9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2016-1084]

RIN 1625-ZA39

Navigation and Vessel Inspection Circular (NVIC) 01-20; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

AGENCY: Coast Guard, DHS

ACTION: Notice of availability

SUMMARY: The Coast Guard announces the availability of Navigation and Vessel Inspection Circular (NVIC) 01-20, titled *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*. This NVIC clarifies the existing MTSA requirements related to computer system and network vulnerabilities of MTSA-regulated facilities. It also provides owners and operators of the facilities with guidance on how to analyze these vulnerabilities in their required Facility Security Assessment (FSA) and address them in the Facility Security Plan (FSP).

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice, call or e-mail, CDR Brandon Link, U.S. Coast Guard; telephone 202-372-1107, e-mail Brandon.M.Link@uscg.mil.

SUPPLEMENTARY INFORMATION:

Discussion

As discussed in the United States Coast Guard Cyber Security Strategy, released

in June 2015,[1] and the draft NVIC,[2] published for public comment on July 12, 2017 (82 FR 32189), cyber security is one of the most serious economic and national security challenges for the maritime industry and our nation. Maritime facility safety and security systems, such as security monitoring, fire detection, and general alarm installations increasingly rely on computer systems and networks. While these computer systems and networks create benefits, they are inherently vulnerable and introduce new vulnerabilities.

There are many resources, technical standards, and recommended practices available to the maritime industry that can help with identifying vulnerabilities to facility computer systems and networks and subsequently incorporating those vulnerabilities into FSPs. However, recent Coast Guard experience suggests the maritime industry may not be aware of or utilizing these resources. Therefore, this NVIC recommends how MTSA-regulated facilities can address and mitigate cyber security risks while ensuring the continued operational capability of the nation's Marine Transportation System (MTS).

The Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. 107-295, November 25, 2002, as codified in 46 U.S.C. Chapter 701) addresses the security of the MTS and authorizes the Coast Guard to prescribe regulations. Under the authority of MTSA, the Coast Guard promulgated regulations in subchapter H of Title 33 of the Code of Federal Regulations (CFR). These regulations established general requirements for facility security and provided facility owners and operators discretion to determine the

[1] https://www.uscg.mil/Portals/0/Strategy/Cyber%20Strategy.pdf

[2] The Coast Guard assigns NVICs based on the year and order in which they are issued in the final form. The draft version of this NVIC was assigned NVIC number 05-17. However, since the final version of the NVIC will be issued in the year 2020, we have assigned it a new number 01-20.

details of how they will comply with those requirements.

This NVIC provides recommended practices for MTSA-regulated facilities to address computer system and network vulnerabilities, more commonly referred to as cyber security vulnerabilities.[3] Based on industry comments, the Coast Guard has revised the NVIC and its Enclosures. We revised the NVIC to clarify its advisory nature and applicability. The Coast Guard also changed the title of the draft NVIC Enclosure (1) from *Cyber Security and MTSA: 33 CFR Parts 105 and 106* to *Cyber Security and MTSA.* The Coast Guard made this change because the revised Enclosure (1) consists of two separate sections: the first section advises on the nature and purpose of the MTSA regulations and the second section discusses specific provisions of 33 CFR parts 105 and 106 that may apply to a Facility Security Plan (FSP) if a Facility Security Assessment (FSA) identifies any computer system and network vulnerabilities. In addition, the revised Enclosure (1) clarifies that MTSA regulations in 33 CFR parts 105 and 106 include a facility's obligation to assess cyber security vulnerabilities while retaining the discretion over the ways to address and mitigate them. We note in the Enclosure that MTSA-regulated facilities must comply with MTSA regulations, but it is up to each facility to determine how to identify, assess, and address the vulnerabilities of their computer systems and networks. We added a line about discussing backup means of communication, which are required by 33 CFR 105.235(d) and 106.240(c) and are part of the information considered when developing the FSA. We also corrected two typos on

[3] The existing regulatory requirement for assessing and addressing vulnerabilities to "computer systems and networks" is written broadly enough to encompass the more common term "cyber security" and to account for advances in technology. Under current regulations, facility owners must regularly update their FSAs and FSPs (*see, e.g.*, 33 CFR 105.310, 105.410, and 105.415) to address new or previously unidentified security vulnerabilities.

page 1-4. In the paragraph titled *Security measures for access control*, we corrected the citation from "33 CFR 105.260" to "33 CFR 106.260" and in the paragraph titled *Security measures for restricted areas*, we corrected the citation from "33 CFR 105.265" to "33 CFR 106.265".

The draft NVIC contained an Enclosure (2) titled *Cyber Governance and Cyber Risk Management Program Implementation Guidance*. This Enclosure provided recommended practices, including the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and NIST Special Publication 800-82. For the reasons described below, we have removed Enclosure (2) from the NVIC.

The Coast Guard sought public comments on the draft NVIC's necessity, robustness, and its costs. Specifically, we sought comments on the feasibility of the implementation of the NVIC's guidance, its flexibility and usefulness in addressing the broad scope of vulnerabilities and risk facing regulated facilities, and its ability to remain valid when technology and industry's use of technology changes. In addition, the Coast Guard sought comments on whether this guidance aligned with activities that industry has already implemented. After the 90-day public comment period closed on October 11, 2017,[4] the Coast Guard reviewed and analyzed the comments contained in 25 letters received. Below we summarize and respond to the public comments.

Comments Received

1. Comments on NVIC's Enclosure (2)

Many of the comments described concerns with Enclosure (2). Enclosure (2) described best practices and expectations for all MTSA regulated entities, and cited to the

[4] The Coast Guard extended the initial comment period end date from September 11, 2017, to October 11, 2017 (82 FR 42560).

National Institute of Standards and Technology's Cyber Security Framework (NIST CSF) to promote effective self-governance. Some commenters perceived Enclosure (2) as overly detailed and not suitable for application by small owners and operators. Other commenters suggested that the Coast Guard simply direct all owners and operators to use the NIST framework. Based on these comments, we have concluded that Enclosure (2) created more confusion than benefit for the owners and operators of MTSA-regulated facilities. For example, some commenters mistook the described examples and the framework for recommended parts of an FSA. Others expressed an expectation for more specific recommendations on various technical specifications. Therefore, the Coast Guard has removed Enclosure (2) from the NVIC. However, in response to several comments supporting the NIST CSF, which was discussed in Enclosure (2), we added a sentence to paragraph (2) of the NVIC encouraging the use of the NIST CSF as a means to improve a facility's cyber posture above what is outlined in the NVIC.

2. Comments on flexibility and adaptability.

Many commenters stated cyber security guidance should be flexible and should allow each facility to create solutions that fit its specific needs and changing risks. The Coast Guard agrees. This NVIC does not include a checklist or otherwise prescribe cyber security solutions. This NVIC emphasizes that existing regulations require MTSA-regulated facilities to assess and address vulnerabilities in computer systems and networks and provides guidance on how to mitigate those cyber security vulnerabilities identified in the facility's FSA.

3. ***Comments on the implementation of the NVIC***

A. The draft NVIC stated that once it was finalized, facility owners and

operators could demonstrate their compliance with MTSA regulations by including cyber security risks and a general description of cyber security measures in their FSPs.

In response to that statement, many commenters expressed concerns regarding potential delays in re-inspections and re-approvals of new FSPs, and economic burdens for ports and facilities (including small ports and facilities with a limited number of employees), that might have to perform new FSAs and re-write existing FSPs immediately after the NVIC's issuance. Similarly, one other commenter suggested that a separate cyber section be added to FSAs and FSPs instead of using all other sections for cyber information. One of the commenters also suggested that smaller facilities with a limited number of employees should have more general roles when it comes to cyber security.

The Coast Guard emphasizes this NVIC applies to MTSA-regulated facilities only and does not apply to ports. However, those ports that manage MTSA-regulated facilities are required to ensure that the facilities comply with MTSA requirements.

This NVIC does not impose any new burdens or requirements on MTSA-regulated facilities. As discussed above, current Coast Guard regulatory authority in 33 CFR parts 105 and 106 already requires MTSA-regulated facilities to evaluate their computer system and network vulnerabilities in their FSAs and address them in the FSPs. Thus, all owners or operators of MTSA-regulated facilities, regardless of size, have to comply with MTSA regulations. As the draft NVIC indicated, the owners and operators could comply with the MTSA regulations by either revising current FSPs or attaching a cyber-annex to the FSP. If the owner or operator elects to create a cyber-annex, it would be the only part of the FSP subject to re-inspection and re-approval. Likewise, if the

owner or operator chooses to incorporate cyber security vulnerabilities into the FSP, then only those new parts would be subject to re-inspection and re-approval. The MTSA regulations governing FSP amendments can be found in 33 CFR 105.415 and 106.415.

As to the general roles of employees at small MTSA-regulated facilities, this NVIC does not prescribe individual roles within a facility's organization. It is the facility's responsibility to determine the individual roles of its employees and how they can address cyber security risks identified by the FSA.

Based on comments received, we have revised the final text of the NVIC and Enclosure (1) to clarify the NVIC's advisory nature and a facility's obligations under the MTSA regulations. We also added a sentence to Enclosure (1) stating that the Coast Guard would only review the newly added cyber-annex or FSP parts related to cyber security.

B. The draft NVIC recommended facility owners and operators describe the roles and responsibilities of facility cyber security personnel, and provide facility cyber security information to Coast Guard personnel conducting FSP reviews or approvals.

Based on those recommendations, some commenters expressed concerns about the new methods of evaluation and approval of their FSAs and FSPs; the role and level of cyber security knowledge and training of Coast Guard personnel in reviewing FSAs and FSPs; and the level of knowledge, required qualifications, and duties of a Facility Security Officer (FSO). Some of the commenters also asked the Coast Guard to provide training and conduct exercises for inspectors and port personnel. In addition, the commenters asked if a facility's IT department should become a part of the facility personnel with security duties; if the IT data stored offsite would be subject to the MTSA

requirements; and if an FSA would be expected to extend to the building where critical cyber systems are housed.

This NVIC does not alter the process the Coast Guard uses to conduct FSA and FSP evaluations and approvals. This NVIC provides guidance to facility owners and operators in complying with current statutory and regulatory requirements to assess, document, and address computer system and network vulnerabilities. Therefore, facility owners and operators whose FSAs and FSPs do not currently address cyber security vulnerabilities should revise them in compliance with MTSA regulations, which require the FSAs and FSPs to be re-evaluated and re-approved. Facility owners and operators are encouraged to work with the local Captain of the Port to determine a suitable timeframe for MTSA-regulated facilities to update their FSAs with computer system and network security vulnerabilities.

Some comments suggested that the Coast Guard personnel lacked cyber security knowledge and training necessary to assess cyber security vulnerabilities. The Coast Guard will assess its needs and may address this issue in the future through internal policy or guidance to Coast Guard personnel. However, it remains the legal obligation of the facility owner or operator to assess and address computer system and network vulnerabilities in the FSA and FSP. In our discussion of FSAs in the 2003 final rule, we explained that a facility's security depends in large part on how well the owner or operator assess vulnerabilities that only he or she would know about.[5] The rule requires that those involved in a FSA be able to draw upon expert assistance in variety of areas

[5] 68 FR 60533. In the same paragraph we added that the facility owner or operator must assume that threats will increase against the vulnerable part of the facility and develop progressively increasing security measures, as appropriate.

including current security threats, techniques used to circumvent security measures, and radio and telecommunications systems including computer systems and networks.[6] The Coast Guard believes this includes the expertise needed to self-assess risk and establish security measures to counter the risks involved with a MTSA-regulated facility's computer systems and networks.

The level of cyber security knowledge and training of facility personnel is the responsibility of a facility's owner or operator, as performed through their FSO. The FSO's responsibilities are provided in MTSA regulations, 33 CFR 105.205 and 106.210. They include the responsibility to ensure the completion of an FSA and completeness of an FSP, which should capture all items identified by the FSA, including existing computer system and network vulnerabilities. At this time, the Coast Guard is not planning to provide specific cyber training nor lead cyber exercises for MTSA-regulated facilities or their personnel. However, in May 2018 the Coast Guard, in coordination with the American Bureau of Shipping (ABS) group, created a "Marine Transportation System Cyber Awareness" webinar. The webinar provides basic cyber awareness with a focus on maritime facility and vessel operations and provides personnel at all levels of an organization with an understanding of cyber terms and issues that may be encountered in the MTS. A recording of the webinar is available online.[7] Maritime industry personnel are encouraged to reach out to their local Area Maritime Security Committee (AMSC) Executive Secretaries for additional information on this webinar.

[6] 33 CFR 105.300(d) and 106.300(d).

[7] http://mariners.coastguard.dodlive.mil/2018/06/08/6-8-2018-marine-transportation-system-cyber-awareness-webinar-recording-available-online/

In response to the question regarding a facility IT department's inclusion into facility personnel with cyber security duties, the Coast Guard notes this NVIC is not intended to dictate the structure of a facility organization. Each individual facility should determine its appropriate organizational structure and determine whether making a facility's IT department a part of the security personnel would help the facility address its cyber security risks.

In response to the question about offsite storage of IT data, the Coast Guard agrees with the commenter that the Coast Guard's MTSA jurisdiction ends at the facility's fence-line in the physical domain. The Coast Guard notes that the regulations found in 33 CFR part 105 or 106 are not drafted to exert regulatory control over computer systems physically located outside the regulated facility's footprint (for example, in a building outside the facility footprint where the critical cyber system is housed). However, if an FSA identifies vulnerabilities to the facility, including to the onsite computer systems, originating from or via computer systems and networks outside of the MTSA-regulated facility's footprint, then the owner or operator needs to address how they will mitigate those vulnerabilities.

Based on the comments received, the Coast Guard added text on pages 1-1 and 1-2 of the NVIC's Enclosure (1) to give the facility owners and operators an example of what they should consider within their broad discretion in addressing their facility cyber security vulnerabilities, including the facility's structure, and its personnel training, roles and responsibilities.

C. Several commenters stated that the NVIC should be revised to use only common cyber security language, and reference specific standards (for example, the

International Association of Drilling Contactors (IADC) Guidelines for Assessing and Managing Cyber Security Risks at Drilling Assets, and IADC Guidelines for Network Segmentation) to assist owners and operators in addressing computer system and network vulnerabilities.

The Coast Guard recognizes the draft NVIC interchangeably used various terms such as, "cyber systems," "cyber risks," "cyber/computer system security," and "cyber security." We agree that the NVIC should use common cyber security language. Based on these comments, the Coast Guard revised the NVIC and its Enclosure (1) to clarify the meaning of provisions of 33 CFR parts 105 and 106. These MTSA regulations require facilities to evaluate their radio and telecommunication equipment, including computer systems and networks, for vulnerabilities. These provisions require facility owners and operators of MTSA-regulated facilities to analyze cyber security vulnerabilities within their facilities.

In regard to the use of specific cyber security references and standards, the Coast Guard encourages facilities to use the NIST CSF, but does not prescribe any particular references or standards at this time. This is to avoid limiting facility owners and operators in the ways they may address computer system and network vulnerabilities at a specific facility. The Coast Guard did not make any edits to the text of the final NVIC in regards to specific references or standards. However, in response to several public comments supporting the NIST CSF, we added a sentence to paragraph (2) of the NVIC encouraging the use of the NIST CSF as a means to improve a facility's cyber posture.

D. The draft NVIC's Enclosure (1) recommended facility owners and operators establish security measures to control access to the facility.

Based on that recommendation, some industry commenters expressed concerns about the NVIC's focus on physical security rather than cyber security. At the same time, other commenters indicated that MTSA was meant to address only physical security of computer systems and networks and did not apply to cyber security.

MTSA requires that security plans address both physical security and communications systems, to deter to the maximum extent practicable a transportation security incident.[8] MTSA regulations in 33 CFR parts 105 and 106 require MTSA-regulated facilities to analyze their "radio and telecommunications equipment, including computer systems and networks."[9] As such, the FSAs must identify vulnerabilities to the facility computer systems and networks, and, if any exist, the FSP must address mitigation for those identified vulnerabilities. Moreover, in the time since the Coast Guard solicited public comment on the draft NVIC, Congress has amended MTSA to explicitly state that FSAs and FSPs must cover cyber security risks.[10] We disagree with assertions that the existing requirement to assess vulnerabilities to computer systems and networks refers only to physical security. In addition to the plain language of "computer systems and networks" used in the 2003 rule, the preamble to the rule specifically

[8] 46 U.S.C. 70103(c)(3). We note that Congress was aware of cyber security issues as early as the 1980s, and specifically addressed viruses and Trojan horses the year after passing MTSA. See, *e.g.*, the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030 (1986) (addressing malicious code and hacking, and under which successful prosecution was brought in the early 1990s for damage caused by Internet-based worms); and the CAN-SPAM Act of 2003, 15 U.S.C. 7701, 7703(c)(1) (2003) (aiming to curb spam email containing viruses, spyware, and other malicious code).

[9] See 33 CFR §§ 105.305(c)(1)(v), 105.400(a)(3), and 105.405(a)(17) for Facilities and 33 CFR §§ 106.305(c)(1)(v), 106.400(a)(3), and 106.405(a)(16) for Outer Continental Shelf Facilities.

[10] Maritime Security Improvement Act of 2018, sec. 1801 *et seq*., Pub. L. 115-254, 132 Stat. 3186 (2018) (the Act is Division J of the FAA Reauthorization Act of 2018). The Coast Guard views this as a reaffirmation and an indication of congressional emphasis, rather than a new authority – a view supported by the House Report accompanying an earlier version of the Act, which said the language is clarifying and "removes ambiguity" as to the Coast Guard's authority under MTSA (H. Rep. No. 115-356 (2018)).

discussed camera monitoring as an alternative to human patrols, showing that the Coast Guard had contemplated electronic systems as part of the facility security systems covered by the rule.[11] The existing regulatory text contemplates a regularly updated plan for responding to existing and developing threats the facility owner or operator identifies. When developing an FSA the facility security officer is expected to either be able to, or draw upon third parties that have expertise to, identify security vulnerabilities, including vulnerabilities to computer systems and networks.[12] This requirement has been in place since 2003. It is not limited to physical threats, and the preamble said that the facility owner or operator must assume that threats will increase, and must develop progressively increasing security measures as appropriate.[13] While initial FSAs and FSPs did focus primarily on physical security issues because those were readily identifiable, the Coast Guard has continually raised cyber security as an emerging issue for over a decade[14] and the NVIC issued today is another form of outreach to industry about this threat to facilities. We think it is clear, therefore, that the existing requirement to assess and mitigate vulnerabilities to computer systems and networks encompasses cyber security.

Moreover, to the extent facility owners and operators have automated physical security measures – for example by controlling access gates with card readers and cameras instead of guards – MTSA's physical security provisions encompass those

[11] 68 FR 60531.

[12] 33 CFR 105.305(c) and (d). In the preamble to the 2003 rule, while discussing current security threats and patterns the Coast Guard stated that "Expertise in assessing risk is crucial for establishing security measures to accurately counter the risk" (68 FR 60515).

[13] 68 FR 60533.

[14] See, *e.g.*, Maritime Transportation System Security Recommendations (October 2005) *available at* https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf ("Use industry outreach to help commercial operators understand what private information could be exploited by terrorists and what cybersecurity controls are appropriate for protecting the information.").

electronic or virtual tools. The regulations specifically enumerate requirements to consider vulnerabilities to access, identification systems, utilities, and similar functions that, if automated, may be vulnerable to cyber security threats. At some facilities, operations and security are so reliant on networks to operate, that cyber security and physical security may be inextricably linked. We recognize that this is not true of all facilities; some facilities may have no computer systems or networks at all. The focus of this NVIC, therefore, is to highlight each facility's responsibility to determine the existence of computer and network vulnerabilities and address them in their FSAs and FSPs.

In response to these and other similar comments, the Coast Guard made clarifying changes to both the NVIC and its Enclosure (1). We added a sentence linking computer systems and networks to the term "cyber security." We indicated that vulnerabilities in computer systems and networks, as referenced in 33 CFR parts 105 and 106, mean cyber security vulnerabilities. We also noted that it was up to each facility to identify, assess, and address the vulnerabilities of their computer systems and networks.

E. Three commenters asked the Coast Guard to recommend specific cyber security technology (including state-of-the art market cyber security solutions) that a facility would need to have, and steps it would need to take, to implement the guidance described in the NVIC. At the same time, some commenters noted that mandating specific cyber risk management tools would not benefit MTSA-regulated facilities as those tools would not be tailored to each individual site.

This NVIC is not intended to inform facilities which cyber security technology they need to use. Rather, it is intended to offer awareness of MTSA regulatory

requirements while allowing each facility the discretion to determine the best way to assess and address any computer system and network vulnerabilities. The NVIC does not mandate that facilities use specific cyber security technology or take specific actions to mitigate a computer system or network vulnerabilities. It simply reminds facility owners and operators of existing MTSA regulations that require the assessment of computer system and network vulnerabilities in their FSAs and incorporation, where applicable, in their FSPs. Therefore, for an owner and operator of an MTSA-regulated facility to comply with the MTSA regulations referenced in the NVIC, they would need to ensure the FSA assesses and FSP addresses computer system and network vulnerabilities of their facility. Based on these comments, the Coast Guard added clarifying language in the final NVIC and its Enclosure (1). We stated that it is up to each facility to identify, assess, and address the vulnerabilities of their computer systems and networks.

F. The draft NVIC's Enclosure (1) recommended that facility owners and operators describe additional cyber-related measures to be taken during changes in MARSEC levels.

In response to that recommendation, several commenters stated that requiring enhanced cyber security measures as a result of a MARSEC level increase would be impractical, and asked the Coast Guard to eliminate this expectation of the facilities. One of the commenters also asked the Coast Guard to inform the industry on the level of cyber security and any necessary response, as it does for physical security, including changes in MARSEC levels.

Although both 33 CFR 105.230 and 33 CFR 106.235 require facility owners and operators to implement additional security measures in the event of a MARSEC level

change, the Coast Guard agrees that it may not always be practical to do the same with cyber security. Some changes in MARSEC level could involve cyber security threats but others may not, and a change in cyber security posture may not always be appropriate. In response to public comments, the Coast Guard revised the NVIC's Enclosure (1) to remove the language related to changes in MARSEC levels and references to 33 CFR 105.230 and 106.235. Under existing regulations including those at 33 CFR 105.405 and 106.405, however, the FSP must indicate how the facility will respond to a changing MARSEC level.

G. The draft NVIC's Enclosure (1) indicated that if any cyber security vulnerabilities were identified in an FSA, owners and operators could choose to provide that information in a variety of formats, such as a stand-alone cyber annex to an FSP, or by incorporating the vulnerabilities into the existing FSP. In response to this statement, some commenters expressed confusion regarding multiple formats in which the Coast Guard will require an incident report. The Coast Guard notes that an FSA, a stand-alone cyber annex, or an amendment to an approved FSP addressing computer system or network vulnerabilities, are documents completely separate from a cyber-incident report. This NVIC addresses MTSA cyber security requirements related to FSAs and FSPs. For more information on reporting a cyber security incident, please consult the CG-5P Policy Letter 08-16 titled "Reporting Suspicious Activity and Breaches of Security," available at https://homeport.uscg.mil. The Coast Guard did not revise the NVIC in response to these comments because this NVIC does not impose any new reporting requirements on owners and operators of MTSA-regulated facilities.

H. The draft NVIC's Enclosure (1) stated that security patches should be

installed as they become available.

One commenter had a question as to the intervals with which security patches should be installed at their facility.

The draft NVIC's Enclosure (1) indicated that it was best to install security patches as they became available. The Coast Guard notes that facilities can choose the intervals with which to install security patches. However, waiting for scheduled intervals to install security patches and other updates instead of performing such actions immediately provides opportunities for system exploitation. However, we have modified the paragraph titled *Security systems and equipment maintenance* in the NVIC's Enclosure (1) to clarify that cyber-related procedures for managing software updates and patch installations should be described in the FSP.

I. One commenter asked about reporting a cyber security incident to a police department as an alternative to the established reporting requirements.

Contacting a local police department does not meet the reporting requirements described in the MTSA regulations at 33 CFR 101.305 ("Reporting"). As noted above, the requirements for reporting suspicious cyber related activity or breaches of security for MTSA-regulated entities are outlined in CG-5P Policy Letter 08-16 titled "Reporting Suspicious Activity and Breaches of Security," available at https://homeport.uscg.mil.

J. Because the draft NVIC referred to various responsibilities of facility employees, two commenters expressed concerns about access facility employees may have to sensitive information and requested more clarity on the access process for such employees. One of the commenters also expressed concerns over making a company's cyber security program more vulnerable to attack by including it into an FSP. Two other

commenters specifically asked about the interplay between this NVIC and the Coast Guard's TWIC regulations. Another commenter was concerned about the Coast Guard interfering with facility business models, which reflect facility operations.

MTSA regulations require the inclusion of computer system and network vulnerabilities into an FSA and an FSP (See 33 CFR 105.305(c)(1)(v) and 105.405(a)(17) for Facilities and 33 CFR 106.305(c)(1)(v) and 33 CFR 106.405(a)(16) for OCS Facilities). This NVIC simply reminds owners and operators of the existence of MTSA regulations related to computer system and network vulnerabilities. These requirements are intended to reduce security risks, not create them. Although the process of granting access to facility employees was not meant to be addressed in this NVIC or prescribed by the Coast Guard, we note that it should be determined by each facility depending on its specific cyber security risks. This NVIC does not change any legal requirements including the existing requirements to operate in accordance with TWIC requirements (see, *e.g.*, 33 CFR 105.115(c)).

As to the comment regarding the inclusion of a facility's cyber security risks into an FSP, the Coast Guard notes that FSPs are considered Sensitive Security Information under 49 CFR 1520.5(b), which can only be accessed by a covered person with a need to know. The risk of adding cyber mitigation measures to an FSP is not higher than the risk currently posed for FSPs that address physical security mitigation measures. FSPs are not released to the public by the Coast Guard,[15] nor should they be released by the facilities.

In regard to the comment about the interplay between TWIC regulations and this NVIC, the Coast Guard notes that this NVIC has no direct impact on the TWIC

[15] See 33 CFR 105.400(c) and (d) and 33 CFR 106.400(c) and (d).

regulations. MTSA-regulated facilities should continue to follow current TWIC regulations as written.

We also note that this NVIC is not intended to interfere with facility business models, but reminds facility owners and operators of their responsibilities under the MTSA regulations, which are meant to help keep their facilities safe from transportation security incidents, including Transportation Security Incidents (TSI) caused by cyber security vulnerabilities.

We made no changes to the final NVIC in response to these comments.

K. Two commenters asked to see a national and port vulnerability assessment for better understanding of the Coast Guard's expectations for individual operators.

The Coast Guard does not believe that a national or port vulnerability assessment is necessary for an individual facility to assess its own cyber security vulnerabilities to comply with MTSA regulations. However, local AMSCs led by Coast Guard Captains of the Port, acting in their capacity as Federal Maritime Security Coordinators, address, discuss, and share maritime security information with the industry. The Coast Guard highly encourages personnel with security duties at MTSA-regulated facilities to participate and collaborate with local AMSCs to gain more insight into port level security issues.

The Coast Guard made no changes to the final NVIC in response to these comments.

4. Comments on the enforcement of the NVIC

The draft NVIC's Enclosure (1) noted that the italicized text of the enclosure

provided general guidance on MTSA regulations that may apply to an FSP, if an FSA identifies any computer system and network vulnerabilities

Based on that statement, many commenters believed the NVIC contained mandatory language. Some of those commenters also asked to clarify the purpose of the italicized text, and how the Coast Guard intended to enforce the NVIC and allocate its resources for this purpose.

The Coast Guard clarifies that the NVIC itself is an advisory document and is not subject to enforcement as a regulation. MTSA regulations, however, are enforceable. Although the Coast Guard will not change the enforcement process as a result of the NVIC, we will verify that facility FSAs and FSPs address cyber security vulnerabilities as required by 33 CFR 105.305(c)(1)(v), 33 CFR 105.400(a)(3), 33 CFR 105.405(a)(17), 33 CFR 106.305(c)(1)(v), 33 CFR 105.40(a)(3), and 33 CFR 106.405(a)(16).

The purpose of the bold text in Enclosure (1) is to provide the industry with a list of regulatory citations that may apply to a facility's FSP. The Coast Guard's recommendation on each regulatory citation, for both FSA and FSP, is contained in italics under each citation.

Based on these comments, the Coast Guard has revised the NVIC and its Enclosure (1) to clarify that although the MTSA regulations in 33 CFR parts 105 and 106 are mandatory, it is up to each facility to identify, assess, and address the vulnerabilities of their computer systems and networks. We also added a sentence to the introduction of Enclosure (1) to explain the purpose of the italicized text.

5. Comments suggesting new provisions or clarifying language

A. Several commenters asked the Coast Guard to add cyber security

recommendations on monitoring activity. In response to these comments, the Coast Guard added the paragraph titled *Security measures for monitoring* to Enclosure (1) of the NVIC.

B. The draft NVIC's Enclosure (1) stated that facility owners and operators may utilize a security plan under the Alternative Security Program (ASP).

In response to that statement, one commenter stated that requiring a focused cyber security plan to go through the ASP program would require facilities to design their own access control, restricted area, cargo handling, and other measures that are not directly related to cyber security. One other commenter suggested that the Coast Guard should allow amendments to the FSP to be submitted under an ASP at the time of the next scheduled revision of the ASP. One of the commenters also asked to clarify if a facility could reference their existing cyber security plan documents as an alternative to the Coast Guard's review.

The ASP does not require a detailed cyber security plan. Nor does it impose any new or different requirements. The ASP is an option that owners and operators may use to comply with the MTSA regulations. In response to the comment about referencing an existing cyber security plan, we note that a facility owner or operator may reference other documents in the ASP, but they would need to be reviewed and considered in the Coast Guard's approval of the ASP.

We revised the NVIC's Enclosure (1) to clarify that the information contained in the NVIC also applies to the ASP, per 33 CFR 101.120(b), which means that the Coast Guard will accept documentation showing equivalent levels of security required by MTSA regulations.

C. Some commenters asked us to use different wording in various parts of the NVIC and its Enclosure (1), and we discuss those changes here.

1. "*[P]revent unauthorized loading/unloading cargo*" instead of "prevent cargo that is not meant for carriage from being accepted"; we made that change.

2. "FSPs are in place and are *considered* to be appropriate and effective" instead of "FSPs are in place and are *believed* to be appropriate and effective"; we made that change.

