United States Coast Guard
U.S. Department of Homeland Security

ALCOAST COMMANDANT NOTICE CANCEL DATE 19 MAR 2021

R 200709 MAR 20
FM COMDT COGARD WASHINGTON DC//CG-5P//
TO ALCOAST
UNCLAS//N16600//
ACN 040/20
SUBJ: PROMULGATION OF NAVIGATION AND VESSEL INSPECTION CIRCULAR (NVIC) NO. 01-20: GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES
A. NAVIGATION AND VESSEL INSPECTION CIRCULAR (NVIC) No. 01-20: GUIDELINES FOR ADDRESSING CYBER RISKS AT MTSA REGULATED FACILITIES
1. The cyber landscape in the Marine Transportation System (MTS) is continually evolving. Cybersecurity, safety, and risk management are of utmost importance as computer systems and technology play an increasing role in systems and equipment throughout the maritime environment. Recognizing the critical role cyber plays, particularly within Maritime Transportation Security Act (MTSA) regulated facilities, the Coast Guard worked closely with industry and other government agencies to provide guidance on complying with cybersecurity requirements. Today, we are proud to announce the release of REF (A).
2. This NVIC provides guidance to facility owners and operators on complying with the requirements to assess, document, and address computer system and network vulnerabilities. In accordance with 33 CFR parts 105 and 106, which implement the MTSA of 2002, regulated facilities (including Outer Continental Shelf facilities) are required to assess and document vulnerabilities associated with their computer systems and networks in a Facility Security Assessment (FSA). Identified vulnerabilities in computer systems and networks are commonly referred to as cybersecurity vulnerabilities. Regulations require that any cybersecurity vulnerabilities identified in the FSA must be addressed in the Facility Security

Plan (FSP) or Alternative Security Program (ASP). This NVIC is intended to assist regulated facility owners and operators in updating FSPs/ASPs to comply with the existing MTSA regulations. This guidance is intended to assist owners and operators in identifying computer systems and networks vulnerabilities which could cause or contribute to a Transportation Security Incident (TSI), a Breach of Security, and/or the identification of Suspicious Activity.

3. When cybersecurity vulnerabilities are identified in the FSA, an owner or operator may demonstrate compliance with the regulations by providing its cybersecurity mitigation procedures in a variety of formats. The information may be provided in a stand-alone cyber annex/addendum, incorporated into the FSP/ASP together with the physical security measures, or some other method identified by the owner or operator with concurrence from the local Captain of the Port (COTP), or in the case of ASPs with Coast Guard Headquarters. Facility owners and operators do not have to identify specific technology or a business model, but should provide documentation on how they are addressing their facility-specific cybersecurity vulnerabilities.

4. Although the MTSA regulations in 33 CFR parts 105 and 106 are mandatory, it is up to each facility to determine how to identify, assess, and address the vulnerabilities of their computer systems and networks.

5. Implementation Guidance: The following information outlines the process and timeline for addressing cybersecurity vulnerabilities in FSAs and FSPs/ASPs after the release of NVIC 01-20. The NVIC does not change the existing requirements found in regulation; it only provides guidance on how facility owners or operators may meet those requirements. Owners and operators may choose alternatives to the guidance in the NVIC if those alternatives meet the regulatory requirements. COTPs are encouraged to review and discuss the regulatory requirements, the NVIC, and this process and timeline information with facilities in their AOR.

a. Implementation Period (1.5 years): No submissions to update an FSA or FSP/ASP will be required within a 1.5 year period ending on 09/30/2021. This initial implementation period will allow MTSA-regulated facility owners or operators time to address cybersecurity vulnerabilities in their FSA and FSP/ASP by incorporating this guidance, or an alternative as best fits their needs. Facility owners and operators who already address cybersecurity in their FSAs and FSPs/ASPs should continue doing so, while considering whether the guidance in NVIC 01-20 can improve their ongoing practices. Additionally, this period allows the Coast Guard time to conduct any necessary training of its field personnel, dissemination of best practices,

or similar internal alignment before FSA and FSP/ASP amendments begin.

b. Phased-in Submittal Timeframe (one year): After the implementation period, and beginning 10/01/2021, facilities should submit cyber FSA and FSP/ASP amendments or annexes by the facility's annual audit date, which is based on the facility's FSP/ASP approval date. COTPs will still have the flexibility based on resource demands, or based upon request from a facility, to adjust when submissions are received, as long as all facility FSA and FSP (Headquarters for ASPs) submissions are received by the end of the one year period, no later than 10/01/2022.

c. The review level of FSA and FSP amendments or annexes will remain at the COTP level, and Headquarters for ASPs. The review should follow the same self-evaluation methodology and review process already in use.

d. Job Aid and Frequently Asked Questions (FAQs): Coast Guard Headquarters COMDT (CG-FAC) is finalizing a cyber-focused job aid and FAQs to assist facility inspectors and industry. Both publications will be released as soon as practicable and will be located on the COMDT (CG-FAC) website: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/. Additional questions will be added to the FAQs as they are received.

6. Commands are encouraged to ensure widest dissemination of this ACN.

7. For questions regarding the NVIC and implementation guidance, units are directed to first contact their District or Area Prevention Office. The COMDT (CG-FAC) POCs: CDR Brandon Link at Brandon.M.Link@uscg.mil or (202) 372-1107 and LT Kelley Edwards at Kelley.C.Edwards@uscg.mil or 202-372-1147.

8. Released by RDML Richard V. Timme, Chief of Prevention Policy (CG-5P).

9. Internet release is authorized.