Talking Points for Mac Wade
Regarding
The
Navigation and Vessel Inspection Circular No. 01-20
(pronounced "Navic")

This NAVIC is simply guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA)- regulated facilities.

Simply put, this NAVIC provides guidance to facility owners and operators with the requirements to assess, document, and address computer system or network VULNERABILITIES. 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.

Although the MTSA regulations are mandatory for facility owners and operators, this NVIC does NOT contain any mandatory provisions. It is simply providing guidelines for mandatory regulations already in place. The NVIC reminds facility owners and operators that they must comply with the existing MTSA regulations related to computer systems and networks, but they have the discretion to determine how best to identify, assess, and address the vulnerabilities of their facility's computer systems and networks.

When cyber security vulnerabilities are identified in the FSA, an owner or operator may demonstrate compliance with the regulations by providing its cyber security mitigation procedures in a variety of formats. The information may be provided in a stand-alone cyber annex to the FSP or incorporated into the FSP together with the physical security measures.

A facility will need to submit an amendment to their respective COTP so that the FSP can be properly amended. You do NOT have to rewrite your FSP.

Beginning 10/01/21, facilities need to incorporate cybersecurity into a FSA and their FSP by their annual audit date (which is based on the facility's FSP approval date), but no later than 10/1/22.

The Port of Morgan City has contracted out with Ms. April Danos, owner of Vibrant Innovative Strategies, to handle the creation of our Cyber Annex (we started and went as far as we could go until we needed additional professional Assistance). Contact information:

April Danos

985-291-2016

Email: AprilDanos@VI-Strategies.com

Website: VI-Strategies.com

Many of you may know April from her years with Port Fourchon and she, also, works with Stephenson Technologies Corporation

NVIC 01-20 Frequently Asked Questions (FAQs) – Dated 4/29/2022

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 should a MTSA facility owner/operator or Facility Security Officer (FSO) contact if there are questions regarding the NVIC that are not covered here?

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

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

No. 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.

For which regulations does NVIC 01-20 provide guidance?

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 within a Facility Security Assessment (FSA). If vulnerabilities are identified, the applicable section(s) of the Facility Security Plan (FSP) must address the vulnerabilities in accordance with 33 CFR 105.400 and 106.400.

Are there approved standards or third parties that can help with training, education, etc.?

While the Coast Guard does not maintain a list of recommended third parties to help with training and education, facilities are welcome to seek out third parties that are qualified and 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 not a Coast Guard-approved list of cybersecurity standards, though the NIST Cybersecurity Framework is one example that has been widely utilized.

Do MTSA facilities have to rewrite their 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 and submitted to the Local Captain of the Port (COTPs) for review and approval. 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.

Does a form CG-6025 for Facility Vulnerability and Security Measures Summary need to be submitted?

Yes. The requirements for submission of form CG-6025 remain unchanged in light of the incorporation of cyber into the FSA and FSP. In accordance with 33 Code of Federal Regulations Part 105.405(a)(18) and (c), the Facility Vulnerability and Security Measures Summary, Form CG-6025) is required.

What is the deadline for updating FSA and FSPs to address computer systems and networks?

The Coast Guard allowed a 1.5 year implementation period of the cybersecurity requirement, which ended on 09/30/2021. 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.

As of 10/01/2021, facilities are required to submit a cybersecurity FSA and FSP/ASP amendments or annexes by the facility's annual audit date, based on the facility's FSP/ASP approval date.

Captains of the Port 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/ASP submissions are received by the end of the one-year period, no later than 10/01/2022.

A facility has incorporated cybersecurity into their FSA/FSP but the COTP has determined that cybersecurity is not adequately addressed. Should a discrepancy be issued to the facility?

The implementation period should have provided industry time to evaluate and incorporate cybersecurity into their FSA and FSP. FSOs, Facility owners and operators should be engaged in discussion with their COTP to work towards acceptable documentation. Discrepancies are not recommended at this time, though the COTP ultimately has the responsibility to ensure the safety and security of the port. As a reminder, FSA and FSP/ASP cyber annex/addendums need to be submitted by the facility's annual audit date to COTPs but no later than 10/01/2022. After 10/1/2022, discrepancies will follow the same regulatory author as with physical security discrepancies.

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

The review level of FSA and FSP amendments or annexes will remain at the COTP level.

The review should follow the same self-evaluation methodology and review process already in place. Facility Inspectors will receive cybersecurity amendments and confirm that the facility did make a reasonable attempt to address any cyber systems covered under the FSP. The facility should show that they have appropriately addressed their cybersecurity vulnerabilities.

