Maritime Transportation System ISAC

Helping Build the Maritime Cybersecurity Community

November 14, 2022

The Honorable Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, D.C. 20032

Comments to Docket: CISA-2022-0010

Dear Ms. Easterly:

The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) is pleased to provide comments on the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information (RFI) about the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

The MTS-ISAC was originally formed by a group of public and private sector critical infrastructure stakeholders in the United States who were interested in more effectively sharing cyber threat information across a community of stakeholders with common interests in improving the cyber resiliency of maritime, transportation, and supply chains. Our stakeholders include port authorities, terminal operators, vessel operators, logistics operators, cruise lines, energy sector, and other stakeholders associated with maritime transportation. Our community has regularly expanded since its inception to include likeminded stakeholders across the international community and includes several of the largest U.S. maritime critical infrastructure owners, operators, and port authorities.

Our stakeholders' reach extends throughout the entire United States, including to geographically isolated and remote communities. Annually, our stakeholders support millions of jobs paying over $500 billion in salaries and wages and more than $1 trillion in total spending across the country. They support all sectors of the economy as over 90% of goods travel by water at some during their supply chain voyages. Of equal importance, our stakeholders support critical military cargo and supply chain operations.

Our stakeholders include the most technologically advanced ports in the nation serving as intermodal transportation hubs and connectors. If the situation maintained the status quo, this would already represent an important cybersecurity aspect to our critical infrastructure. However, the maritime sector is undergoing rapid digitalization efforts which will only increase our criticality in the coming years and present an even larger attack surface.

Given the sector's reliance on technology, every stakeholder has a need for multiple cybersecurity projects. In addition to our internal community efforts, we have participated in several efforts to align cybersecurity programs and have close working relationships with multiple U.S. agencies, including the lead Sector Risk Management Agency for maritime, which is the United States Coast Guard (USCG).

As critical infrastructure, our port and vessel stakeholders have a vested interest in participating in the development of any new regulations that may impact them. As you may be aware, the transportation sector is the only critical infrastructure sector operating under emergency security directives. In addition, several of our U.S. critical infrastructure stakeholders already can have multiple existing cyber incident reporting mandates from the Department of Homeland Security (DHS) through the USCG, the Transportation Security Administration, and U.S. Customs and Border Protection, as well as other U.S. Federal Agencies. We believe that Congress' intent with CIRCIA was to extend cyber reporting

requirements to elements of critical infrastructure, following some high-profile incidents, that did not have reporting requirements as robust as the maritime sector has.

CISA appears to recognize this in the RFI by seeking information on, "Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements."

Our U.S. critical infrastructure stakeholders are regulated facilities under the Maritime Transportation Security Act (MTSA), and as such are required to report activities that may result in a Transportation Security Incident (TSI) – including cyber incidents – to the National Response Center (NRC). The NRC is expected to then notify other relevant agencies, including CISA. Furthermore, multiple states also require cyber incident reporting.

In the midst of a cyberattack, we need critical infrastructure stakeholders focused on effective incident response to hopefully maintain a resilient operating state. We do not need them bleeding their resources dry trying to report to more than a dozen different governmental parties that want the information, especially when they have never clarified how that information will be used to protect critical infrastructure or be shared with other critical infrastructure stakeholders to help prevent additional incidents. As disruption to supply chains is incredibly costly, we need resources focused on the task at hand. Given that at least 18 Federal agencies have a role in the maritime sector, adding an additional layer of bureaucracy is most unwelcome for our stakeholders and would further impede their ability to respond to a cyberattack, restore critical systems, and return to normal functions. This is a disappointing aspect of CIRCIA. It represents a one-way street of additional reporting to the U.S. government with no guarantees or timelines as to when that information will be shared with the U.S. critical infrastructure community. This must be remedied to have a positive effect on critical infrastructure cyber resiliency.

As we saw in 2021, an incident at a U.S. maritime critical infrastructure stakeholder was identified and reported to CISA, the USCG, the FBI and the MTS-ISAC. The same day the MTS-ISAC quickly and anonymously shared the information regarding a zero-day attack with stakeholders so they immediately had situational awareness of an ongoing active exploit so they could act. This information stayed secure amongst trusted stakeholders. CISA and the other agencies took weeks to share this information. The reporting party was then identified in Senate testimony, a possible violation of the Cybersecurity Information Sharing Act of 2015 (CISA of 2015).

What assurance do stakeholders have that incidents reported under CIRCIA will not be disclosed in a similar fashion by CISA? What investigation was conducted to identify protection controls that need to be strengthened? What measures have been taken since last year to ensure these violations do not persist? Given the existing reporting requirements, do we need CIRCIA to be applied to the maritime sector?

The MTS-ISAC requests that CISA recognize compliance with both the spirit and text of CIRCIA through current processes and regulations rather than imposing an additional and further redundant reporting requirement. However, we would encourage CISA whether through CIRCIA implementation or other avenues to improve the communication and dissemination of cyber incident reporting across federal agencies and to other critical infrastructure stakeholders. If CISA believes that current maritime sector cyber reporting is insufficient in terms of how CIRCIA is written, then any additional regulatory requirements should be minimized.

Similarly, while we know that there is current reporting to the U.S. government happening regarding cyber incidents as required by law, cyber threat information related to these incidents is not distributed to critical infrastructure stakeholders. Again, we strongly encourage that as part of the rulemaking that it includes a no greater than 24-hour requirement for the reported threat information related to an incident to be shared back out to the critical infrastructure sectors. This sharing should include via the National Council of ISACs and/or the MTS-ISAC for incidents related to our critical infrastructure sector. This information is vital to be shared to limit the damage done by cyber attacks and improve the overall resiliency of the sector. We need our Federal partners to actively engage and provide two-way communication in order to allow us to prepare for and respond to threats. Currently this partnership is sorely lacking, and the transportation sector has been to date excluded entirely from the Joint Cyber Defense Collaborative (JCDC).

We appreciate the opportunity to provide feedback and look forward to providing more detailed comments as the rulemaking process progresses, including technical recommendations. Please do not hesitate to reach out if to me directly if you have any questions or would like more information.

Sincerely,

Scott Dickerson

Scott Dickerson
Executive Director