U.S. Department of Homeland Security

United States Coast Guard

Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20593-7501
Staff Symbol: CG-5P

COMDTPUB xxxxxxx
NVIC 05-17

DRAFT NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 05-17

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

Ref: (a) Title 33 of the Code of Federal Regulations (CFR) Subchapter H, Maritime Security
(b) National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF)

1. PURPOSE. In accordance with 33 CFR parts 105 and 106, MTSA-regulated facilities are instructed to analyze vulnerabilities with computer systems and networks in their Facility Security Assessment (FSA). This Navigation and Vessel Inspection Circular (NVIC) will assist Facility Security Officers (FSOs) in completing this requirement. Additionally, this NVIC provides guidance and recommended practices for Maritime Transportation Security Act (MTSA) regulated facilities to address cyber related vulnerabilities. Until specific cyber risk management regulations are promulgated, facility operators may use this document as guidance to develop and implement measures and activities for effective self governance of cyber vulnerabilities.

2. ACTION.

Enclosure (1) provides draft interpretive guidance regarding existing regulatory requirements in 33 CFR parts 105 and 106, which instruct facilities to conduct FSAs and address any vulnerabilities identified in the FSA in the Facility Security Plan (FSP). This guidance would detail how those existing requirements relate to cybersecurity measures, and what would be recommended to be included in the FSP.

Enclosure (2) provides draft guidance on implementing a cyber risk management governance program to include establishment of a cyber risk management team, policies, programs, and identification of critical systems. This guidance is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82, and provides more detail regarding the development of a Cyber Risk Management Program (CRMP) and specific examples as to how such a program can be implemented in a variety of system and business configurations.

Appendix (A) contains the tables referred to in Enclosure (2).

2. DIRECTIVES AFFECTED. None.

3. BACKGROUND

a. Maritime Transportation Security Act (MTSA) regulations are designed to provide the general parameters for port and facility security while allowing facility owners and operators the discretion to determine the details of how they will comply. The result is that the owners and operators are responsible for assessing vulnerabilities and ensuring the security of their facilities with Coast Guard oversight and guidance. The Coast Guard currently has the regulatory authority to instruct facilities and Outer Continental Shelf (OCS) facilities regulated under MTSA to analyze computer systems and networks for potential vulnerabilities within their required FSA and, if necessary, FSP.

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

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

d. There are many resources, technical standards, and recommended practices available to the marine industry that can help their governance of cyber risks. Facility operators should use those resources to promote a culture of effective and proactive cyber risk management.

4. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any party. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements.

5. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this NVIC and the general policies contained within it have been thoroughly reviewed by the originating office, and are categorically excluded (CE) under current USCG CE # 33 from further environmental analysis, in accordance with Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series). Because this NVIC implements, without substantive change, the applicable Commandant

Instruction or other federal agency regulations, procedures, manuals, and other guidance documents, Coast Guard categorical exclusion #33 is appropriate.

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

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

7. FORMS/REPORTS. None.

P. F. Thomas
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Policy

Encl: (1) Cyber Security and MTSA
(2) Cyber Governance and Cyber Risk Management Program Implementation Guidance

Cyber Security and MTSA: 33 CFR Parts 105 and 106.

Under current regulations in 33 CFR parts 105 and 106, facilities and outer continental shelf (OCS) facilities (hereinafter described as "facilities") are required to identify and assess security threats, and develop a Coast Guard-approved Facility Security Plan (FSP) to address and mitigate those threats. The specific threats are covered by the existing language in parts 105 and 106 in general, but the Coast Guard interprets this language to specifically include threats to computer systems and attacks in the electronic (cyber) domain.

In this draft document, the Coast Guard is laying out its interpretation of regulatory provisions in parts 105 and 106 as applicable to electronic and cybersecurity systems. This enclosure discusses the specific regulatory provisions that instruct owners/operators of a Maritime Transportation Security Act (MTSA) regulated facility to address cyber/computer system security in the Facility Security Assessment (FSA) and, if applicable, provide guidance within their FSPs to address any vulnerabilities identified in the Facility Security Assessment (FSA). This document intends to assist the owner/operator in identifying cyber systems that are related to MTSA regulatory functions, or whose failure or exploitation could cause or contribute to a Transportation Security Incident. If there are electronic or cybersecurity-related vulnerabilities identified in an FSA, an owner/operator may choose to provide this information in a variety of formats, such as a stand-alone cyber annex to their FSP, or by incorporating cybersecurity procedures alongside the physical security measures of their FSP.

In many cases, companies have established cybersecurity and risk management programs that provide for strong cyber defense. For those situations, the owner/operator may demonstrate that those policies meet or exceed the requirements of 33 CFR parts 105 and 106. Owners/operators that already employ a comprehensive cybersecurity plan for their organization, or who wish to apply a standard security program that incorporates cybersecurity to multiple facilities, may wish to submit a security plan under the Alternative Security Program, 33 CFR 101.120.

Once this guidance is finalized, an owner/operator may demonstrate compliance with the regulations by including cyber risks in their FSA and including a general description of the cybersecurity measures taken in the FSP, if appropriate. Owners/operators do not need to indicate specific or technical controls, but should provide general documentation on how they are addressing their cyber risks.

Recommended Cyber Analysis as part of the FSA:

A FSA is the recommended analysis that accounts for possible threats, vulnerabilities, consequences, and protective measure procedures and operations. A thorough FSA is the foundation for determining further applicable requirements of subchapter H in Title 33 of the Code of Federal Regulations. The italicized text provides general guidance on how to potentially incorporate cyber aspects into those requirements.

Facility Security Assessment requirements

33 CFR 105.305 (d)(2)(v)

33 CFR 106.305 (d)(2)(v)

Ensure information on cyber/computer systems is provided to person(s) conducting the facility security assessment and is considered in the analysis and recommendations and contained in report.

Recommendation to Address Identified Cyber Vulnerabilities (as applicable):

Depending on the results of the FSA, this section contains portions of subchapter H that may be applicable. The italicized text provides general, recommended guidance on how to mitigate cyber vulnerabilities determined during the FSA.

Security administration and organization

33 CFR 105.200(b)

33 CFR 106.200(b)

Describe the roles and responsibilities of cybersecurity personnel for the facility, including how and when physical security and cyber security personnel will coordinate activities and conduct notifications for suspicious activity, breaches of security, or heightened security levels.

Personnel training

33 CFR 105.205

33 CFR 105.210

33 CFR 105.215

33 CFR 106.205

33 CFR 106.210

33 CFR 106.215

33 CFR 106.220

Describe how cyber security is included as part of personnel training, policies and procedures.

Drills and exercises

33 CFR 105.220

33 CFR 106.225

Describe how drills and exercises will test cybersecurity aspects of the FSP. 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 at all MARSEC levels and enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

Records and documentation
33 CFR 105.225
33 CFR 106.230
Operators should 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.

Response to change in MARSEC Level
33 CFR 105.230
33 CFR 106.235
Describe additional cyber-related measures to be taken during changes in MARSEC levels.

Communications
33 CFR 105.235
33 CFR 106.240
Facility operators should be able to communicate security conditions 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 perform this function, describe how those systems are protected and an alternative means of communication should the system be compromised or degraded.

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

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

Security systems and equipment maintenance
33 CFR 105.250
33 CFR 106.255
Cyber systems used to perform or support functions identified in the FSP should be maintained, tested, calibrated, and in good working order (e.g., conduct regular software updates and install security patches as they become available).

Security measures for access control
33 CFR 105.255
33 CFR 105.260
Facility operators should 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 vital cyber systems within secure or restricted areas, such as cargo or industrial control systems.

Describe the security measures for access control at all MARSEC levels.

Security measures for restricted areas
33 CFR 105.260
33 CFR 105.265
Describe measures to limit unauthorized access to all of the restricted areas and systems to include those controlled by cyber networks. Unauthorized access might be possible either by manipulating a cyber-controlled gate, allowing physical access, or by accessing the protected system via cyber means, such as by hacking into files that contain sensitive security information. If the area or function has no cyber nexus, indicate "N/A."

Security measures for handling cargo
33 CFR 105.265
Describe security measures to protect cargo handling at all MARSEC levels to include measures that protect cargo manifests and other cargo documentation to deter tampering and prevent cargo that is not meant for carriage from being accepted.

Security measures for delivery of stores
33 CFR 105.270
33 CFR 106.270
Describe cybersecurity measures to protect delivery of vessel stores and bunkers at all MARSEC levels to include procedures, which protect electronic files to deter tampering and ensure integrity of stores.

Facility Security Plan
33 CFR 105.400(a)(3)
33 CFR 106.400(a)(3)
Facility owners or operators should ensure the FSO develops and implements an FSP that addresses each cyber vulnerability identified in the Facility Security Assessment.

Audits and security plan amendments
33 CFR 105.415(b)
33 CFR 106.415(b)
Facility owners or operators should conduct an annual audit of their security plans. Operators may choose to conduct the cyber portion of their audits with either the aid of a

third party or cybersecurity specialists within the organization. The audit report should clearly indicate that the cybersecurity provisions detailed in the FSP are in place and are believed to be appropriate and effective. The audit should include the name, position, and qualification of the person conducting the audit.

Cyber Governance and Cyber Risk Management Program Draft Implementation Guidance

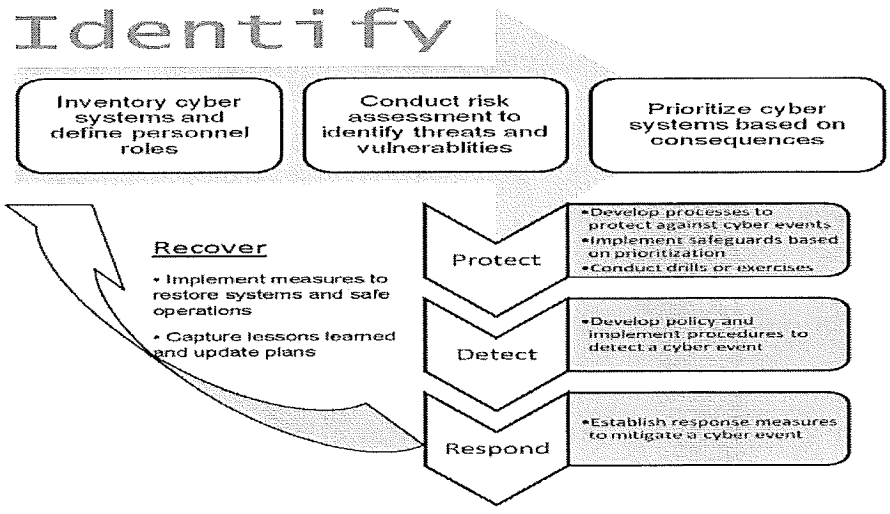
Background:
This enclosure is based on principals from various accepted references from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82 and provides guidelines that facility owners/operators may use to identify and address the cyber-related risks to their cyber systems and applications. Facility owner/operators should consider these guidelines in conjunction with their own risk management policies to help ensure they account for cyber risks.

The NIST CSF:

Sections 1 - 4 utilize the NIST CSF as the recommended foundation for development of a cyber risk management program. The NIST CSF establishes the following functions that is illustrated in Figure 1:

- **Identify** – The administrative structure for cyber risk management as well as the hardware, software, and other components of a system.
- **Protect** – The technical, administrative, physical, and other procedures to protect systems from failure or exploitation.
- **Detect** – Procedures to monitor systems and detect when they may have become compromised.
- **Respond** – The initial actions and notifications needed to limit the consequences of a cyber event.
- **Recover** – Follow up actions needed to restore full functionality and operations.

Figure 1:



A. Identify and Cyber Governance

Section A is divided into two subsections (Sections 1 and 2):

> Section 1 on *Establishing Cyber Risk Management* details methods of selecting members for a Cyber Risk Management Team, provides guidance on establishing Cyber Risk Management Policy, and how to implement that policy with a Cyber Risk Management Program. Section 2 on *Enterprise Wide Inventory and Analysis* details procedures for a thorough enterprise-wide cyber system inventory and analysis. Organizations should adapt this guidance to appropriately address the size, scope, operational needs, level of cyber network utilization, structure, and nature of operations of their individual enterprise.

1. Establishing Cyber Risk Management: Forming a Cyber Risk Management Team (CRMT), Defining Cyber Risk Management Policy, and Establishing a Cyber Risk Management Program

Cyber risk management is an ongoing process of identifying and assessing vulnerabilities, responding to cyber events, and adjusting policies, programs, and procedures to minimize potential disruption. Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

1.1 Define Cyber Responsibilities and Create a Cyber Risk Management Team

Management, strategic planning, and employee engagement form the foundation of efforts to improve information systems and operation systems security. Without a systematic process to identify gaps and launch remedial action, even the most resource-intensive efforts could fail to adequately secure a network. As described in the NIST CSF, the "Identify" step in the process includes identifying the organizational structure responsible for assessing risk, establishing priorities, and ongoing cyber governance procedures.

To assess cyber risk, management should designate a responsible individual who will assemble and lead the CRMT. This individual may also be the organization's Facility Security Officer. This person should have:

- Direct access to communicate with the highest level in the organization and with appropriate intermediate management levels
- Responsibility to monitor cyber risk management activities for facility operations
- Authority to ensure adequate resources to meet cyber risk management objectives

A robust CRMT establishes a process to both initially develop and periodically review policies and program for suitability, adequacy, and effectiveness. Cyber risk management

should be added to the organization's project management cycle to ensure that cybersecurity risks are identified and addressed as part of any given project that may alter cyber systems or organization. This should apply generally to all projects (e.g. a core business process, IT, facility management, etc.).

