# Marine Safety Information Bulletin

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

MSIB Number: 18-20
Date: July 24, 2020
Contact: Brandon Link, CDR
Phone: (202) 372-1107
E-Mail: brandon.m.link@uscg.mil

## URGENT NEED TO PROTECT OPERATIONAL TECHNOLOGIES AND CONTROL SYSTEMS

The cyber landscape in the Marine Transportation System (MTS) is continually evolving. Computer systems and technology play an increasing role in systems, equipment, and operations throughout the maritime environment. While advances in systems and technologies can improve the efficiency and scope of operations, there is a heightened risk of increased threats posed by malicious actors. These cyber actors have demonstrated a willingness to conduct malevolent activity against maritime critical infrastructure by exploiting internet-accessible operational technology (OT) assets.

Internet-accessible OT assets are prevalent across maritime critical infrastructure. Legacy OT systems that were not designed to defend against current threats and activities, along with a failure to take necessary actions to protect newer systems and equipment, create opportunities for vulnerabilities and exploitation. The nature of maritime operations lends itself to interactions with multiple actors and touch points for cyber intrusion, necessitating a continually increasing focus on mitigating cyber threats.

The Cybersecurity and Infrastructure Security Agency (CISA) has released an alert entitled, Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, which is directly relevant to the MTS. The maritime sector heavily utilizes the technologies discussed in this alert and the recommendations in it can help reduce cyber risk.

The Coast Guard continues to work with maritime stakeholders to develop guidance, policy, and recommended best practices. Recently released policy includes Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. This NVIC provides guidance to Maritime Transportation Security Act regulated facility owners and operators on complying with requirements to assess, document, and address computer system and network vulnerabilities. Additionally, a Facility Inspector Cyber Job Aid was developed to provide Coast Guard marine safety personnel with additional guidance as they address facilities' documented cyber vulnerabilities. Facility security personnel may likewise reference this guide for additional familiarization.

As always, any potential threat to the cybersecurity of your vessel or facility should be taken seriously, and Breaches of Security or Suspicious Activities resulting from cyber incidents shall be reported to the National Response Center at 1-800-424-8802. For additional technical support, consider calling the Coast Guard Cyber Command's 24x7 watch at 202-372-2904 or via email at CGCYBER-SMB-NOSC-BWC@uscg.mil. Your willingness to comply and report in a timely manner helps the U.S. respond quickly and effectively and makes the maritime critical infrastructure safer.

Richard V. Timme, RDML, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends