

Marine Safety Information Bulletin

07-22

February 25, 2022

MTSA Regulated Facilities Cyber Risk

In accordance with Maritime Transportation Security Act (MTSA) regulations in 33 CFR 105 and 33 CFR 106, Navigation and Vessel Inspection Circular (NVIC) 01-20 and additional clarification found in the NVIC 01-20 Frequently Asked Questions page, MTSA regulated facilities are required to assess and document vulnerabilities associated with their computer systems and networks in a Facility Security Assessment (FSA) and address these cyber security related vulnerabilities within the facility's Facility Security Plan (FSP). As per this guidance, the submittal timeframe for these FSA reports and amendments/annexes to FSPs ends **October 1, 2022**.

All facilities that do not currently address cybersecurity within their FSA report and FSP are highly encouraged to begin updating their FSA reports and FSPs to meet this guidance. Only the updates to the cyber portions of the FSA report and FSP or the Cybersecurity Annex will be subject to re-approval. Such updates may include the following:

- Updating or amending their FSA report to include computer system and network vulnerabilities.
- Amending their FSP to include computer system and network vulnerabilities.
- Creating a standalone Cybersecurity Annex to the FSPs

Facilities are advised to consider vulnerabilities in multiple security environments taking into account actions at various MARSEC Levels. Additionally, facilities are encouraged to be mindful of Information Technology (IT) and Operational Technology (OT) risks. Operations where IT and OT crossover can cause significant harm to a facility and its surrounding infrastructure. Guidelines for information sharing regarding cybersecurity incidents and lessons learned are addressed in the Traffic Light Protocols on the Cybersecurity and Infrastructure Security Agency (CISA) webpage.

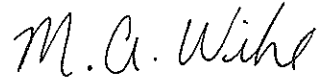
Facilities are encouraged to consider requesting the Coast Guard's Maritime Cyber Readiness Branch Cyber Protection Team (CPT) to conduct an analysis of your cybersecurity posture and receive further guidance to optimize cyber incident prevention and response.

Early submissions are encouraged as October 1, 2022 aligns with the peak of the Coast Guard's personnel transfer season and hurricane season. Late submissions may result in delays to the review process. Should an MTSA regulated facility need assistance meeting the regulations, or the deadline, please reach out to the contact avenues listed below.

Please contact the Marine Safety Unit Port Arthur Facilities Division at 409-460-0640 or 406-719-5033.

Facilities are reminded of the existing requirements in 33 CFR 101.305 to report suspicious activities, breaches of security, and transportation security incidents including cyber threats to the National Response Center at 1-800-424-8802.

This notice will be posted on the Coast Guard's HOMEPORT website at <http://homeport.uscg.mil> and the VTS website at <https://www.atlanticarea.uscg.mil/vtsportarthur/>. If you have any questions regarding this notice, please call Vessel Traffic Service Port Arthur at (409) 719-5070 (24-hours).

A handwritten signature in black ink that reads "M. A. Wike". The signature is written in a cursive style with a large initial "M" and a stylized "A".

M. A. Wike
Captain, U. S. Coast Guard
Captain of the Port