



Maritime Cybersecurity Assessment and Annex Guide (MCAAG)

January 2023

This publication is available free of charge. More information on the U.S. Coast Guard's efforts in cybersecurity can be found here: [USCG Office of Port & Facility Compliance - Cybersecurity](#), here: [USCG Cyber Command - Maritime Cyber Readiness Branch](#), and here: [USCG Maritime Commons blog](#).

Abstract

The United States Coast Guard (USCG) Navigation and Vessel Inspection Circular (NVIC) 01-20¹ published in February 2020 provides voluntary guidance to facility owners and operators on complying with requirements to assess, document, and address computer system and network vulnerabilities in accordance with 33 Code of Federal Regulations parts 105 and 106, implementing the Maritime Transportation Security Act (MTSA) of 2002.² MTSA regulated facilities are required to name a Facility Safety Officer (FSO), conduct a Facility Safety Assessment (FSA) to identify physical security and cybersecurity vulnerabilities and develop a Facility Security Plan (FSP) to address those vulnerabilities. Facilities may choose to address cybersecurity vulnerabilities within their FSP by way of separate cyber annex, addendum, or other method so long as the requirements within the regulations are met. Facilities may also choose to address cybersecurity vulnerabilities as a part of the renewal process of their existing FSP, which is valid for 5 years and audited annually.

This *Maritime Cybersecurity Assessment and Annex Guide (MCAAG)* provides a recommended, yet voluntary, process for identifying and describing cybersecurity vulnerabilities in the context of an FSA. It provides a format for creating a cyber annex addition to the FSP, which can be used by the FSO in close collaboration with the facility's cybersecurity, information technology and/or operational technology staff.

This voluntary MCAAG was developed in collaboration with maritime industry stakeholders and subject matter experts, along with Coast Guard subject matter experts. Please note, the information in this guide is intended to assist stakeholders in meeting requirements, and the authority to accept and/or approve an FSA and/or FSP remains with the Captain of the Port. Likewise, facility owners and operators are not required to adhere to any specific guidance and may use whatever guidance or tools best meet their needs, so long as the regulatory requirements are met.

Key Words

1. Maritime Transportation Security Act of 2002 (MTSA)
2. Facility Safety Officer (FSO)
3. Facility Security Plan (FSP)
4. Cyber Annex
5. Marine Transportation System (MTS)
6. Maritime Cybersecurity Assessment and Annex Guide (MCAAG)
7. Cybersecurity Officer (CySO)

¹ https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023

² <https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H>

Table of Contents

1	Introduction.....	1
1.1	Caveats.....	2
1.2	Structure of the MCAAG	2
2	MTSA Facilities: Terms and Architectures	3
2.1	Cyber Attacks on IT Systems	7
2.2	Cyber-Attacks on OT & BCS.....	8
3	FSP and Cyber Annex Production Overview.....	9
3.1	Identify a Cybersecurity Officer (Step 1)	9
3.2	Determine Scope (Step 2)	10
3.3	Establish Cybersecurity Vulnerability Definition (Step 3).....	10
3.4	Determine the Cybersecurity Vulnerabilities for the FSA (Step 4)	11
3.5	Create Remediation Plans (Step 5)	13
3.6	Create the Cyber Annex (Step 6).....	14
Appendix A	Cyber Annex Template	16
Appendix B	CSF Cybersecurity Baseline	18
Appendix C	Cyber Annex Implementation Guidance	27
C.1	Facility Security Assessment Requirements	27
C.2	Security Administration and Organization	28
C.3	Personnel Training.....	30
C.4	Drills and Exercises	31
C.5	Records and Documentation.....	32
C.6	Communications	33
C.7	Procedures for Interfacing with Vessels	35
C.8	Security Systems and Equipment Maintenance	36
C.9	Security Measures for Access Control	37
C.10	Security Measures for Restricted Areas.....	39
C.11	Security Measures for Handling Cargo.....	40
C.12	Security Measures for Delivery of Stores.....	41
C.13	Security Measures for Monitoring.....	42
C.14	Facility Security Plan.....	44
C.15	Audits and Security Plan Amendments.....	44
List of Acronyms	46
Glossary	47

List of References..... 50

List of Figures

Figure 1. Example of the Interconnected Systems at a Container Terminal 4
Figure 2. Terminal Network Diagram Example..... 6

List of Tables

Table 1. Facility IT/OT Systems 5

This page intentionally left blank

1 Introduction

The purpose of the MCAAG is to provide voluntary guidance to Maritime Transportation Security Act of 2002 (MTSA) regulated facilities on how to produce a cybersecurity component for the required Facility Security Plan (identified in this guide as a “Cyber Annex”), ensuring alignment with the Code of Federal Regulations (CFR) and supporting guidance, Navigation and Vessel Inspection Circular (NVIC) 01-20.

- The ***goal of MCAAG*** is to provide a voluntary framework for producing a Cyber Annex:
 - That is achievable for the smallest of facilities
 - That is scalable to the largest and most complex of facilities
 - The Cyber Annex should provide Facility Security Officers (FSOs) with assurance the facility’s cybersecurity protections and mitigation efforts are relevant and sufficient regarding the facility’s physical security and safety
- Achieving this goal requires addressing ***three challenges***:
 - What can be done to facilitate effective collaboration between the FSO (who may not have deep cybersecurity experience), and the information technology (IT) and cybersecurity subject matter experts supporting them?
 - How should cybersecurity vulnerabilities and protections be defined?
 - What is the relationship between physical vulnerabilities identified in the Facility Security Assessment (FSA) and the cybersecurity vulnerabilities and protections described in the Cyber Annex?
- To address these challenges, the guidance in the MCAAG is based on ***three primary recommendations***:
 1. **Identify a Cybersecurity Officer (CySO) –**

The FSO should identify a person or group of people who can speak authoritatively about the cyber enabled systems, networks and cybersecurity protections in the facility, and who can partner with the FSO to create the Cyber Annex. The CySO may be a single person from the information technology or cybersecurity organization of the facility, or it may be a group of people. There is nothing precluding the FSO and the CySO from being the same person, provided they have adequate cybersecurity training and knowledge. *Note: while the MCAAG is intended to be accessible to personnel with a minimal cybersecurity background, [Appendix B](#) and [Appendix C](#) provide specific cybersecurity guidance and are written for personnel who have sufficient IT and cybersecurity experience.*
 2. **Define cybersecurity vulnerabilities and protections based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) –**

The concepts of “cybersecurity vulnerability” and “cybersecurity protection” are flexible and can be understood at the level of the cybersecurity program and policy level, the system design and configuration level and all the way down to the level of individual exploitable software flaws and patches in an operating system or application. It is recommended the Cyber Annex addresses vulnerabilities and protections primarily at the programmatic and

policy level. While certain vulnerabilities and protections will require more specific language to be used in the Cyber Annex, NIST CSF subcategories provide a standardized vocabulary that is easily aligned with a facilities cybersecurity programs and policies.

3. **Map physical security vulnerabilities to related cybersecurity vulnerabilities, then map the identified cybersecurity vulnerabilities to cybersecurity protections –**

Two things are true at the same time. On the one hand, the Cyber Annex is not intended to address all possible cybersecurity vulnerabilities in a facility. Instead, it should *at least* address those cybersecurity vulnerabilities related to physical vulnerabilities identified in the FSA in accordance with 33 CFR 105 and 106. On the other hand, the typical way cyber attackers subvert systems directly affecting physical security and safety, is by first gaining access to the facility’s IT systems and then moving through the network until they gain access to their intended target. Thus, credible protection for relevant cybersecurity vulnerabilities can only be achieved if the facility’s network meets or exceeds a minimum level of cyber hygiene.³ To achieve the correct scope of cybersecurity vulnerabilities addressed in the Cyber Annex, the CySO should determine or establish whether all cyber security vulnerabilities necessary to address the physical vulnerabilities have been identified and addressed, and the FSO should determine or establish whether each cybersecurity vulnerability in the Cyber Annex is relevant to the physical vulnerabilities in the FSA.

1.1 Caveats

The MCAAG provides supplemental guidance intended to further support the guidance provided by NVIC 01-20 and associated development of an FSP Cyber Annex. While inclusion and use of the recommendations in the MCAAG does not guarantee acceptance of the Cyber Annex by the Captain of the Port, these recommendations provide guidance on a process for use in creating a Cyber Annex and the kinds of information it should provide.

Any recommendations made within this guide are not new requirements or regulations, but considered *voluntary* guidance for addressing cybersecurity within a FSA and FSP.

1.2 Structure of the MCAAG

- The body of the MCAAG describes a *framework for creating a Cyber Annex*:
 - [Section 2](#) – Provides a discussion of terms and concepts intended to foster effective collaboration between the FSO and CySO
 - [Section 3](#) – Provides an overview of a Cyber Annex development process
- The appendices provide *supplemental reference material*:
 - [Appendix A](#) – Provides a flexible format for completing the Cyber Annex
 - [Appendix B](#) – Provides a CSF-based minimum cybersecurity baseline for the MTS context

³ Cyber hygiene can be defined as “A set of routine practices for using basic security capabilities to mitigate cyber risks due to common or pervasive threats”; The MITRE Corporation, 2021. *Defining Cyber Hygiene to Enable Trade-off Analysis*. Bedford.

- [Appendix C](#) – Provides supplemental threat and cybersecurity implementation guidance that can be considered when identifying cybersecurity vulnerabilities and protections for the Cyber Annex
- [Glossary](#) – Provides a glossary of terms used in the MCAAG

2 MTSA Facilities: Terms and Architectures

A cybersecurity architecture, or network security architecture, is considered the basis of any organization's cyber risk management. It includes tools, policies, processes and technologies used to prevent or mitigate attacks. However, before the architecture can be discussed, a common global language needs to be established to address cyber security issues for port communities.

MTSA regulated facilities vary greatly in size and complexity, and cyber risk management will be unique to each facility; identifying and defining a clear set of baseline terms will facilitate clear and unambiguous communication across organizations and reduce the likelihood of misunderstanding and/or miscommunication. *Part of establishing this common language is identifying who owns the responsibility for understanding and managing the cyber risk management effort.*

Per 33 CFR 105.220, the **Facility Security Officer (FSO)** is responsible for the development, and implementation of the Facility Security Plan (FSP)⁴. Additionally, the FSO must incorporate cybersecurity into an existing security program, including commissioning a cyber security assessment and incorporating the findings into their existing FSA. Findings from the cybersecurity assessment will be used to develop a cybersecurity plan that can be incorporated into the existing FSP.

It is recommended that a **Cybersecurity Officer (CySO)** be identified and tasked with assessing risk and addressing cyber vulnerabilities in the annex of the FSP in collaboration with the FSO. A CySO should have a thorough understanding of the cyber-enabled systems that have an effect on facility security, the networks those systems are connected to, the cyber-threats that affect those systems and networks, and the cyber protections available to the facility.

The remainder of this section is intended to provide a set of common terms and definitions that will facilitate communication between the FSO and the CySO/IT personnel. A reference network architecture of a representative port will be detailed so the FSO will be better prepared to communicate with internal and/or external cybersecurity experts concerning the services required to meet the intent of regulations and standards.

⁴ Ecf.gov. 2022. *eCFR :: 33 CFR Part 105 Subpart B -- Facility Security Requirements*. [online] Available at: <<https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105/subpart-B>> [Accessed 29 June 2022].



Figure 1. Example of the Interconnected Systems at a Container Terminal⁵

The Marine Transportation System (MTS) is a complex, interconnected network of information, sensors, and infrastructure developed over time to promote the efficient transport of goods and services around the globe.⁶ The MTS is continually evolving to increase efficiency and transparency; this technological evolution has created a complex interdependency between the information technology (IT) and operational technology (OT) systems.

IT and OT systems are very different, each system has a unique purpose and relies on different technologies and protocols. Understanding what systems exist in a facility, the associated vulnerabilities for each system, and the consequences for failure, will help the FSO and the CySO coordinate efforts for planning and protecting against cyberattacks. Expanded definitions for IT/OT are provided in the remainder of this section, as well as a list of IT/OT systems commonly found at a maritime facility ([Table 1](#)).

IT is equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data and/or information, to include:

- Directories and authentication
- Business applications and databases
- Records systems
- External Internet Connections

⁵ USCG.mil. 2021. *United States Coast Guard Cyber Strategic Outlook*. [online] Available at: <<https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf>> [Accessed 30 June 2022].

⁶ Ibid.

- Network Infrastructure

OT consists of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). OT includes:

- Supervisory control and data acquisition (SCADA) systems, such as transport and transfer systems
- Automated or semi-automated container handling systems: stacking cranes, ship-to-shore cranes, rail mounted gantries, automated guided vehicles
- Automated container tracking systems
- Vessel communications interface for position, tracking, and navigation (e.g., Automatic Identification System (AIS))

A subset of OT is the **Building Control Systems (BCS)**, which include energy-management systems, physical-security access-control mechanisms (e.g., Transportation Workers Identification Credentials (TWIC) readers), and fire-alarm systems. These systems are directly responsible for safety and security of personnel at the facility and should be separated from other OT systems when laying out the network architecture.

Table 1. Facility IT/OT Systems

Information Technology Systems	Operational Technology Systems
Terminal Operating System	Programmable Logic Controllers (PLC) for Container Handling Equipment
Email Servers	AIS (Automatic Identification System)
Enterprise Resource Planning	CTS (Container Tracking System)
Sales	Ramp Control Systems
Inventory Control	Entry Gate Control
Accounting	Building Control Systems
Web Servers	Interior Lighting Systems
Human Resources	Elevators and Escalators
Telecommunication	Access Control
	HVAC Systems
	Fire Alarm/Sprinkler Systems
	Surveillance Systems/Intrusion Detection

The **network architecture** of a facility refers to the computer networks' structural and logical layout; it describes how the network devices are connected and the rules that govern how data is transferred between them. The computer network will include hardware, physical and wireless connections, communication protocols, and software; a simplified network diagram for a terminal is provided in [Figure 2](#), which illustrates the separation of IT, OT, and BCS using firewalls.

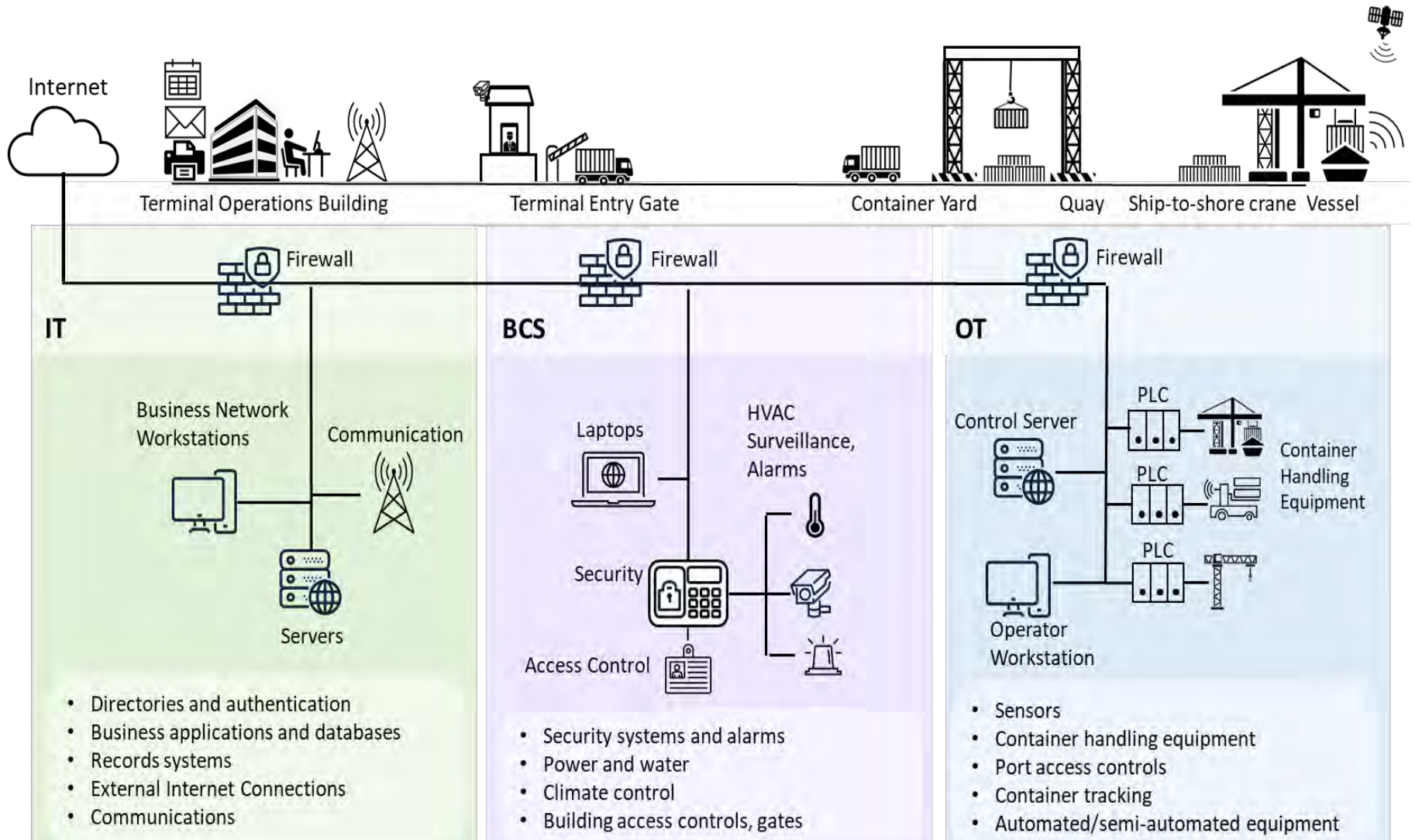


Figure 2. Terminal Network Diagram Example

A recommended best-practice is for IT, OT, and BCS systems to operate on physically separated networks. If this is not operationally feasible, the networks should be logically separated using some form of boundary protection, and extreme care and attention must be used to ensure the boundary protection prevents unauthorized traffic between the networks. A form of boundary protection is a **firewall**, which is a hardware device or software link in a network designed to inspect data traffic between devices, systems, or networks. A firewall can be configured to restrict network traffic according to defined rules. Boundary protection systems such as firewalls are critical, as is providing adequate protections for: email servers, internet-facing web and business application servers, and email clients and web browsers on desktop systems.

2.1 Cyber Attacks on IT Systems

IT systems that connect to the internet provide the most common path for cyber attackers to enter the network and compromise physical security systems. These cyber-attacks can be initiated by either insider threats or external threats.

Insider threats are users who have legitimate authorized access to a company's network and inadvertently or deliberately allow unauthorized access to network system leaving it vulnerable to a cyber-attack. Insider threats are typically current employees who are careless of security policies; compromised personnel who are disgruntled current or former employees; contractors, business partners, or suppliers with system access. Insider cyber-attacks can be initiated remotely through the internet, or locally through physical access to the system.

Internal attacks can be accomplished by compromised personnel who pose an inside threat to IT systems if they can gain physical access to them. Strict physical security measures should be implemented to prevent unauthorized access to cyber enabled systems, (i.e., network connection outlets, physical connections to IT systems (e.g., USB ports), operator terminals and human machine interface (HMI) panels). The systems should be housed in a room that can be secured; barriers such as fences, gates, walls, and doors all act as physical deterrents to criminal entry. Additionally, locks, visible security measures, and signs all increase deterrence of an attack by cybercriminals.

External threats are attackers who focus on obtaining access to protected systems by exploiting vulnerabilities in systems that connect to the internet and then moving through the facility's networks until they gain access to their intended target. To gain initial entry to the facility IT network, attackers will often attempt to manipulate employees that are unaware by deploying phishing emails, malware, or through spear phishing, to name a few examples.

- **Phishing emails** are emails sent by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals.
- **Malware** is software usually inadvertently downloaded from the internet that compromises the operating system of an IT or networked asset with different types of generic or customized malicious code.
- **Spear phishing** is an attack that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss.

Whether the cyber attacker is an internal or external threat, once they gain entry on an IT network, they typically attempt to acquire administrative credentials that will allow them to move laterally to other IT systems and potentially to attack OT systems and the BCS.

2.2 Cyber-Attacks on OT & BCS

OT systems historically were isolated from IT systems, but to stay competitive, some facilities are turning to the integration of OT and IT systems to improve operational efficiency. ***Common IT systems that cross the OT system boundary include, but are not limited to:***

- Enterprising Resource Planning (ERP) – Data is passed between the ERP IT system and OT systems to support inventory control, supply chain management, billing, and scheduling.
- Predictive maintenance – Monitoring of equipment to identify potential failures
- Software and/or firmware updates

OT and BCS failures can result in the loss of control of operational processes which can result in economic impacts, physical consequences, structural damage to equipment or facilities and environmental ramifications. ***Examples of high-profile OT and BCS scenarios include:***

- Equipment damage due to Stuxnet malicious worm causing PLCs within Iran’s nuclear centrifuges to spin too quickly and tear themselves apart
- Safety issue when diver tender station-keeping system on an offshore asset “blue screened” and drifted away, severing the diver umbilical
- Operation downtime when a tidal turbine was hacked, and its operating software was encrypted. The utility was held for ransom, resulting in a 15-day delay.
- Property damage when a German steel mill’s ICS was hacked, disabling the ability to shut down a blast furnace and subsequently resulting in an explosion causing major damage to the facility

Within a port or terminal, consequences for cyber-attacks that result in an OT and BCS failure could include:

- Failure of physical security systems, such as TWICs readers, automated gates, and video monitoring systems
- Failure of safety systems, such as fire suppression, resulting in property damage and loss of life
- Failure of container handling equipment resulting in damaged property and operational downtime
- Failure of communications system causing scheduling back-logs
- Failure of ERP resulting in mishandled or misplaced containers, scheduling conflicts, and/or loss of confidential data

The typical way cyber attackers subvert OT and BCS systems that directly affect physical security and safety is by first gaining access to the facility’s IT systems, and then moving through the network until they gain access to their intended target. ***Thus, protection of the OT network starts***

with the IT network by ensuring the cybersecurity protections for all of the facility's networks meets or exceeds a minimum level of cyber hygiene. A cybersecurity baseline expressed in terms of NIST CSF and based on relevant MTS industry best practices is provided in [Appendix B](#).

3 FSP and Cyber Annex Production Overview

Some physical vulnerabilities identified in an FSA are related to or created by cybersecurity vulnerabilities. The purpose of the Cyber Annex is to describe the facility's cybersecurity plans to address these cybersecurity vulnerabilities.

33 CFR 105, 106 and NVIC 01-20 give the facility tremendous freedom in terms of determining what constitutes a cybersecurity vulnerability in the context of the FSA and how to describe security plan protections to address them.

This section provides guidance on how to define cybersecurity vulnerabilities in the context of 33 CFR 105, 106 and NVIC 01-20, how to describe protections within the facility's cybersecurity plan, and how to combine them both to create a Cyber Annex. *While inclusion of the following recommendations does not guarantee acceptance of the Cyber Annex, these recommendations provide guidance on the kinds of information the facility should provide in the Annex.*

Creating a Cyber Annex can be described in six primary steps. Each of these steps is described in more detail in the corresponding subsections of this section.

➤ **Six Steps to Creating a Cyber Annex:**

[Step 1](#) - Identify a person or committee to act as the CySO in support of the FSO

[Step 2](#) - Identify all cyber-enabled systems and networks related to the physical security vulnerabilities in the FSA

[Step 3](#) - Determine/establish a facility definition of "cybersecurity vulnerability" in the context of the FSA

[Step 4](#) - Gather information necessary to identify cybersecurity vulnerabilities and finalize the list to be addressed in the Cyber Annex

[Step 5](#) - Determine the remediation plan for each vulnerability expressed in terms of cybersecurity protections appropriate for the facility

[Step 6](#) - Use the provided template to document the physical vulnerabilities in the FSP, the cybersecurity vulnerabilities, any relationships between them, and the protections within the facility's cybersecurity plan

3.1 Identify a Cybersecurity Officer (Step 1)

Creating a Cyber Annex requires a thorough understanding of the cyber-enabled systems that have an effect on facility security, the networks those systems are connected to, the cyber-threats that affect those systems and networks, and the cyber protections available to the facility. It is recommended a CySO be identified to provide support to the FSO during the entirety of the Cyber Annex development process. *The CySO may be a single person, a group of people, or the FSO.*

The guidance provided in the MCAAG is intended to aid FSOs in their collaboration with a CySO to produce the Cyber Annex. Portions of this guide, particularly the technical aspects of

some of the appendices, assumes a CySO with the appropriate cybersecurity experience has been identified and is a part of the Cyber Annex development process.

3.2 Determine Scope (Step 2)

Facility security processes and functions are increasingly reliant on computers or computer-based systems, such as networked video monitors and electronic badge systems. Typically, these systems are attached to networks. If these networks are attached to internet, even in an indirect manner, it is possible for cyber-attackers to penetrate the facility's networks and subvert the facility's security processes and functions by disabling or altering the systems they rely upon.

When a physical vulnerability involves one or more cyber-enabled systems, there is a challenge in determining the scope of any cybersecurity plan to protect those specific systems. Most cyber-attacks on facilities involve a cyber attacker making initial entry on a facility network by way of a system that connects to the internet and then moving internally from system to system until they are able to compromise the targeted system. Thus, there is a strong argument to be made that any plan to protect a particular system relies on the protection plan for the entirety of the facility's networks.

- The recommended approach to *determine the scope for the cybersecurity protections* contained in the Cyber Annex is as follows:
 - Identify all cyber-enabled systems associated with physical security controls or physical vulnerabilities
 - Identify the networks these systems attach to. If two networks have a physical network connection between them, consider them to be a single network (even if there are robust boundary protections such as firewalls between them). Note, for many facilities there will be only one network
 - When describing cybersecurity protections to remediate vulnerabilities, describe the plan to protect the network the associated systems operate on

3.3 Establish Cybersecurity Vulnerability Definition (Step 3)

It is strongly recommended that the *FSA and CySO establish and agree upon an approach to define and identify cybersecurity vulnerabilities* in the context of the FSA, and that this approach be reviewed and endorsed by the facility's senior leadership and relevant risk managers. It is recommended that the facility have a formal risk management process by which senior leadership and risk managers can describe acceptable and unacceptable levels of risk and through which the definition of FSA-related cybersecurity vulnerabilities can be determined.⁷

➤ **Two observations may be helpful:**

- NVIC 01-20 asserts that, "It is up to each facility to determine how to identify, assess, and address the vulnerabilities of their computer systems and networks."⁸

⁷ The NIST Risk Management Framework (RMF) is one way for facilities to define and manage risk. See: <https://csrc.nist.gov/projects/risk-management/about-rmf>

⁸ United States Coast Guard. (February 2020). Guidelines For Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.

This means it is up to the FSO and the CySO to determine what should be counted as a cybersecurity vulnerability with respect to the FSA.

- “Cybersecurity vulnerability” is a flexible concept that can be understood at the programmatic and policy level, the system design and configuration level and all the way down to the level of individual exploitable software flaws in an operating system or application.

For example, NIST defines a vulnerability as: “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”⁹

For the purpose of creating a Cyber Annex to support an FSP, it is recommended that **cybersecurity vulnerability** be defined at the program and policy levels, not at the individual system configuration or patch level. For example, if one or more systems critical to the security of the facility are not correctly patched, then possible vulnerabilities to address in the Cyber Annex might include:

- The facility does not have a defined patching policy
- The facility does not have defined patching procedures and/or assigned personnel
- The facility’s patching procedures are not fully implemented

If a facility relies on cyber-enabled systems for its operations and security, then it is critically important it have an adequately defined and staffed cybersecurity program. The cybersecurity program should be able to ensure minimum cyber hygiene practices are implemented on its systems and networks.

For this reason, it is recommended the definition of **cybersecurity vulnerability**, for the creation of the Cyber Annex, include (*but not be limited to*):

- Gaps in the facility’s cybersecurity program relative to the cybersecurity baseline provided in [Appendix B](#) of this guide¹⁰
- Inadequate cybersecurity hygiene protections for cyber-enabled systems that support facility security (e.g., automated gates, video monitoring, personnel training records)
- Inadequate cybersecurity training and/or drills

3.4 Determine the Cybersecurity Vulnerabilities for the FSA (Step 4)

After the FSO and CySO have determined how to define cybersecurity vulnerability (as described in [Section 3.3](#)), effective identification of vulnerabilities can be done in *three steps*:

Step 4(a) - Assemble a team of subject matter experts with adequate knowledge of the facility’s physical security, IT, OT and cybersecurity operations

⁹ Csrc.nist.gov. 2022. *vulnerability - Glossary / CSRC*. [online] Available at: <<https://csrc.nist.gov/glossary/term/vulnerability>> [Accessed 29 June 2022].

¹⁰ The provided cybersecurity baseline is described in terms of NIST Cybersecurity Framework (CSF) subcategories. It is based on NVIC 01-20, MTS related NIST CSF Profiles, and industry cyber hygiene best-practice documents. See [Appendix B](#) for more details.

Step 4(b) - Collect sufficient organizational information to ensure the cybersecurity vulnerability assessment team has adequate visibility and awareness

Step 4(c) - Collaboratively compile a list of cybersecurity vulnerabilities and cross-reference them to the physical security vulnerabilities in the FSA

Assembling a team of subject matter experts ([Section 3.4, Step 4\(a\)](#)) with the necessary persons to include in the cybersecurity vulnerability identification does not come without challenges. It is possible a FSA may not completely or adequately identify the facility's cybersecurity vulnerabilities associated with the FSA physical security vulnerabilities. *Identifying the cybersecurity vulnerabilities that have a bearing on the FSA, requires strong collaboration between stakeholders with strong knowledge of the facility's **physical security operations** and those with strong knowledge of the supporting **IT, OT and cybersecurity operations**.*

To sufficiently **gather information** ([Section 3.4, Step 4\(b\)](#)), the following are recommended:

- **Conduct a CSF self-assessment** that covers the cybersecurity practices for each network.¹¹ If the cybersecurity of the networks is managed separately, it is recommended to conduct separate, parallel self-assessment for each.
- **Identify cyber-enabled systems** that support facility security as discussed in NVIC 01-20 and the originating CFRs including (*but not limited to*):
 - Web Servers
 - Domain Controllers
 - Databases
 - File Shares
 - Email Servers
 - Records System for Training & Incidents
 - Other Business Applications
 - User Endpoint Computers
 - Boundary Firewalls
 - Routers
 - Network Architecture (Segregation)
 - Wireless Access Points
 - VPN Access
 - Vessel Communication Interface
 - Cyber-Enabled Physical Security Systems
 - Cargo Handling Systems
 - Vessel Stores and Bunkering Systems

¹¹ The Facility Cybersecurity Framework Core Assessment is one of many free CSF-based self-assessment tools. See: <https://facilitycyber.labworks.org/assessments/coreAssessment>

- Physical Monitoring Systems
- **Identify personnel (or roles or offices) responsible** for monitoring and reporting security and cybersecurity incidents to approved internal and external recipients.
- **Identify all training and drills** involving cybersecurity, physical access to computer systems, and facility security processes supported by cyber-enabled systems.

Lastly, the final *identification of cybersecurity vulnerabilities* ([Section 3.4, Step 4\(c\)](#)) should be approved by both the FSO and the CySO. The CySO should be satisfied the list is complete and all relevant cybersecurity vulnerabilities that have a bearing on the physical security vulnerabilities identified in the FSA have been considered. The FSO should be satisfied each cybersecurity vulnerability listed is relevant and important to one or more of the FSA physical security vulnerabilities.

3.5 Create Remediation Plans (Step 5)

Each vulnerability addressed in the Cyber Annex should be accompanied by a plan to remediate it. In the same way it is recommended to describe vulnerabilities at the programmatic, policy and procedure level (as opposed to the system configuration or patch level), it is recommended protections be articulated at the same level. For the purpose of the MCAAG, the term **cybersecurity protection** (or simply, protection) will be defined as a discrete unit of a facility's cybersecurity protection plan¹². Examples of cybersecurity protections include, but are not limited to cybersecurity:

- Program capabilities
- Policies
- Procedures

It is possible for new cybersecurity protections to have unintended negative consequences on the facility's critical functions, including its security and safety. For this reason, the FSO and CySO should form teams of subject matter experts with strong operational knowledge of the systems and networks involved. *Ideally, all newly proposed cybersecurity protections should be reviewed and approved according to the facility's established, agreed upon and documented approval and risk management processes.*

➤ Resources to aid in the selection of new cybersecurity protections:

- First, [Appendix B](#), provides a recommended cybersecurity baseline for cybersecurity programs expressed in terms of the NIST CSF. If a CSF-based self-assessment of the facility reveals gaps in the facility cybersecurity program relative to the minimum baseline, then it is recommended the facility consider implementing the missing CSF subcategories as a part of its cybersecurity plan.
- Second, [Appendix C](#) provides more specific guidance in addressing cybersecurity vulnerabilities relative to physical vulnerabilities that may be identified in the FSA. This guidance summarizes the related cybersecurity threats typically associated with

¹² The term **protection** is intentionally defined loosely to provide facilities with maximum flexibility in the level of detail they provide in their Cyber Annex.

the topic, provides possible cybersecurity protections that could be applied, and links to associated CSF-subcategories from the provided cybersecurity baseline.

In many cases, there will be a many-to-many relationship between cybersecurity vulnerabilities and new cybersecurity protections. *A single protection may help remediate multiple vulnerabilities, and the remediation of a single vulnerability may require multiple new security plan protections.* For this reason, it recommended the FSO and the CySO collaborate, establish and *agree upon* a traceability matrix that maps cybersecurity vulnerabilities to their associated new cybersecurity protections.

3.6 Create the Cyber Annex (Step 6)

33 CFR 105.405 (a) requires that an FSP either be organized according to 22 individual, specified sections, or provide an index for the required sections within the FSP.¹³ This organizational structure is mirrored by the 15 guidance statements listed in NVIC 01-20.

While these categories are applicable to organizing the physical security vulnerabilities addressed in the FSP, the many-to-many relationships between physical security vulnerabilities and their related cybersecurity vulnerabilities, and between cybersecurity vulnerabilities and their associated cybersecurity protections, makes it difficult to organize the Cyber Annex according to these categories without introducing duplication.

[Appendix A](#) provides a recommended format for a Cyber Annex designed to both simplify the Cyber Annex while making clear the relationships between the physical security vulnerabilities in the FSA and the cybersecurity protections in the Cyber Annex.

➤ The recommended **Cyber Annex template** is structured as follows:

- **List the physical security vulnerabilities** from the FSA and FSP with identifiers and organized according to the categories specified in 33 CFR 105.405 (a)
 - ✓ Alternatively, list the FSA vulnerabilities with identifiers and provide a traceability matrix between them and the categories specified in 33 CFR 105.405(a)
- **List the cybersecurity vulnerabilities** to be addressed in the Cyber Annex with identifiers
 - ✓ Provide a traceability matrix between the cybersecurity vulnerabilities and their associated physical security vulnerabilities
- **List the cybersecurity protections** that will collectively address the identified cybersecurity vulnerabilities
 - ✓ Provide a traceability matrix between the cybersecurity protections and the cybersecurity vulnerabilities they remediate
 - ✓ Provide a traceability matrix between the cybersecurity protections and NIST CSF subcategories

¹³ Ecf.gov. 2022. *eCFR :: 33 CFR Part 105 -- Maritime Security: Facilities*. [online] Available at: <<https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105>> [Accessed 29 June 2022].

Appendix A Cyber Annex Template

This appendix provides a recommended format for a Cyber Annex designed to both simplify the Cyber Annex while making clear the relationships between the physical security vulnerabilities in the FSA and the cybersecurity protections in the Cyber Annex. While inclusion of the following recommendations does not guarantee acceptance of the Cyber Annex, these recommendations provide guidance on the kinds of information to be provided. **Any recommendations within this Appendix A are not new requirements or regulations but are considered voluntary guidance in the development of a Cyber Annex.**

➤ The recommended **Cyber Annex template** is structured as follows:

- **List the physical security vulnerabilities** from the FSA with identifiers (i.e., “PV.1”, “PV.2,” etc.) and organized according to the sections specified in 33 CFR 105.405 (a).

- ✓ Alternatively, list the FSA vulnerabilities with identifiers and provide a traceability matrix between them and the categories specified in 33 CFR 105.405(a)

- ✓ For example:

Physical vulnerabilities (PV) identified in the FSA:

PV.1: <first physical vulnerability>

PV.2: <second physical vulnerability>

...

PV.N: <nth physical vulnerability>

- **List the cybersecurity vulnerabilities** to be addressed in the Cyber Annex with identifiers (i.e., “CV.1”, “CV.2, etc.). For each cybersecurity vulnerability, list the associated physical vulnerabilities they contribute to. Alternatively, express the relationship between physical vulnerabilities and their associated cybersecurity vulnerabilities in the form of a traceability matrix. If the traceability matrix is large, it can be provided as a supplemental attachment in spreadsheet form.

- ✓ Provide a traceability matrix between the cybersecurity vulnerabilities and their associated physical security vulnerabilities

- ✓ For example:

Cybersecurity vulnerabilities (CV) as determined jointly by the FSO and CySO and/or identified by FSA:

CV.1: <first cybersecurity vulnerability>

<list of associated physical vulnerabilities>

CV.2: <second cybersecurity vulnerability>

<list of associated physical vulnerabilities>

...

CV.N: <nth cybersecurity vulnerability>

<list of associated physical vulnerabilities>

- **List the cybersecurity protections** that will collectively address the identified cybersecurity vulnerabilities
 - ✓ Provide a traceability matrix between the cybersecurity protections and the cybersecurity vulnerabilities they remediate
 - ✓ Provide a traceability matrix between the cybersecurity protections and NIST CSF subcategories

List all protections within the cybersecurity plan to address the cybersecurity vulnerabilities. Similar to the recommendations on how to define a cybersecurity vulnerability, it is strongly recommended the cybersecurity protections be described in terms of cybersecurity program elements and policy. NIST CSF subcategories provide a robust standard vocabulary for cybersecurity protections at this level. If it is beneficial to define some protections at a more granular level than a CSF subcategory (similar to or derived from the guidance provide in [Appendix C](#)), associate those protections with the appropriate CSF subcategory.

For each protection, list the cybersecurity vulnerabilities the protection helps to remediate. Alternatively, express the relationship between cybersecurity vulnerabilities and their associated cybersecurity protections in the form of a traceability matrix. If the traceability matrix is large, it can be provided as a supplemental attachment in spreadsheet form.

Appendix B CSF Cybersecurity Baseline

This appendix provides a recommended cybersecurity baseline expressed in terms of the NIST CSF subcategories. CSF subcategories provide a vocabulary for describing areas of functionality in a cybersecurity program.

The baseline is based on the CFRs, NVIC 01-20, NIST published MTS-related CSF profiles and a variety of industry best practices.¹⁴



➤ **The baseline can be used in two ways in the development of a FSP Cyber Annex:**









- It can be used as a *basis for conducting a CSF-based self-assessment* to identify cybersecurity programmatic gaps to be listed as cybersecurity vulnerabilities in the FSP Cyber Annex as discussed in [Section 3.4](#)
- And/or, it can be used to *describe new cybersecurity protections to address* the cybersecurity vulnerabilities, as described in [Section 3.5](#)



➤ **The baseline is described at three levels:**

- A *minimal level* of cybersecurity is provided by the subcategories designated as “*minimum baseline*” and are denoted with **green** colored dots in the table below
- An *enhanced level* of cybersecurity is provided by implementing the “*additional supporting*” subcategories, which are denoted in the table with **amber** colored dots
- An *optimal level* of cybersecurity is provided by implementing the **entirety** of the CSF subcategories



¹⁴ The MITRE Corporation, 2021. *Defining Cyber Hygiene to Enable Trade-off Analysis*. Bedford.

-  Minimum Baseline
-  Additional Supporting

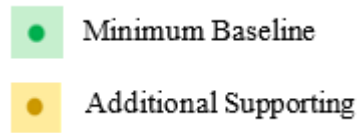
Function	Category	Subcategory	Recommended MTS Baseline
IDENTIFY (ID)	<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.</p>	ID.AM-1: Physical devices and systems within the organization are inventoried	
		ID.AM-2: Software platforms and applications within the organization are inventoried	
		ID.AM-3: Organizational communication and data flows are mapped	
		ID.AM-4: External information systems are catalogued	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	
	<p>Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	ID.BE-1: The organization’s role in the supply chain is identified and communicated	
		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are</p>	ID.GV-1: Organizational cybersecurity policy is established and communicated	
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	

-  Minimum Baseline
-  Additional Supporting


Function	Category	Subcategory	Recommended MTS Baseline
Function	understood and inform the management of cybersecurity risk.	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	●
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	
		ID.RA-3: Threats, both internal and external, are identified and documented	●
		ID.RA-4: Potential business impacts and likelihoods are identified	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●
		ID.RA-6: Risk responses are identified and prioritized	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	●
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	●


-  Minimum Baseline
-  Additional Supporting










Function	Category	Subcategory	Recommended MTS Baseline
	implemented the processes to identify, assess and manage supply chain risks.	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	●
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	●
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	●
		PR.AC-2: Physical access to assets is managed and protected	●
		PR.AC-3: Remote access is managed	●
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	●
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	●
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	●
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)	●
	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	●
		PR.AT-2: Privileged users understand their roles and responsibilities	●
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	●



Function	Category	Subcategory	Recommended MTS Baseline	
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		PR.AT-4: Senior executives understand their roles and responsibilities	●	
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	●	
		PR.DS-1: Data-at-rest is protected	●	
		PR.DS-2: Data-in-transit is protected	●	
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●	
		PR.DS-4: Adequate capacity to ensure availability is maintained		
		PR.DS-5: Protections against data leaks are implemented	●	
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity		
		PR.DS-7: The development and testing environment(s) are separate from the production environment	●	
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity		
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	●
			PR.IP-2: A System Development Life Cycle to manage systems is implemented	
			PR.IP-3: Configuration change control processes are in place	●
			PR.IP-4: Backups of information are conducted, maintained, and tested	●
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met			●	
PR.IP-6: Data is destroyed according to policy			●	
PR.IP-7: Protection processes are improved				


 Minimum Baseline


 Additional Supporting

Function	Category	Subcategory	Recommended MTS Baseline	
DETECT (DE)		PR.IP-8: Effectiveness of protection technologies is shared		
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed		
		PR.IP-10: Response and recovery plans are tested		
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)		
		PR.IP-12: A vulnerability management plan is developed and implemented		
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools		
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access		
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy		
		PR.PT-2: Removable media is protected and its use restricted according to policy		
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities		
		PR.PT-4: Communications and control networks are protected		
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations		
	DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	
			DE.AE-2: Detected events are analyzed to understand attack targets and methods	


Function	Category	Subcategory	Recommended MTS Baseline
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	
		DE.AE-4: Impact of events is determined	
		DE.AE-5: Incident alert thresholds are established	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	●
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	●
		DE.CM-4: Malicious code is detected	●
		DE.CM-5: Unauthorized mobile code is detected	●
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●
		DE.CM-8: Vulnerability scans are performed ¹⁵	●
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	●
		DE.DP-2: Detection activities comply with all applicable requirements	
		DE.DP-3: Detection processes are tested	
		DE.DP-4: Event detection information is communicated	
DE.DP-5: Detection processes are continuously improved			
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident	●


¹⁵ It is not recommended to run active vulnerability scans on OT networks, particularly those with safety instrumented systems, to minimize the risk of unintentionally causing disruptions.



 Minimum Baseline

 Additional Supporting

Function	Category	Subcategory	Recommended MTS Baseline
Response	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed	●
		RS.CO-2: Incidents are reported consistent with established criteria	●
		RS.CO-3: Information is shared consistent with response plans	●
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	●
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	●
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	
		RS.AN-2: The impact of the incident is understood	
		RS.AN-3: Forensics are performed	
		RS.AN-4: Incidents are categorized consistent with response plans	
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	●
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained	
		RS.MI-2: Incidents are mitigated	
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	●
		RS.IM-2: Response strategies are updated	●

 Minimum Baseline

 Additional Supporting

Function	Category	Subcategory	Recommended MTS Baseline
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	
		RC.IM-2: Recovery strategies are updated	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed	
		RC.CO-2: Reputation is repaired after an incident	
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	

Appendix C Cyber Annex Implementation Guidance

The following recommendations are provided as supplemental background information. They are intended to aid and guide the FSO and CySO as they collaborate on reviewing the facility's cybersecurity program and preparing a cybersecurity plan to address the cybersecurity vulnerabilities in the Cyber Annex. **Any recommendations within Appendix C Cyber Annex Implementation Guidance are not new requirements or regulations, but are considered voluntary guidance for implementing NVIC 01-20 and associated regulations within 33 CFR parts 105 and 106.**

- **For each statement within Enclosure (1) of NVIC 01-20, this section discusses:**
 - **Threat Summary** – The cybersecurity threats associated with the NVIC 01-20 statement
 - **CSF Baseline Guidance** – Related CSF-subcategories from the provided baseline for consideration
 - **Sample Additional Cybersecurity Protections** – Implementation recommendations to consider as possible additional cybersecurity protections

This appendix is organized according to the guidance statements in NVIC 01-20. To use this appendix, it is recommended to map the physical security vulnerabilities addressed in the FSP to the NVIC guidance statements, and then refer to the corresponding subsection of this appendix to determine the associated cybersecurity vulnerabilities and to develop cybersecurity protections to remediate them.

C.1 Facility Security Assessment Requirements

A Facility Security Assessment 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.

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)*

Threat Summary

- Facilities that conduct FSAs or author FSPs that are not based on accurate or timely information can contain undiscovered physical security and cybersecurity vulnerabilities that can be exploited by attackers

CSF Baseline Guidance

- Implement PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, ID.GV-2 to establish roles and responsibilities of personnel involved in facility assessments. This includes post-assessment activities (e.g., amending response and recovery plans).

- Implement RS.RP-1, RS.IM-1, RC.RP-1, RC.IM-1 to ensure FSP considers cybersecurity vulnerabilities and risk tolerances
- Implement ID.AM-6 and ID.GV-2 to ensure the information is provided to the facility's personnel conducting the FSA
- ID.AM-1 and ID.AM-2 need to be implemented as a prerequisite to accomplish the NVIC 01-20 statement.

Sample Additional Cybersecurity Protections

- Ensure cybersecurity roles and risk management address cybersecurity risks
- FSO is informed of assessment results/reports and has awareness of cyber-physical and network vulnerabilities that could impact the facility
- FSOs and IT Manager or Cybersecurity Personnel coordinate to develop response and recovery processes and procedures with respect to identified cyber vulnerabilities
- IT Staff or Cybersecurity Personnel are involved in facility assessments and physical inspections
- Operational personnel are involved in facility assessments and physical inspections
- Assessments include physical infrastructure of networks and network connected operational security equipment
- Credentials and audit logs for physical and network access are maintained
 - Establish processes to routinely assess or evaluate suppliers or third-party partners accessing facility IT/OT networks

C.2 Security Administration and Organization

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

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*

Threat summary

- Facilities with insufficient cybersecurity processes can be compromised by cyber attackers which can lead to loss of proprietary data, financial loss, the inability to operate, and physical harm to personnel, the public, the physical plant, and the environment
- The increasing reliance on cyber technologies in operational and building control systems demands traditional physical security/safety and cybersecurity work together as a comprehensive whole

- Cyber attackers most often gain access to OT and BCS networks by first gaining access to the organization's IT network. Blended attacks involving coordinated cyber and physical attacks are possible.
- Conversely, gaining physical access to IT, OT, or BCS systems can give cyber attackers the ability to easily compromise them. So, weaknesses in the physical security of the systems can lead to cyber penetration of IT systems.

CSF Baseline Guidance

- It is recommended the cybersecurity roles for the IT, OT, and BCS networks meet or exceed those identified at the "baseline" level
- Practices and roles at the "recommended" level provide higher levels of protection and should be considered
- Implement at a minimum ID.AM-1, ID.AM-2, ID.SC-2, ID.SC-3, ID.SC-4, DE.CM-7, baseline PR.AC controls (PR.AC-1 through PR.AC-7), PR.IP-1, PR.PT-1 to encompass controls needed to ensure the facility's cybersecurity program addresses critical control areas for cyber-physical systems
- Implement ID.AM-6 to establish cybersecurity roles and responsibilities of facility personnel
- Apply DE.CM baseline controls (DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-7, DE.CM-8) to monitor facility environment for potential cybersecurity events
- Apply RS.CO-1, RS.CO-2, RS.CO-3 to establish communication processes and procedures between FSO, CySO, or other identified relevant parties during raised IT cybersecurity threat levels and observed incidents
- Implement RS.RP-1 and RC.RP-1 to ensure the facility initiates response and recovery plans following notifications of suspicious activity, breaches of security, or heightened security levels

Sample Additional Cybersecurity Protections

- Perform a CSF-based self-assessment for the facility's IT, OT, and BCS networks to ensure the security program meets or exceed the provided "baseline" level
 - This guide provides a recommended cybersecurity baseline based on industry best practices for MTS facilities and expressed in terms of NIST CSF subcategories that can be used to identify and organize the organization's cybersecurity roles.
- Ensure that facility's cybersecurity programs for its IT, OT, and BCS networks provide adequate implementation of the following critical control areas for all cyber-enabled systems:
 - Maintain lists of approved hardware devices and software
 - Perform regular hardware and software asset inventories
 - Detect, log, and remove/isolate unapproved hardware and software
 - Ensure all hardware and software are currently supported by their vendor

- Have a process to identify, test, and deploy firmware updates, software updates, and patches using automated distribution tools when available
- Ensure all default passwords set by the manufacturers of hardware and software have been changed
- Ensure dedicated administrative accounts are used for all administrative tasks
- Establish secure configurations are established, approved, implemented and audited for
- Enable, store, and regularly review audit logs
- The FSO (or their delegates) should monitor information sources to track physical threats and security levels and to monitor security incidents and communicate those to the IT cybersecurity team
- The CySO (or their delegates) should identify and communicate IT cybersecurity threat levels and observed incidents to the FSO
- The organization should clearly identify the thresholds for which kinds of events and incidents should be internally communicated

C.3 Personnel Training

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

- 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*

Threat summary

- Improper or inadequate cybersecurity training for personnel can lead to cybersecurity breaches.

CSF Baseline Guidance

- Apply PR.AT baseline controls (PR.AT-1 through PR.AT-5) to all system roles (IT, OT, BCS)
- Understanding of cybersecurity roles and responsibilities, through application of ID.AM-6, must be established prior to carry out the personnel training required in this NVIC 01-20 statement

Sample Additional Cybersecurity Protections

- Ensure all training has a person (or role or office) responsible for its execution, a schedule for execution, and records of completion
- Consider the use of online personnel training systems that can deliver different training modules to different types of personnel, track completion rates, and store results
- Training should address the different levels of access personnel have, such as: physical access, authenticated operator, system administrator
 - Ensure all personnel with physical access to the facility understand the physical attack vectors for cyber-enabled systems and how to protect them; including, consoles, HMIs, network access points (e.g., ethernet outlets), removable device connection ports (e.g., USB ports, CD readers)
- Training should address different cybersecurity practices for IT, OT, and BC systems
- FSO and CySO should have a shared understanding of the physical location of all cyber related systems and networks, which personnel have access of any kind, and the scheduling and efficacy of the cybersecurity training received by personnel

C.4 Drills and Exercises

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

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*

Threat Summary

- Insufficient awareness of cyber security vulnerabilities may result in a higher likelihood of an attacker targeting systems/devices and establishing a foothold onto the facility's network
 - Access or manipulation attempts through user interaction (e.g., spear-phishing, social engineering) can compromise user accounts and the facility's cybersecurity posture
- Lack of drills and exercises to test organizational and personnel readiness may lead to inadequate ability to detect, respond, and prevent targeted attacks

CSF Baseline Guidance

- Apply PR.AT baseline controls (PR.AT-1 through PR.AT-5) to ensure personnel can identify and respond to cyber-physical scenarios demonstrated in drills and exercises
- Implement RS.IM-1 and RC.IM-1 to ensure response and recovery plans reflect outcomes from drills and exercises

Sample Additional Cybersecurity Protections

- Establish schedule for regular drills and exercises
- Define personnel involved and their role/responsibilities
 - IT Staff, operations personnel, and physical security personnel are included in drills and exercises to test cyber vulnerabilities identified in the FSP
- Development of organizational cybersecurity policy and the FSP is informed by or updated to reflect results from drills and exercises
- Prior to drills/exercises, FSO and IT personnel will coordinate to plan specifics of cyber-physical scenarios. IT personnel will lead participants through the scenario during drills.
- Prior to drills/exercises, FSO and Operations personnel coordinate to plan specifics of the drill to test cybersecurity awareness of operational staff.

C.5 Records and Documentation

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

33 CFR 105.225

33 CFR 106.230

- ✓ *Maintain records of training, drills, exercises, security incidents (including cybersecurity incidents), and other events*
- ✓ *Electronic records should be protected against unauthorized deletion, destruction, or amendment*

Threat Summary

- Inadequately trained users, operators, and administrators may be susceptible to threat actors (e.g., spear phishing). Attackers may access systems to compromise the confidentiality, integrity, or availability of electronic records. They may access or exfiltrate sensitive information (e.g., client, cargo, or proprietary data) risking facility or MTS operations.
- Ransomware attacks can cause operational delays until the facility can restore systems and data

CSF Baseline Guidance

- Apply PR.AT baseline controls (PR.AT-1 through PR.AT-5) to ensure personnel can identify a potential campaign/attack and know how to respond accordingly

- Implement ID.AM-1, ID.AM-2 to ensure the facility maintains an inventory of systems and software that hold electronic records and need to be protected
- Implementation of PR.IP-4, PR.IP-6 ensures the facility has adequate data retention policy and backups of electronic records
- Implementation of PR.DS-1, PR.DS-5 protects the integrity and confidentiality of the electronic records
- Implement PR.AC baseline controls (PR.AC 1 through PR.AC-7) to prevent unauthorized modification of records

Sample Additional Cybersecurity Protections

- Ensure integration of records system into related processes
 - Maintain an inventory of electronic record systems
- Electronic records systems should be protected by application of complete cybersecurity program (CSF)
- Facilities have an established policy, process, or procedure to review, transfer, share, alter, etc., the records to ensure data quality is maintained
- Facilities establish a data retention policy. Records or data are categorized and classified with data protection measures applied relevant to the categorization
- All relevant cybersecurity training, events and incidents are recorded; including, CSF referenced PR.AT controls, logging and incident management records

C.6 Communications

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

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*

Threat Summary

- Unreported physical security incidents can lead to successful cyber attacks
- Unreported cybersecurity incidents can lead to physical security and safety breaches
- Unreported physical security and cybersecurity incidents in facilities can lead to physical security or cybersecurity incidents at other MTS facilities and vessels and at the regional or national level

CSF Baseline Guidance

- Implement ID.AM-6 cybersecurity roles and responsibilities are established as it pertains to who needs to be involved and what needs to be communicated between stakeholders (e.g., FSO, CySO, COTP, national and local authorities)
- Apply PR.AT baseline controls for understanding of roles and responsibilities
- Apply at a minimum RS.CO-1, RS.CO-2, RS.CO-3 for communications of cybersecurity conditions and threats between the facility, Coast Guard, and relevant stakeholders. Additional recommended controls RS.CO-4, RS.CO-5 may be implemented to achieve the NVIC 01-20 statement
- Apply PR.IP-9, RS.RP-1, and RC.RP-1 to ensure response and recovery plans reflect processes and procedures for communications of cybersecurity related information and updates
- For protection of cyber dependent systems carrying out communications activities:
 - Implement ID.AM-1 to identify facility communications systems that should be protected
 - Apply PR.PT-4, PR.PT-5, and DE.CM-1 to ensure protection and availability of cyber-dependent communication systems, and communication and control networks

Sample Additional Cybersecurity Protections

- Cyber-dependent communication systems should be identified and protected
- Cyber-dependent monitoring systems and analysis (hand-off notes) systems should be identified and protected
- Monitoring and communication systems crossing any boundaries between the IT, OT, BC, and external networks should be identified, and the systems and communication paths should be protected
 - Network security best practices include physical separation of IT, OT and BC networks
- Response and recovery plans include processes and procedures for sharing information and reporting incidents internally and externally.
- Physical and cybersecurity personnel understand their roles and responsibilities through training and testing

- Personnel exchange cybersecurity related information and updates during daily activities (e.g., shift change), and in the event systems are compromised

C.7 Procedures for Interfacing with Vessels

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

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*

Threat Summary

- Compromised systems aboard vessels or in port facilities could propagate through interconnectivity between vessels and facilities sharing Wi-Fi, network connections, or removable media
- Lack of physical or logical segmentation may allow an attacker to access sensitive systems and information

CSF Baseline Guidance

- Apply PR.AC-3 to manage remote access during interface/network interactions
- Implement PR.PT-2 to ensure portable media restrictions are in place and applied when interfacing between facilities and vessels
Apply ID.AM-6, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4 to establish roles and responsibilities for communicating vulnerabilities internally and externally
- Implement PR.DS-2 and PR.PT-4 for protection of data transmitted through the networks
- Implement DE.CM-1 to ensure identification of vulnerabilities on the networks for shore-to-ship connections

Sample Additional Cybersecurity Protections

- Assume vessel networks, systems and media are compromised by an advanced, persistent threat (APT)
- Facilities protect communication and control networks by employing measures such as:
 - Disallowing portable media
 - Establishing isolated trusted paths
 - Monitoring externally and internally managed interfaces
 - Implementing network segregation for publicly accessible components
 - Maintaining a baseline of network operations and expected data flows and interactions between vessels and facilities.
- Include risks of connecting to onshore networks during DOS process

- FSOs and Vessel Security Officers (VSOs) coordinate to determine actions to address cybersecurity concerns, including communicating suspicious or anomalous activity for network operations
- Limit connections between vessels and terminal Wi-Fi
 - Do not have open wireless networks
 - Implement password-enabled system or establish guest accounts on a separate wireless network for incoming vessels
 - Implement authentication control/restricted privileges for remote access
- Encrypt data transmitted on the network between facilities and vessels through encryption protocols
- Manage updates and patches for access point software
- FSO and IT staff identify network vulnerabilities and threats (i.e., to information security and quality of communication service)

C.8 Security Systems and Equipment Maintenance

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

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*

Threat Summary

- Unpatched systems or systems not regularly tested for patch status can contain known vulnerabilities that can be used by cyber attackers to compromise or take control of systems
- Unauthorized devices and software are not regularly updated and can contain vulnerabilities or unauthorized functionality that can be used by cyber attackers
- Inadequately tested patches can negatively impact the performance of critical systems
- Poorly planned or executed patch installations can disrupt critical systems and business processes
- Patch installation on some OT and BC systems may require physical access which could allow a malicious insider or contractor to compromise the system via the use of removable media or a maintenance laptop

CSF Baseline Guidance

- Apply ID.AM-1 and ID.AM-2 for an inventory of approved hardware devices and software in the facility and its relevant information (e.g., owner, authorization date)

- Apply DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-7 to monitor facility networks for potential cybersecurity events or suspicious activity related to facility software and systems
- Apply Baseline ID.SC (ID.SC-2, ID.SC-3, ID.SC-4) baseline controls for software updates and patch installations required on third party systems that will be done by their suppliers
 - Implementation of ID.SC-1 supports implementation of the baseline ID.SC controls
- Apply PR.DS-3 to ensure the management of systems during removal (i.e., if they no longer support software updates or patches), transfers, or dispositions
 - Management may include identifying the software or systems and logs of approvals/deployment of patches

Sample Additional Cybersecurity Protections

- Inventory all cyber-enabled systems in the facility and identify the system owner, last authorization date, the network its authorized for (IT, OT, BCS), and its assigned physical location
- Utilize network monitoring tools to detect devices and confirm they are authorized. Have processes to remove or quarantine unauthorized systems
- Maintain a list of approved software. For the sake of this inventory, consider hardware firmware as software. Consider software that is automatically installed by operating system but that can be uninstalled as separate software. For each approved software:
 - Specify which devices (or sets of devices) it is authorized to run on
 - Verification that it is currently supported by the vendor (unsupported software should not be approved)
 - The personnel (or role) responsible for managing and updating the software
- For each approved and managed software:
 - Have policies, procedures, and assigned personnel to identify and test new software patches or updates
 - Have policies, procedures, and assigned personnel to deploy patches either by automated means (preferred) or manually (if necessary)
- For each cyber-enabled system, have policies, procedures and assigned personnel to:
 - Inventory the software installed, preferably using automated tools
 - Determine if the patch/update status is current, preferably using automated tools

C.9 Security Measures for Access Control

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

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*

Threat summary

- Cyber attackers can remotely control cyber-enabled building control and physical security systems as a part of a blended cyber-physical attack. For example, a cyber attacker could unlock gates and disable cameras to allow a physical attacker to gain unauthorized access. Alternatively, a cyber attacker could lock automated doors and disable fire suppression systems to maximize damage from a physical attack.
- Physical attackers (which can include malicious insider personnel) who gain unauthorized physical access to computer systems and networks can initiate cyber-attacks on those systems and networks, particularly via computer consoles, HMIs, removable media connections (e.g., USB), or network connections (e.g., Ethernet jacks).

CSF Baseline Guidance

- Apply PR.AC controls (PR.AC-1 through PR.AC-7) to ensure access to the facility and its physical and cyber systems is limited to authorized users, processes, and devices
 - For identification of cyber-dependent physical access control systems and potential attack vectors, ID.AM-1 and ID.AM-2 needs to be implemented as a prerequisite
 - Implement PR.AC-5 and PR.PT-4 for facility network protections
 - Implement DE.AE-1 for management of the facility network baseline
- Apply RS.CO baseline controls (RS.CO-1, RS.CO-2, RS.CO-3) to establish roles and responsibilities and processes and procedures for reporting cyber incidents
 - Application of additional recommended control DE.DP-1 may supplement cybersecurity and physical teams in establishing detection thresholds

Sample Additional Cybersecurity Protections

- Cyber-dependent physical access control systems should be identified and protected including but not limited to:
 - Automated doors and gates
 - Video monitoring cameras
 - Badge readers
 - Physical security operator stations
 - Cyber-enabled power control systems
- Physically exploitable computer and network access points should be identified and protected including but not limited to:
 - Computer consoles
 - HMIs

- Removable media connections (e.g., USB)
- Network connections (e.g., Ethernet jacks)
- Wireless networks
- Physical security management systems that cross any boundaries between the IT, OT, BC, and external networks should be identified and the systems and communication paths should be protected
 - Network security best practices include physical separation of IT, OT, and BC networks
- The cybersecurity team should establish thresholds to report cyber incidents to the FSO that could have a bearing on the cyber-enabled physical access control systems
- The physical security team should establish thresholds to report physical security incidents that could have a bearing on computers and networks in the facility

C.10 Security Measures for Restricted Areas

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

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*

Threat Summary

- Attackers may access restricted areas (either through physical or cyber means) to compromise the confidentiality, integrity, or availability of sensitive systems or data. They may access or exfiltrate sensitive information risking facility or MTS operations.
- Physical access to restricted areas may result in physical damage to facility assets or cargo theft that can significantly delay or temporarily shut down terminal operations
- Misuse of cyber systems internally or by vendors or other third parties could lead to cyber-safety threats (e.g., environmental damage, disruption to MTS)

CSF Baseline Guidance

- Apply PR.AC controls (PR.AC-1 through PR.AC-7) to ensure access to physical and logical assets that are considered “restricted” is limited to authorized users, processes, and devices
- Implement PR.DS-1, PR.DS 2 to protect the sensitive data on facility networks
- Implement PR.PT-1 for documentation and review of facility audit and log records

- Implement ID.SC-3 to limit suppliers or third-party access to restricted areas

Sample Additional Cybersecurity Protections

- Determine restricted areas, systems, and data stores:
 - “Restricted Areas” include:
 - Physical areas used to perform operations
 - Physical areas used to house digital equipment
 - Physical Security
 - Identify cyber-enabled systems used to control access to restricted areas
 - Security systems should be protected by complete cybersecurity program
 - Data Security
 - Identify sensitive data on IT network, including PII and proprietary data
 - Identify sensitive data on OT network, including OT rule sets
 - Identify sensitive data on BCS network, including data logs
- Develop, approve, and maintain a list of individuals with authorized access to the facility restricted areas
- Enforce physical access authorizations and maintain physical access logs
- Establish key management for facility access to restricted areas
- Limit contractor/third party access to restricted areas (i.e., physical areas and specified IT assets)
- Do not retain default passwords for systems/assets
- Employ encryption measures for sensitive data on the IT, OT, and BCS networks

C.11 Security Measures for Handling Cargo

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

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*

Threat Summary

- Attackers may target systems that hold sensitive client and cargo information to steal or tamper with cargo or move prohibited items through the terminal

CSF Baseline Guidance

- Apply PR.AC controls (PR.AC-1 through PR.AC-7) to ensure access to physical and cyber systems that contain cargo documentation is limited to authorized users, processes, and devices
 - PR.AC-3, PR.AC-7 to manage remote access authorizations for shore-to-ship connections
 - PR.AC-2 for management of physical access to terminals, specifically prevention of "unauthorized loading/unloading" of cargo
- Implement PR.PT-2 to restrict portable media exchanges during cargo handling
- Apply PR.DS-1 and PR.DS-2 to ensure protection of data and cargo manifests
- Implement PR.IP-4 to maintain backups of cargo data and cargo manifests in the event of a cybersecurity attack or other issues with cargo documentation

Sample Additional Cybersecurity protections

- Restrict portable media exchanges during cargo handling
- Manage wireless connections made between vessels and facilities during cargo handling
- Authorize remote access to systems prior to allowing connections between vessels and facilities during cargo handling
- Manage access (physical and cyber) to systems containing cargo documentation
- Encrypt data being transmitted on the network between facilities and vessels through encryption protocols
- Encrypt electronic records of cargo manifests and documentation

C.12 Security Measures for Delivery of Stores

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

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*

Threat summary

- Cyber attackers can remotely control cyber-enabled OT and IT systems used to manage vessel stores and bunker. These cyber-attacks can lead to direct physical damage to stores and bunkers. Additionally, information management system can be corrupted leading to incorrect and damaging management of stores.
- Cyber attackers can remotely control building control and physical security systems used to support vessel stores, bunkers and the IT and OT systems use to manage them. For example, a cyber attacker could unlock gates and disable cameras to allow a physical

attacker to gain unauthorized access. Alternatively, a cyber attacker could lock automated doors and disable fire suppression systems to maximize damage from a physical attack.

- Physical attackers (which can include malicious insider personnel) who gain unauthorized physical access to computer systems and networks can initiate cyber-attacks on those systems and networks, particularly via computer consoles, human-machine interfaces (HMIs), removable media connections (e.g., USB), network connections (e.g., Ethernet jacks).

CSF Baseline Guidance

- Apply ID.AM-1 and ID.AM-2 for identification of IT and OT systems related to delivery of vessel stores and bunkers
- Apply PR.AC controls (PR.AC-1 through PR.AC-7) to ensure access to the facility and physical and cyber systems that support delivery of vessel stores and bunkers is limited to authorized users, processes, and devices
 - Implement PR.AC-5 and PR.PT-4 for facility network protections needed for delivery of vessel stores and bunkers
 - For better understanding of communication and data flows, additional recommended control ID.AM-3 may be implemented to supplement protection of systems and communication paths
- Apply PR.DS-1 and PR.DS-2 to ensure protection of electronic files relevant to delivery of stores and bunkers

Sample Additional Cybersecurity Protections

- Identify and protect OT and IT systems used to manage vessel stores and bunkers
- Identify and protect cyber-dependent physical access control systems for security zones that contain vessel stores, bunkers, and the OT, IT and BC systems used to manage and support them should be identified and protected
- Identify and protect physically exploitable computer and network access points in the security zones that contain vessel stores, bunkers, and the OT, IT, and BC systems used to manage and support them should be identified and protected
- Systems used to manage vessel stores and bunkers management systems that cross any of the boundaries between the IT, OT, BC, and external networks should be identified and the systems and communication paths should be protected
- Network security best practices include physical separation of IT, OT and BC networks

C.13 Security Measures for Monitoring

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

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*

Threat Summary

- Unmonitored facilities or terminal headquarters may be susceptible to threats accessing sensitive information or stealing cargo through the terminals
- Physical threat actors may gain unauthorized physical access to computer systems and networks can initiate cyber-attacks on those systems and networks
- Unmonitored systems and networks may be susceptible to ransomware attacks that can disrupt facility operations, loss of sensitive information, etc.
- Compromised OT systems could interrupt port operations or cause physical damage to facility equipment and pose risks to personnel safety

CSF Baseline Guidance

- Apply DE.CM baseline controls (DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-7, DE.CM-8) to ensure information system and assets are monitored to identify cybersecurity events
- Apply PR.AC controls (PR.AC-1 through PR.AC-7) to ensure access to the facility, restricted areas, and vessels is limited
 - Specifically, PR.AC-2 is implemented for management of physical access to facilities
- Apply RS.CO-1 and RS.CO-4 for coordination to discuss and review results of monitoring
- For identification of cyber-connected assets that needs to be monitored, ID.AM-1 needs to be implemented as a prerequisite prior to monitoring
- Implement PR.PT-1 to establish processes and procedures to ensure audit logs are enabled and to review access logs

Sample Additional Cybersecurity Protections

- Identify network-connected Operational Security equipment (e.g., CCTV cameras, credentialing systems and applications) and monitor those assets (including the network) for anomalous behavior
- Monitor physical access to servers and systems that support facility OT systems
- Review physical access logs regularly and following potential indication of an incident or event
- FSO, IT Manager, and VSO coordinate to determine continuous monitoring security measures and discuss results of reviews/investigations
- All facility systems and networking devices have audit logging enabled
- Align physical access monitoring with intrusion detection systems or other facility system monitoring capabilities for comprehensive threat coverage

- IT personnel performs log monitoring/monitoring for anomalous behavior

C.14 Facility Security Plan

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

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*

Threat Summary

- Systems and facilities with known, unaddressed vulnerabilities can be compromised by cyber attackers

CSF Baseline Guidance

- Apply ID.AM-6, ID.GV-2, and DE.DP-1 to establish roles and responsibilities of personnel assigned to detecting and addressing vulnerabilities. Among those responsibilities is developing an FSP with mitigations that address the vulnerabilities identified in the FSA
- Implement RS.AN-5 for the analysis and response of vulnerabilities
- Apply RS.MI-3 to ensure course of action is determined for newly identified vulnerabilities (i.e., identify mitigations or accept as tolerable risk)

Sample Additional Cybersecurity protections

- Each vulnerability should be assigned a person (or role) responsible for developing the corresponding courses of action for the vulnerability
- Courses of action should be developed in consultation with operations that rely on affected systems to ensure that functionality is maintained and the CySO to ensure that the courses of action sufficiently remediate the vulnerability

C.15 Audits and Security Plan Amendments

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

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*

Threat summary

- Facilities that are not regularly audited can contain undiscovered physical security and cybersecurity vulnerabilities that can be exploited by attackers

CSF Baseline Guidance

- Apply ID.AM-1 and ID.AM-2 to inventory systems and software as a basis for FSP auditing
- Apply ID.RA-1, PR.IP-12, PR.MA-1, PR.MA-2, and DE.CM-8 to identify, document and manage cybersecurity vulnerabilities and to apply updates and patches to systems
- Apply ID.SC-2 and ID.SC-4 to assess products and services from suppliers and third-party partners
- Apply PR.AC-1 to audit the use of identities and credentials
- Apply PR.IP-1 and PR.IP-3 to establish, audit and maintain baseline configurations for systems
- Apply PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, and DE.CM-7 to audit system and network usage for anomalies

Sample Additional Cybersecurity protections

- Ensure that auditing tools and techniques are not disruptive to OT, BC and mission critical IT systems
- External 3rd party service providers may be used to conduct the audit
 - Establish clear mechanism of trust and liability before allowing 3rd party service providers access to systems or networks
- When planning the audit ensure that:
 - The FSO and CySO have coordinated to identify all cyber-enabled systems that support the FSP, along with their physical security zones
 - Audit metrics, acceptable evidence and acceptable thresholds are defined for each aspect of the FSP
 - FSO and CySO have coordinated to assess the risk of all newly identified vulnerabilities considering both cyber to physical and physical to cyber-attack paths

List of Acronyms

Acronym	Definition
AIS	Automatic Identification System
APT	Advanced Persistent Threat
BCS	Building Control Systems
CFR	Code of Federal Regulations
CSF	Cybersecurity Framework
CySO	Cybersecurity Officer
CTS	Container Tracking System
ERP	Enterprising Resource Planning
FSA	Facility Security Assessment
FSO	Facility Security Officers
FSP	Facility Security Plan
HMI	Human Machine Interface
IT	Information Technology
IT/OT	Information Technology and Operational Technology
MCAAG	Maritime Cybersecurity Assessment and Annex Guide
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act of 2002
NIST	National Institute of Standards and Technology
NVIC	Navigation and Vessel Inspection Circular
OT	Operational Technology
PLC	Programmable Logic Controllers
SCADA	Supervisory Control and Data Acquisition
TWIC	Transportation Workers Identification Credentials
USCG	United States Coast Guard
VSO	Vessel Security Officers

Glossary

The glossary contains terms used throughout the MCAAG as well as common cyber security terms. *When possible*, glossary definitions were taken from the NIST Handbook: Introduction to Computer Security.¹⁶

Glossary Term	Definition
Access Control	The discipline, technology, process and/or control for limiting access to an organization's applications, systems, platforms, critical assets, and facilities to authorized entities (e.g., authorized personnel, workflows, and/or data exchanges).
Adware	Specialized advertising software designed to present pop-up messages, windows, or banners on an application that is running. Adware typically captures, tracks, and passes on a user's personal information to third parties without the user's knowledge or agreement. Over time, adware degrades computer performance.
Anti-Virus Software	Specialized software that is designed to detect and where possible mitigate malware before it attacks a system. To be effective, anti-virus software must be maintained with the latest updates so that it can effectively identify, isolate, and repair infected files.
Authentication	The process employed to verify the identity and authenticity of a named user, device, system, or application as a condition for gaining access to a protected resource.
Authorization	The process for approving or permitting an individual, application, and/or system to do something.
Availability	The condition for facilitating timely and consistent access to an asset, data set, or information-based system or service.
Backdoor	An undocumented gap in a software application or computer system that allows access to unauthenticated users, circumventing security processes.
Backup	A practice of duplicating files onto a high-capacity tape, disc, or cloud-based managed service provided by a third party to save electronic files against inadvertent loss, destruction, damage or unavailability.
Computer Security Incident	A violation of established computer security policies, including acceptable use policies or other standardized security practices as defined within the organization's security plans.

¹⁶ National Institute of Standards and Technology Special Publication 800-12 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-12 Rev. 1, 101 pages (June 2017)

Glossary Term	Definition
Cyber Attack	An event that is launched via the Internet against a target with the intent to deny, disrupt, destroy, or exploit a computer-enabled operating environment.
Cyber Security	The capability to protect or defend against unauthorized access to or use of cyber space from cyber-attacks. Cyber security consists of the collective measures implemented to defend a computer or computer-enabled system against cyber-enabled threats, such as hackers, hacktivists, foreign intelligence services and organized criminal syndicates, among others.
Cyber Security Plan	A document that identifies and defines the cyber security requirements and associated controls necessary for meeting those requirements.
Cyber Security Risk	The risk to an organization's information technology and/or operational technology-based assets and resources, along with its supporting functions, processes, and reputation as a result of unauthorized access, compromise, exploitation, disruption, denial, or destruction.
Encryption	A cryptographic method used to encode a set of information for the purpose of protecting it from unauthorized access or modification prior to sending it to a specified recipient.
Firewall	A gateway that limits access between networks in accordance with local security policy.
Firmware Update	Is code that upgrades a device without requiring modifications to the hardware; firmware updates come directly from the manufacturer.
Human Machine Interface (HMI)	Software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency.
Malware	A generic term for software that compromises the operating system of an IT or networked asset with different types of generic or customized malicious code.
Monitoring	The collection, aggregation, recording, analysis and distribution of specific information sets related to application, system and user behaviors. It supports an ongoing process regarding the identification and analysis of risks to an organization's critical assets, applications, systems, platforms, processes, and personnel.
Multifactor Authentication	The required application of two or more factors that a user must employ to authenticate to an application, system, or platform.
Patch	A small, customized security update issued by a software provider to correct known bugs in existing software applications. Most software programs

Glossary Term	Definition
	and/or operating systems can be easily configured to automatically check for patches or other updates.
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information.
Software Update	Changes to software to update, fix, or improve it. Software updates replace older versions of the same software and are usually released by the software developer.
Spam	The use of unsolicited and unwanted bulk messages, in an attempt to convince the recipient to purchase something or reveal personal information, such as a phone number, address, or bank account information. Email is the most typical medium for spam, but spam also occurs in other areas, such as text messages, instant messages, and social networking websites.
Spyware	Software that is installed covertly on a computer to allow an attacker to steal data and, possibly, personally identifiable information. This malicious software is often combined with software that a user voluntarily downloads and will remain on the user's computer even if the voluntarily downloaded program is deleted.
Threat	An action or event that can, through the exploitation of IT, OT, or communications infrastructure vulnerability, cause a risk to become a loss or damage, with negative consequences for the operations and resources of an organization. This could, for example, occur through unauthorized access, denial of service, or spoofing.
Threat Assessment	An evaluation of potential threats, including their severity, and their possible effects on an organization's IT, OT and communications infrastructure.
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code.

List of References

1. Csrc.nist.gov. 2022. NIST Risk Management Framework | CSRC. [online] Available at: <<https://csrc.nist.gov/projects/risk-management/about-rmf>> [Accessed 10 July 2022].
2. Csrc.nist.gov. 2022. *vulnerability - Glossary / CSRC*. [online] Available at: <<https://csrc.nist.gov/glossary/term/vulnerability>> [Accessed 29 June 2022].
3. E CFR.gov. 2022. *eCFR :: 33 CFR Part 105 -- Maritime Security: Facilities*. [online] Available at: <<https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105>> [Accessed 29 June 2022].
4. E CFR.gov. 2022. *eCFR :: 33 CFR Part 105 Subpart B -- Facility Security Requirements*. [online] Available at: <<https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105/subpart-B>> [Accessed 29 June 2022].
5. The MITRE Corporation, 2021. *Defining Cyber Hygiene to Enable Trade-off Analysis*. Bedford.
6. National Institute of Standards and Technology Special Publication 800-12 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-12 Rev. 1, 101 pages (June 2017).
7. USCG.mil. 2022. *United States Coast Guard Cyber Strategic Outlook*. [online] Available at: <<https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf>> [Accessed 30 June 2022].
8. United States Coast Guard. (February 2020). Guidelines For Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.