Maritime Transportation System Cyber Resilience

Project Objective

Cybersecurity disruption impacts the ability of multiple critical infrastructure entities to work together in a coordinated fashion as required by the maritime industry. Ports, terminal operators, shipping companies, railroads, utilities and emergency services all need to operate in a seamless fashion to make commerce and the maritime system function. A cyber disruption could drastically impact the maritime industry as a whole, and send ripples through the global transportation system.

Today there are no established protocols or processes in place to provide guidance to the broader maritime community about what to report, when to report it, how to report it, and, to whom to report maritime cyber incidents. Because the maritime transportation system is dependent on public and private interconnections, this broad group must define what a cyber incident is and identify reporting protocols and processes. This project seeks to articulate the strategy for sharing ongoing cybersecurity threats and the operational instructions to do so via a concept of operations (CONOPS).

Coast Guard attends Sofie Maersk in Honolulu (Source: USCG)

Project Overview

This project will generate a regional maritime notification protocol for critical infrastructure organizations to report cyber events. The goal will be to establish a single point for the collection of cyber-incidents that will be responsible for sharing this information, as appropriate, with other organizations operating in support of maritime transport operations. This reporting structure will support the CONOPS and enhance cybersecurity. The end result will be a defined criteria for reporting incidents that have been socialized with appropriate critical infrastructure owners and operators that enhance their cyber- resilience, and a baseline level of cyber infrastructure will be established. Finally, training port partners and employing an intern/mentorship program will help enhance regional cybersecurity. It will help build a directory of best practices to follow when a cyber incident occurs and an inventory of resources for cyber response and recovery.

Next Steps

As a result of this project, coordination will exist to facilitate a better regional analysis to provide a synchronized response to specific threats. This initiative will reduce risk in a coordinated, cost effective manner by developing a concise and easy to follow set of guidelines, and will develop a tool for reporting. It will also assist ports and critical service providers in reducing vulnerabilities through the development of checklists and options for cybersecurity consideration. It will provide a mechanism for reporting and sharing information that can reach all levels of government. This will result in enhanced coordination and information sharing regarding threats and attacks, and ensure incidents and vulnerabilities are escalated to appropriate response agencies and stakeholders.

To learn more about this program, contact
Jay Robinson, DHS Program Manager, at jay.robinson@hq.dhs.gov or
Ewell Balltrip, CEO, NIHS at eballtrip@thenihs.org