A multi-disciplinary CRMT with a variety of perspectives and expertise will be best able to identify safety and security critical systems, recognize the consequences, should those systems fail or be exploited, and establish the most effective and efficient solutions. While information technology (IT) specialists should be part of this effort, they may not fully recognize the various operational systems on a waterfront, the potential consequences, should they fail, or have an operator's perspective on potential non-technical (and lower cost) solutions. In short, a team consisting only of IT professionals will only identify IT related threats and IT related solutions. Ideally, a risk management team will include:

- Facility operators
- Port engineers
- Facility Security Officers
- Information technology specialists
- Safety management/industrial safety experts
- Emergency managers

A CRMT may also include third-party experts in cyber technology, risk assessment methodology, or other needed skills, or individuals serving in multiple capacities within the team.

Some large organizations with diverse operations may centralize their cyber risk management policies at the corporate level. While this can be useful to ensure consistency across the organization, it is crucial that corporate cyber risk management policy addresses facility-specific risks. Facility operators should be in communication with the corporate cyber risk management policy office to ensure the policy is aligned with their specific vulnerabilities and operations.
(Source: NIST SP800-82-4.2.2)

1.2 Define Cyber Risk Management Policy

Management should define and approve a cyber risk management policy. The policy should be communicated to employees and relevant external parties as needed. The CRMT is a critical source of input for development of effective cyber risk policy. The policy should include clear direction regarding:

- Policy administration (e.g. policy implementation, maintenance, enforcement, and revision)

- Protection of computer systems
    - Authentication (e.g. password policies)
    - Physical access control
    - Network management
    - Configuration management
    - Privilege management
    - Education and training
- Detection (e.g. intrusion detection)
- Response to a cyber incident
- Recovery (e.g. business continuity and disaster recovery)
- The ongoing role of the CRMT

(Source: NIST SP800-82-4.2.1)

1.3 Create a Cyber Risk Management Program

Management, with the input of the CRMT, should establish a cyber risk management program to ensure that employees and contractors requiring access to the organization's networks, receive job-relevant cyber awareness training. In order to develop a managable and realistic program, an organization's cyber risk management policy should take into account the organzation's risk tolerance and available resources. Key cyber risk management measures can also involve making potentially sensitive revisions to new and existing employee, supplier, and third-party contracts to ensure cyber risk management responsibilities are appropriately defined. The cyber risk management policy should include a definition of roles and responsibilities, including those expected of all users, senior management, privileged users, third-party stakeholders (e.g. suppliers, contractors, customers, partners), and physical and information security personnel. The CRMT lead should have responsibility for the development, review and evaluation of the policy, with approval and oversight by senior management.

One common practice to mitigate the difficulty of managing cybersecurity within large/complex organizations is to appoint an owner for each IT/OT asset, who then becomes responsible for its day-to-day protection.

The suggested cyber risk management process begins with a full inventory of cyber-connected systems (see Section 2). This inventory is then used to generate a list of systems whose failure or disruption would have the most severe consequences (Section 3.1). These systems should then be evaluated for exploitable vulnerabilities. Based on the evaluation of the severity of vulnerability, operators can prioritize systems for mitigation. While these functions are described sequentially, facility operators should think of them as a continuous, repeating process.

2. Enterprise-Wide Inventory and Analysis

The purpose of these steps is to gain the knowledge that allows a company to focus and prioritize its cybersecurity efforts, consistent with business needs.

2.1 Perform Inventory

To inform the cyber risk management process, the CRMT should inventory cyber-connected systems and identify those systems that perform or support vital operational, safety, security, or environmental protection functions. This inventory should include an on-scene survey of cyber-dependent equipment, to identify any systems not on current network maps. Input from operators, security personnel, and OT engineers may prove vital at this stage.

Perform inventory of facility cyber and cyber connected systems using the following suggested process or equivalent:

2.1.1 **Map the system.** Map the entire system(s) and identify hardware, connections, identify users, and major systems. One method to do this is to deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to the organization's public and private network or networks. Automated tools enable tracking, updating, and custom reporting of the inventory. This software is commonly available; however, it is important that the selected version be capable of examining proprietary and standard OT (industrial) systems as well as IT systems. Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. Identify all ports, protocols, and services with validated business needs running on each system.

2.1.2 **Inventory Software.** Develop a complete list of authorized software (including documentation of software versions currently in use) that is required in the organization for each type of system. Include industrial equipment, printers, servers, workstations, laptops, tablets, and smart phones. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified beyond authorized updates. This step has the additional benefit of allowing managers to determine that licenses are up to date.

