# NVIC 01-20 Frequently Asked Questions (FAQ) – Dated 3/20/2020

The following is a list of FAQs related to Navigation and Vessel Inspection Circular (NVIC) 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. The Coast Guard will continue to review and update these FAQs in order to provide accurate, up-to-date information. Additionally, the Coast Guard will look at opportunities to engage with industry on the NVIC, including a future webinar to discuss key points of the NVIC and review some of the frequently asked questions.

**Who can I contact if I have questions regarding the NVIC that aren't covered here?**

Facility owners, operators, and FSOs should reach out to the local Captain of the Port (via the Facilities or other Inspection Division as appropriate).

**Is this Navigation and Vessel Inspection Circular (NVIC) 01-20 a new regulation or new requirement?**

NVIC 01-20 is not a regulation. It is intended only to provide clarity regarding existing requirements under the law. It does not change any legal requirements, and does not impose new requirements on the public. This NVIC provides guidance to facility owners and operators in complying with the existing regulatory requirements to assess, document, and address computer system or network vulnerabilities. Not all recommendations will apply to all facilities, depending on individual facility operations. Facility owners and operators may use a different approach than this NVIC recommends, if that approach satisfies the legal requirements.

**What regulations does this NVIC provide guidance for?**

In accordance with 33 CFR Parts 105 and 106, which implement the Maritime Transportation Security Act (MTSA) of 2002 as codified in 46 U.S.C. Chapter 701, 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). If vulnerabilities are identified, the applicable sections of the Facility Security Plan (FSP) must address the vulnerabilities in accordance with 33 CFR 105.400 and 106.400.

Existing regulations require the owners and operators of MTSA-regulated facilities to analyze vulnerabilities associated with radio and telecommunication equipment, including computer systems and networks. Vulnerabilities in computer systems and networks are commonly referred to as cybersecurity vulnerabilities. Under the MTSA regulations, an FSP must address any cybersecurity vulnerabilities identified in the FSA.

**Are there approved standards or 3rd parties that can help?**

While the Coast Guard does not maintain a list of 3rd parties working on this issue, facilities are welcome to seek out 3rd parties that are working independently to provide training, education, and other services regarding the assessment and implementation of cyber in the FSAs, FSPs, and Alternative Security Programs (ASPs), as well as general facility operations.

Additionally, there are numerous cybersecurity standards that may assist in incorporation of cybersecurity and cyber risk management into the FSA, FSP, and operations. Currently there is no CG-approved list of cybersecurity standards, though the NIST Cybersecurity Framework is one example that has been widely utilized.

**Do I have to rewrite my FSP?**

No. If the FSA identifies a vulnerability to the computer system or network that is not already addressed in the FSP, the FSP needs to be amended to address that vulnerability. The Coast Guard will accept an annex, addendum, or other method identified by the facility owner/operator so long as the requirements within regulation are met. A complete rewrite is not necessary, unless the facility owner/operator prefers that approach.

**What documentation is acceptable to demonstrate a facility has addressed cybersecurity?**

An updated FSP, or an annex, addendum, or other "attachment," is acceptable so long as the submission shows that the facility has assessed, and addressed if necessary, vulnerabilities associated with its computer systems and networks.

**I need to update my FSA and FSP to address computer systems and networks. What is the deadline for doing that?**

The Coast Guard is allowing a 1.5 year long implementation period of the cybersecurity requirement, ending on 09/30/2021. This initial implementation period will allow MTSA-regulated facility owners/operators time to address cybersecurity vulnerabilities in their FSA and FSP or 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 or ASPs should continue doing so, while considering whether the guidance in NVIC 01-20 can improve their ongoing practices.

Once this implementation period is over (beginning 10/01/2021), facilities should submit cybersecurity 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. Captains of the Port (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 submissions are received by the end of the one year period, no later than 10/01/2022. The same flexibility is available to facilities using ASPs, except they should communicate with Coast Guard Headquarters rather than a COTP.

**What is required of the FSP in regards to a company's organizational structure, number of employees, employee roles, responsibilities, access permissions, training, etc.?**

The FSP should document items as required in the CFR. Whatever has been covered previously should continue to be included, but with the addition of any applicable cybersecurity risks.

**A facility has incorporated cybersecurity into their FSA/FSP before the end of the implementation period, but the Captain of the Port has determined that cybersecurity is not adequately addressed. Should a discrepancy be issued to the facility?**

The implementation period has been established to provide industry with time to evaluate and incorporate cybersecurity into their FSA and FSP. This period of time allows for discussion between facility owners/operators and the COTP to work towards acceptable documentation. Discrepancies during the implementation period are not recommended, though the COTP ultimately has the responsibility to ensure the safety and security of the port.

**Is there any training for owners, operators, FSOs, or other members of industry?**

There is no Coast Guard-developed or approved training for industry related to cybersecurity requirements. Facility owners/operators are welcome to seek out 3rd parties that are working independently to develop training in this space, but are not required to do so.

**Who will be reviewing the cybersecurity portion of my FSA and FSP?**

The review level of FSA and FSP amendments or annexes will remain at the COTP level, and at Headquarters for ASPs. The review should follow the same self-evaluation methodology and review process already in use. Facility Inspectors will simply be asked to receive cybersecurity amendments and confirm that the facility did make a reasonable attempt to address any cyber systems affecting what is covered under the FSP, and that the facility feels that they have appropriately addressed their cybersecurity vulnerabilities.

**Why the focus on this now?**

Per the National Cyber Strategy (September 2018), maritime cybersecurity is of particular concern because lost or delayed shipments can result in strategic economic disruptions and potential spillover effects on downstream industries. Given the criticality of maritime transportation to the United States and global economy, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote and enhance mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure.

To this end, the Coast Guard worked closely with industry and other government agencies to provide guidance on complying with cybersecurity requirements for MTSA regulated facilities.

**Does this NVIC address cybersecurity for vessels?**

This NVIC addresses MTSA-regulated facilities, though other maritime facilities are welcome to utilize the guidance for their own efforts. The Coast Guard is currently developing separate guidance to address cybersecurity on board vessels.