3. "Describe how those systems are protected and an alternative means of communication *as well as the communication responsibility* should the system be compromised or degraded" instead of "describe how those systems are protected and an alternative means of communication should the system be compromised or degraded." We made this change with some modifications.

4. "Describe cyber-related procedures for interfacing with vessels to include any network interaction, portable media exchange, or wireless access sharing or *remote vendor servicing*" instead of "Describe cyber-related procedures for interfacing with vessels to include any network interaction, portable media exchange, or wireless access sharing." Similarly, another commenter suggested that we add the term "remote access" before the words "portable media exchange" in the original sentence. We added the term "remote access" and believe it captures the intent of both commenters.

5. "Describe cyber-related procedures for managing software updates and patch installations of systems used to perform or support functions identified in the FSP (e.g. identification of needed security updates, planning and testing of patch installations)" instead of "Cyber systems used to perform or support functions identified in the FSP

should be maintained, tested, calibrated, and in good working order (e.g., conduct regular software updates and install security patches as they become available)." We made this change.

6. "Describe how cyber security is included as part of personnel training, policies and procedures *and how the cyber security training material will be kept current and monitored for effectiveness"* instead of "Describe how cyber security is included as part of personnel training, policies and procedures." We added language about keeping training material current.

7. Another commenter asked the Coast Guard to add the following sentence to the paragraph titled "Communications" in Enclosure (1): "During crew or shift changes, handover notes should include cyber security related information and updates." The Coast Guard agrees that this recommendation may be useful to other facilities. We have added this recommendation as an example under the paragraph titled "Communications" in Enclosure (1).

8. One of these commenters also asked us to add the following sentence "*In case gaps are identified, corrective actions should be taken in order for the provisions in the FSP to be satisfied*." to the end of "The audit should include the name, position, and qualification of the person conducting the audit." We did not incorporate the new audit sentence into the NVIC because it is expected that the FSPs should account for gaps in security.

D. One commenter requested that we add guidelines applicable to MTSA-regulated vessels.

The Coast Guard notes this NVIC was not meant to address vessels. It addresses

MTSA-regulated facilities only. We will consider addressing cyber security vulnerabilities for vessels in the future.

Based on this comment, we have revised the text of the final NVIC to clarify its applicability to MTSA-regulated facilities only.

E. Another commenter asked us to clarify where the abbreviation "N/A" was supposed to be placed as asked in the following sentence of Enclosure (1): "If the area or function has no cyber nexus, indicate "N/A."

We have added the clarification as requested and added the following to the end of the sentence: "'N/A" *in the FSA and FSP*."

F. The Coast Guard was also asked to re-number the draft NVIC's Enclosure (1) to preserve traditional NVIC formatting, which we have done.

G. Five commenters asked us to clarify the definition of the term "general documentation" in the paragraph titled *MTSA regulations in 33 CFR parts 105 and 106* in the NVIC's Enclosure (1).

The Coast Guard used the term "general documentation" to indicate that owners and operators would not have to use any specific forms or indicate the use of any specific technology when demonstrating compliance with the MTSA regulations. In addition, the Coast Guard's intent was to highlight that facility owners and operators could use an ASP to submit documentation showing equivalent levels of security required by MTSA.

Based on these comments, we deleted the word "general" from Enclosure (1) and added a footnote stating "[i]n addition, facility owners and operators may rely on the Coast Guard Alternative Security Program to submit documentation showing equivalent levels of security required by MTSA."

H. Three other commenters requested a clarification of security requirements for ports, transportation sector facilities, seaport systems, offshore facilities, and individual operators, based on their operating environment.

We note that this NVIC was not intended to address security requirements for ports, transportation sector facilities, or seaport systems. This NVIC applies to MTSA-regulated facilities, including offshore facilities, and individual operators subject to MTSA. The NVIC's Enclosure (1) references MTSA regulations that may apply to MTSA-regulated facilities, depending on a facility's operating environment and structure. It is each facility's responsibility to determine what computer system and network vulnerabilities may be created by their operating environment and address those vulnerabilities in their FSAs and FSPs.

Based on these comments, we have revised the final text of the NVIC and its Enclosure (1) to clarify the NVIC's applicability.

I. Two industry commenters asked the Coast Guard to provide additional language on Global Positioning Systems (GPS) and Internet of Things (IoT) devices**.** Specifically, one of the commenters asked the Coast Guard to include into the NVIC the following language: "A powerful but little recognized method of cyberattack, GPS disruption can disable end-use devices, interfere with communications links, and provide hazardously misleading information to users and databases. Because GPS signals undergird nearly every technology, DHS officials have called GPS a single point of failure for critical infrastructure."

If GPS systems or IoT devices present a vulnerability to a MTSA-regulated facility's computer or network system, they fall within the existing regulations at 33 CFR

parts 105 and 106, and should be addressed in the FSP. However, these concerns are broad and, in the case of IoT, still developing, and so we don't think it is appropriate to devote a section of the NVIC to them at this time.

Therefore, the Coast Guard did not make edits to the text of the final NVIC based on these two comments

J. One other industry commenter asked for the NVIC to address the risks of third party contractor access to critical cyber systems and networks.

These concerns are valid. However, it is up to the owner or operator of a particular facility to determine if a third party having access to the facility's computer systems and networks presents a risk that should be mentioned in the facility's FSA and FSP.

We made no changes to the final NVIC in response to this comment.

K. Three commenters suggested that we classify MTSA facilities as "critical control systems/controls" and require them to be air-gapped from business network systems. Two other commenters requested more clarity on mitigation of cyber security risks.

This NVIC is not meant to impose requirements on the owners and operators of MTSA-regulated facilities or suggest specific ways cyber risks should be mitigated. This NVIC is meant to make facility owners and operators aware of the existence of the MTSA regulations, which are meant to assist them in protecting their facilities. It is up to each facility to determine if computer system and network vulnerabilities existing at the facility require air-gapping to mitigate vulnerabilities.

We made no changes to the final NVIC in response to this comment.

6. Other comments about the NVIC

A. The draft NVIC stated: "[u]ntil specific cyber risk management regulations are promulgated, facility operators may use this document as guidance to develop and implement measures and activities for effective self-governance of cyber vulnerabilities."

Based on these statements, two commenters expressed concerns as to the Coast Guard's regulatory authority to control how companies execute their cyber risk management and its authority to issue this NVIC without a notice of proposed rulemaking (NPRM). Another commenter asked the Coast Guard to perform a risk assessment and cost benefit analysis as a next step in the NVIC's development.

The Coast Guard acknowledges the comments and notes that this NVIC is not a rule. As explained in detail earlier in this notice, the Coast Guard is also not using its regulatory authority to issue this NVIC or control how companies execute their cyber risk management decisions. To the contrary, this NVIC constitutes advisory guidance meant to assist facility owners and operators in complying with existing MTSA regulations. The NVIC emphasizes that a facility is already obligated by existing MTSA regulations to assess and address vulnerabilities in computer systems and networks, but it has discretion to determine how it will comply with the regulations and address its own cyber security risks.

Based on these comments, we have revised the text of the NVIC and its Enclosure (1) to clarify the advisory nature of the NVIC.

B. The U.S. Chamber of Commerce asked us to keep the NVIC in the draft form and to have an ongoing dialog facilitating input from industry stakeholders. The

Chamber suggested that the Coast Guard present the NVIC as a voluntary risk management tool, which might become a beacon around which cyber security efforts could orient.

The Coast Guard acknowledges this comment and agrees that the NVIC is a voluntary risk management tool, in that it informs owners and operators about their existing regulatory obligations, and provides suggestions for fulfilling those obligations. However, the Coast Guard believes that finalizing the NVIC will provide owners and operators with needed guidance on how to comply with the MTSA regulations relating to computer and network security. Dialogue about cyber risk management will continue to occur in a variety of forms, and the NVIC provides contact information should the regulated public wish to contact the Coast Guard with questions or concerns.

Based on this comment, we did not make any revisions to the final NVIC.

C. The draft NVIC stated the Coast Guard had the regulatory authority to instruct MTSA-regulated facilities to analyze computer systems and networks for potential vulnerabilities within their required FSA and, if necessary, address those vulnerabilities in their FSP.

In response to that statement, three commenters suggested the Coast Guard state that the facilities, to comply with MTSA, could limit their cyber security measures to those information technology systems and networks that have a direct maritime nexus. One of the commenters also asked the Coast Guard to develop clear guidelines on cyber TSIs and connections to MTSA facilities.

The Coast Guard is vested with authority to verify that MTSA-regulated facilities comply with MTSA regulations, including the ones relating to computer systems and

networks regardless of whether that system or network has a direct maritime nexus. In regards to a TSI and connections to MTSA facilities, the Coast Guard notes that this NVIC was not intended to discuss TSIs. However, we note that a TSI, as defined in 33 CFR 101.105, is not limited to incidents with a specific maritime cause. A TSI may result from a physical or cyber security incident which originates from outside of the maritime environment. For example, plausible TSIs caused by cyber threats could include: deliberate disabling of a facility's fire detection equipment, security cameras, or security locks; a hack or ransomware that leaves such systems inaccessible; damage to computer-controlled ventilation or temperature control features at chemical facilities; or tampering with or disabling the automated supply chain in a way that causes significant economic disruption.

For the reasons stated, we did not make any changes to the text of the final NVIC.

D. The draft NVIC's Enclosure (1) recommended that owners and operators address cyber security vulnerabilities in their FSPs.

In response to that recommendation, some commenters expressed general concerns about regulating fast-paced cyber security demands of the commercial industry, the NVIC's focus on cyber vulnerabilities rather than cyber risk management, and provided a suggestion for the government to protect private companies from cyber-attacks.

These comments are general in nature and do not raise any specific issues within the NVIC. The Coast Guard acknowledges these comments and will consider them as part of the general on-going dialog on how to improve cyber security at maritime facilities. We did not make any changes to the final NVIC based on these comments.

The Coast Guard appreciates all the comments received. We will continue to study this issue in light of the comments received before issuing other notices or policy letters on this matter.

Dated: February 26, 2020.

Karl L. Schultz,
Admiral, U.S. Coast Guard,
Commandant.
[FR Doc. 2020-05823 Filed: 3/19/2020 8:45 am; Publication Date: 3/20/2020]