2.1.3 **User Census.** Develop a list of authorized users for each system to include authorized levels and methods of access. Ensure out-of-date or expired profiles are removed from the system. Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network managers.

2.1.4 **Vendor and Employee Review.** Review Contracts. Contractual obligations for employees and contractors should reflect the organization's policy for cyber risk management. A code of conduct may be used to state employee or contractor cyber risk management responsibilities, including but not limited to:

- Confidentiality
- Data protection
- Ethics
- Appropriate use of the organization's equipment and facilities
- Reputable practices expected by the organization

2.1.5 **Categorize Systems.** Use the inventory to develop a list of Major Systems. Major Systems are those that perform a significant process for the enterprise and are made up of subsystems which perform individual steps in the process. For example, an Emergency Management System (Major System) may be made up of fire alarm, sprinkler, and smoke purge subsystems.

Major system categories can include physical security, safety, and environmental protection systems that perform any of the following functions:

- Fire detection, firefighting, and other emergency response
- Access control and security monitoring
- Communications
- Fuel and HAZMAT control and transfer
- Environmental control and monitoring
- Industrial controls
- Other components identified in a Facility Security Plan (FSP), a Facility Response Plan (FRP), or a Facility Operations Manual (OPSMAN)
- Any component that supports, protects, or effects one or more of the above functions

(Source: NIST SP800-82, Rev. 2, Guide to Industrial Control Systems (ICS) Security, at-4.5.1)

2.1.6 **Conduct Business Impact Analysis.** The purpose of Business Impact Analysis (BIA) is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

B. Cyber Risk Management Plan Implementation Guidance

This section will provide guidance on implementation methods for identifying critical systems and assessing, prioritizing, and mitigating their vulnerabilities. It is divided into two subsections:

3. Consequence Analysis, Vulnerability Analysis, and Prioritization. This section is a step-by-step guide to evaluating current cybersecurity posture in order to develop a course of action for reducing overall cyber risk utilizing information gathered by the process in Part A of this enclosure.

4. Protect, Detect, Respond, and Recover. This section provides examples of recommended practices.

3. Consequence Analysis, Vulnerability Analysis, and Mitigation Prioritization

3.1 Identify Critical Systems: Evaluate Consequences of Worst Case Scenarios

Consequences of a cyber incident can be as varied as the threat actors, ranging from negligible or even unnoticed effects to catastrophic incidents. The tables referenced in this section are located in Appendix A. In evaluating potential consequences, operators should not assume that cyber events will occur in isolation, or at the best possible times. Cyber systems should be evaluated for both security and safety risks, as defined below.

Cybersecurity Risks – Potential for intentional disruption, compromise, or exploitation of a computer network or control system by non-authorized personnel.

Cyber Safety Risks – Potential for accidental disruption of a computer network or control system by an owner, operator, other actor, or as an unintended consequence of a mishap within a connected cyber system.

Deliberate cyber attacks may occur before or in conjunction with physical attacks. Less targeted, but equally significant cyber events may occur when key personnel are not available, other equipment is down for repair, during natural disasters, or any time when multiple risk factors will be present. It is important to not only plan for consequence scenarios within the realm of possibility, but to objectively consider worst case scenarios.

MTSA plan holders may examine consequences by reviewing the scenarios used to develop the Facility Security Plans or by examining system by system, asking, "What system failures could cause the worst possible consequences?" and "What is the worst possible consequence of a failure or disruption of this major system?". This will create a picture of which systems require the most rigorous examination.

As with the inventory, the most effective consequence determinations will involve input from the entire CRMT. Using the inventory results along with this wide ranging personnel input will help reveal cascading effects where one system failure or malfunction leads to another. Failure of backup and failsafe systems, either electronic or manual, should be part of the "worst case" examined during this process.

The use of a Maximum Tolerable Downtime (MTD) matrix will allow operators to assess the total amount of time managers are willing to accept for a mission or business process outage and consider all impact implications.

Event consequences are described in **Table 1** (Appendix A, page 1) and will assist in identifying systems for which further analysis is warranted. Consequences range in severity from *Catastrophic* to *Insignificant.* Determining the severity of consequences will be one factor that, along with the presence and severity of a vulnerability, will determine the level of

mitigation a system demands to prevent a Transportation Security Incident[1], or to address other security, safety, and environmental risks.

- An *Insignificant Event* would result in a brief business disruption and diminished efficiency during correction of the issue. A brief flickering of the lights or having to re-start a computer are examples.
- A *Minor Event* would result in diminished performance of equipment, a small but discernible business impact, or reduced efficiency. