Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 02-22
Date: April 11, 2022
Phone: (202) 372-1107
E-Mail: Brandon.m.link@uscg.mil

CYBERSECURITY AWARENESS & ACTION

The Coast Guard continues to monitor world events and their potential impact on the Marine Transportation System (MTS). We remain engaged with our interagency partners and industry stakeholders to share information and coordinate the federal government's preparedness and response efforts to minimize disruptions to the MTS, including disruptions due to cyber threats.

CISA's "Shields Up" website remains the primary location for information and recommendations for adapting a heightened cybersecurity posture, and we highly encourage all MTS stakeholders to visit the site regularly for updates and reminders. MTS stakeholders can also receive CISA's subscription service for timely updates/bulletins. The Coast Guard continues to monitor guidance and products from CISA and partner agencies and will distribute these materials to stakeholders, along with maritime-specific context, as appropriate.

Per CISA's "Shields Up" guidance, "Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. Government. In this heightened threat environment, these thresholds should be significantly lower than normal." The Coast Guard fully supports this guidance and stands ready with our partner agencies to respond to these reports. Considering the heightened risk, stakeholders should closely monitor their computer systems, telecommunications systems, and networks for suspicious activity and breaches of security and, when in doubt, report to the National Response Center (NRC). Maritime Transportation Security Act (MTSA) regulated vessels and facilities *are required*, and other MTS stakeholders are encouraged, to report breaches of security or suspicious activity to the NRC at 1-800-424-8802. The CG-5P Policy Letter 08-16, Reporting Suspicious Activity and Breaches of Security provides additional guidance on the reporting of cyber incidents.

The Coast Guard continues to review policies, procedures, and guidance to address the evolving nature of cyber risk management. The Coast Guard published Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, as well as a Vessel Cyber Risk Management Work Instruction, to assist stakeholders in incorporating cybersecurity into facility and vessel security assessments and plans. Additionally, in ports across the country, Area Maritime Security Committees (AMSC) serve as a key resource for local, state, federal and private entities to engage on information sharing, best practices,

and port safety and security. We will continue to leverage these committees to address cyber risks in the MTS.

While breaches of security and suspicious activity are required to be reported to the NRC, the Coast Guard's Cyber Command is available to provide technical support to help MTS stakeholders prepare for or respond to a cyber-incident. Their 24x7 watch can be reached at: 202-372-2904 or CGCYBER-SMB-NOSC-BWC@uscg.mil.

Thank you for your continued vigilance.

John W. Mauger, RADM, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends.