguarding, the ISAC communities in legislation related to critical infrastructure cybersecurity efforts. Any bill associated with critical infrastructure cybersecurity efforts that does not reflect the positive, critical, and irreplaceable role that ISACs and industry representatives and stakeholders provide to our critical infrastructure communities, and does not include provisions requiring Federal agencies to effectively collaborate with them, should be opposed. Thank you again for the opportunity to provide this testimony.