Point of clarification for ASPs:

An Alternative Security Program (ASP) is approved at the HQ level, but individual facility implementation of an ASP is still verified at the COTP level. In the case of the NVIC 01-20 implementation, this means a facility implementing an ASP is still required to submit documentation to the local COTP. MTSA Facilities operating under an ASP must conduct an assessment to incorporate cyber into their site-specific FSA report and the local COTP should verify this has been done. MTSA Facilities operating under an ASP must submit to their local COTP documentation (amendment/ addendum) indicating what mitigating measures the facility has put in place to address those cyber vulnerabilities which were identified within their FSA.

Why 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 and the supply chain.

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 has worked closely with industry and other government agencies to provide guidance on complying with cybersecurity requirements for MTSA regulated facilities. Since the 2018 National Cyber Strategy, the Coast Guard Cyber Strategic Outlook (CSO) was published in 2021, which involves three lines of effort to address cybersecurity issues: (1) Defend and operate the enterprise mission platform, (2) Protect the Marine Transportation System, and (3) Operate in and through cyberspace. More detailed explanation of the role cybersecurity plays in the Maritime Transportation System (MTS) can be found in the hyperlinked CSO.

Does this NVIC address cybersecurity for vessels?

No. This NVIC addresses cybersecurity for facilities. The Coast Guard is currently developing separate guidance to address cybersecurity on board vessels.

Will there be an extension provided to implement NVIC 01-20?

No. The NVIC 01-20 implementation period ended 09/30/2021. The requirement to submit FSP cyber annex/addendums by next audit date but no later than 10/1/2022 remains.

Facility owners/operators should already be engaged with their COTP and cognizant Facility Inspectors regarding cyber annex/addendums submissions, and most especially if a facility owner/operator feels they cannot meet the deadline.

Does the Coast Guard have a template cyber annex/addendum that industry can use to implement the NVIC 01-20?

No. While there is no Coast Guard-approved cyber annex or addendum to the FSP template, there are many frameworks available that can assist in assessing and/or identifying cyber vulnerabilities, conducting the cyber portion of the FSA, and building out the FSP cyber annex or addendum. Additionally, the Coast Guard does have a Job Aid for inspectors that can also be used by industry. This job aid is posted at: Facility Inspector Cyber Job Aid.pdf (uscg.mil)

What cyber training or resources does the Coast Guard recommend to Facility Security Officers (FSO) and other facility security personnel for implementation of NVIC 01-20?

At this time, there are no Coast Guard approved or recommended cyber training(s) for FSOs. FSOs and facility owner/operators are encouraged to seek out and build relationships within their company's IT/technical staffs to continue bridging the cyber knowledge and awareness gaps and to further assist in identifying potential cyber vulnerabilities.

What should an FSO or facility owner/operator anticipate when implementing NVIC 01-20 when they are responsible for multiple MTSA regulated facilities, including facilities across multiple Coast Guard COTP zones?

This process should be approached the same as any other review of a MTSA facility's FSA and FSP/ASP. Facility owners/operators and FSOs are encouraged to engage early and often with applicable COTPs for discussion. Important reminder: every MTSA regulated facility unique or individual vulnerabilities that will need to be addressed specifically in separate cyber annex/addendums. FSOs and facility owners/operators should avoid submitting blanket annex/addendums for multiple facilities, and should work directly with appropriate COTPs to determine if individual facility vulnerabilities have been identified and addressed adequately.

What if a MTSA facility's IT system is controlled remotely, such as at the corporate or enterprise level (not at the facility itself)? In this circumstance, how does the facility owner/operator or FSO adequately identify cyber vulnerabilities within their FSA, and then also address those vulnerabilities within their FSP?

The facility owner/operator or FSO should determine who within their company is responsible for their IT network and systems. It is common, especially within larger organizations, for a facility's IT systems be controlled and managed by an IT department at the corporate or

enterprise level. Historically, IT staff/department may not have had significant engagement or interaction with FSOs or facility level operators/managers. However, this engagement is highly encouraged to adequately conduct the cyber portion of a facility's FSA, and to address cyber vulnerabilities at a facility. Once the FSO, facility owner/operator, and IT staff have jointly identified which vulnerabilities may impact a given facility, and at what level (corporate/enterprise, local, etc.), the FSO should then work with those IT individuals to determine how those vulnerabilities would then need to be addressed within the FSP cyber annex/addendum (in other words, conduct cyber portion of FSA/incorporate cyber into the FSA).

For example, an FSO may determine with the assistance of the company's IT personnel that certain IT policies or plans be included or referenced within the FSP to address known vulnerabilities.

Is a MTSA facility required to provide a network diagram as a part of their FSP?

No. Current law and regulations do not require a network diagram to be included in the FSP.