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

Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20593-7618
Staff Symbol: CG-FAC
Phone: (202) 372-1107

COMDTPUB P16700.4
NVIC 01-20
February 26, 2020

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 01-20

Subj: GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES

Ref: (a) Title 33 of the Code of Federal Regulations (CFR) Subchapter H, Maritime Security

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) provides guidance to facility owners and operators in complying with the requirements to assess, document, and address computer system or network vulnerabilities. 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.

2. DISCLAIMER. This NVIC 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. Not all recommendations will apply to all facilities, depending on individual facility operations. Facility owners and operators may use a different approach that has greater or lesser complexity than this NVIC recommends, if that approach satisfies the applicable legal requirements (*i.e.*, this NVIC does not represent a minimum requirement for compliance).

3. ACTION.

a. Enclosure (1) provides a list of existing MTSA regulatory requirements that may apply once a facility owner or operator identifies computer system and/or network vulnerabilities in

DISTRIBUTION - SDL No. 170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	X	X	X		X									X										X		
C					X																				X	
D				X							X															
E					X									X				X								
F																										
G																										
H						X				X																

NON-STANDARD DISTRIBUTION

the FSA. Enclosure (1) also explains how these requirements relate to cyber security measures, and which measures should be included in an FSP. This list is not exhaustive, but is intended to be an informative guide to updating FSAs and FSPs, taking into account computer system and network vulnerabilities, or cyber security vulnerabilities, as referred to in this NVIC.

b. The Coast Guard also encourages facility owners and operators to apply the standards of National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (version 1.1, dated April 16, 2018) and NIST Special Publication 800-82 to improve a facility's cyber posture.

c. The focus of this NVIC is MTSA-regulated facilities only. This NVIC does not address cyber security vulnerabilities of vessels, ports in general, transportation sector facilities, or seaport systems.

4. DIRECTIVES AFFECTED. None.

5. BACKGROUND.

a. MTSA regulations in 33 CFR parts 105 and 106 provide general requirements for facility cyber security while allowing facility owners and operators the discretion to determine the details of how they will comply. These regulations also give the Coast Guard the authority to review for compliance and approve FSAs and FSPs. The result is that the owners and operators are responsible for assessing cyber security vulnerabilities and ensuring cyber security of their facilities with Coast Guard's oversight and guidance.

b. Although the MTSA regulations are mandatory for facility owners and operators, this NVIC does not contain any mandatory provisions. It constitutes voluntary guidance meant to assist the owners and operators of MTSA-regulated facilities in understanding and complying with the mandatory regulations. 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.

c. The maritime industry continues to increase its use of cyber technology. Facility operators use computers and cyber-dependent technologies for communications, engineering, cargo control, environmental control, access control, passenger and cargo screening, and many other purposes. Facility safety and security systems such as security monitoring, fire detection, and general alarm installations increasingly rely on computers and networks.

d. Collectively, these technologies enable the Marine Transportation System to operate with an impressive record of efficiency and reliability. While these computer and network systems create benefits, they introduce new vulnerabilities that increase risk. Exploitation, misuse, disruption, or simple failure of cyber systems can cause injury or death, harm the marine environment, disrupt vital trade activity, and degrade the ability to respond to other emergencies.

e. There are many resources, technical standards, and recommended practices available to the marine industry that can help with governance of cyber risks. Facility operators should use those resources to promote a culture of effective and proactive cyber risk management. Specifically, facilities are encouraged to be familiar with cyber security guidance released by the NIST.

6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this NVIC and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This NVIC is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion (CATEX) A3 from further environmental analysis in accordance with "Implementation of the National Environmental Policy Act (NEPA)", DHS Instruction Manual 023-01-001-01 (series).

b. This NVIC will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this NVIC must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

7. RECORDS MANAGEMENT CONSIDERATIONS. This NVIC has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not create significant or substantial change to existing records management requirements.

8. FORMS/REPORTS. None.

Karl L. Schultz
Admiral, U.S. Coast Guard
Commandant

Encl: (1) Cyber Security and MTSA

CYBER SECURITY AND MTSA

MTSA regulations in 33 CFR Parts 105 and 106.

Under the current regulations in 33 CFR parts 105 and 106, facilities, including Outer Continental Shelf (OCS) facilities, are required to identify and assess their radio and telecommunication equipment, including computer systems and networks, and update or revise their FSAs and FSPs to address and mitigate any identified vulnerabilities.

This enclosure discusses these regulatory provisions and provides facility owners and operators with compliance guidance. It does not change any legal requirements: facility owners and operators already in compliance with regulatory requirements remain in compliance. This enclosure provides examples and recommendations on how to meet applicable requirements. Notably, the examples and recommendations in this enclosure also do not represent a minimum standard or required level of demonstrated compliance.

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.[1] Vulnerabilities in computer systems and networks are commonly referred to as cyber security vulnerabilities. Under the MTSA regulations, an FSP must address any cyber security vulnerabilities identified in the FSA. This NVIC is intended to assist regulated facility owners and operators in updating FSPs to comply with the existing MTSA regulations. This NVIC is also intended to assist owners and operators in identifying computer systems and networks whose failure or exploitation could cause or contribute to a Transportation Security Incident (TSI).

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. If the owner or operator elects to create a cyber-annex, the new annex would be the only part of the FSP subject to re-inspection and re-approval upon receipt by the Coast Guard. If the owner or operator chooses to incorporate cyber security vulnerabilities into the FSP, only those new parts would be subject to re-inspection and re-approval upon receipt. Facility owners and operators may include a general description of the cyber security vulnerabilities and mitigation measures to be taken. They do not have to identify specific technology or a business model, but should provide documentation on how they are addressing their facility-specific cyber security vulnerabilities.[2]

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

[1] *See* 33 CFR 105.305(c)(1)(v) and 33 CFR 105.405(a)(17) for Facilities and 106.305(c)(1)(v) and 33 CFR 106.405(a)(16) for OCS Facilities.

[2] In addition, facility owners and operators may use a Coast Guard-approved Alternative Security Program (ASP) to submit documentation showing equivalent levels of security required by MTSA.

computer systems and networks. For example, each individual facility should determine the organizational structure; number of employees; the employee roles, responsibilities, and access permissions; and, the employee training needed so that its security personnel can address the facility's cyber security risks. Each facility should also determine how, and where, its data is stored and, if it is stored offsite, whether the data has a critical link to the safety and/or security functions of the facility. If such a critical link exists, the facility should address any vulnerabilities.

Below is a list of MTSA regulations that may apply to an FSP, if an FSA identifies any computer system and network vulnerabilities. Under each of the citations, italicized text provides general and non-exclusive examples of how cyber security vulnerabilities may be identified during the FSA and incorporated into an existing FSP or an FSP's cyber-annex. These are examples: facility owners and operators may use other approaches that have greater or lesser levels of complexity if those approaches meet the regulatory requirement.

Cyber Analysis as part of the FSA:

An FSA is the written assessment required by 33 CFR 105.305 and 106.305 that is based on information of possible threats and vulnerabilities to facilities. A thorough FSA is the foundation for analyzing further applicable requirements of subchapter H ("Maritime Security") in Title 33 of the CFR.

Facility Security Assessment requirements
33 CFR 105.305(d)(2)(v)
33 CFR 106.305(d)(2)(v)
Ensure information on computer systems and networks, including their cyber security vulnerabilities, is provided to the facility's personnel conducting the facility security assessment (FSA), considered in the facility's security analysis and recommendations, and contained in the facility security plan (FSP).

Recommendation to Address Identified Cyber Security Vulnerabilities (as applicable):

Depending on the results of the FSA, this section contains portions of subchapter H that may be applicable.

Security administration and organization
33 CFR 105.200(b)
33 CFR 106.200(b)
Describe the roles and responsibilities of cyber security personnel for the facility, including how and when physical security and cyber security personnel will coordinate activities and conduct notifications for suspicious activity, breaches of security, or heightened security levels.

Personnel training
33 CFR 105.205
33 CFR 105.210
33 CFR 105.215
33 CFR 106.205
33 CFR 106.210
33 CFR 106.215
33 CFR 106.220
Describe how cyber security is included as part of personnel training, policies, and procedures, and how this material will be kept current and monitored for effectiveness.

Drills and exercises
33 CFR 105.220
33 CFR 106.225
Describe how drills and exercises will test cyber security vulnerabilities of the FSP. Facility owners and operators may wish to meet this requirement by employing combined cyber-physical scenarios. In general, drills and exercises must test the proficiency of personnel assigned to security duties and enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

Records and documentation
33 CFR 105.225
33 CFR 106.230
Maintain records of training, drills, exercises, security incidents (including cyber security incidents), and other events. Electronic records should be protected against unauthorized deletion, destruction, or amendment.

Communications
33 CFR 105.235
33 CFR 106.240
Describe how security conditions are communicated to and between vessels and facilities, to the Captain of the Port, and to national and local authorities. To the extent that cyber dependent systems are used to perform this function, describe how those systems are protected, an alternative means of communication, and the personnel communication responsibilities should the system be compromised or degraded.

Describe how physical security and cyber security personnel will communicate cyber security conditions and threats to one another, and how cyber-related suspicious activity and breaches of security will be communicated to the Coast Guard.

During crew or shift changes, handover notes should include cyber security related information and updates.

Describe the backup means of internal and external communications.

Procedures for interfacing with vessels
33 CFR 105.240
33 CFR 106.245
Describe cyber-related procedures for interfacing with vessels to include any network interaction, portable media exchange, remote access, or other wireless access sharing.

Security systems and equipment maintenance
33 CFR 105.250
33 CFR 106.255
Describe cyber-related procedures for managing software updates and patch installations on systems used to perform or support functions identified in the FSP (e.g. identification of needed security updates, planning and testing of patch installations).

Security measures for access control
33 CFR 105.255
33 CFR 106.260
Establish security measures to control access to the facility. This includes cyber systems that control physical access devices such as gates and cameras, as well as cyber systems within secure or restricted areas, such as cargo or industrial control systems.

Describe the security measures for access control.

Security measures for restricted areas
33 CFR 105.260
33 CFR 106.265
Describe measures to limit unauthorized access to all of the restricted areas and systems to include those controlled by cyber networks. Unauthorized access might be possible either by manipulating a cyber-controlled gate, allowing physical access, or by accessing the protected system via cyber means, such as by hacking into files that contain sensitive security information. If the area or function has no cyber nexus, indicate "N/A" in the FSA and FSP.

Security measures for handling cargo
33 CFR 105.265
Describe measures to protect cargo handling to include measures that protect cargo manifests and other cargo documentation to deter tampering, prevent unauthorized loading/unloading of cargo, and prevent acceptance of cargo that is not meant for carriage.

Security measures for delivery of stores
33 CFR 105.270

33 CFR 106.270

Describe measures to protect delivery of vessel stores and bunkers to include procedures that protect electronic files to deter tampering and ensure integrity of stores.

Security measures for monitoring

33 CFR 105.275

33 CFR 106.275

Describe security measures to continuously monitor the facility and its approaches on land and water; restricted areas within the facility; vessels at the facility; and, areas surrounding the vessels.

Facility Security Plan

33 CFR 105.400(a)(3)

33 CFR 106.400(a)(3)

Ensure the FSO develops and implements an FSP that addresses each cyber security vulnerability identified in the FSA.

Audits and security plan amendments

33 CFR 105.415(b)

33 CFR 106.415(b)

Conduct an annual audit of FSPs. Facility owners and operators may choose to conduct the cyber security portion of their audits with either the aid of cyber security specialists from a third party or within the organization. The audit report should clearly indicate that the cyber security provisions detailed in the FSP are in place and are considered to be appropriate and effective. The audit should include the name, position, and qualification of the person conducting the audit.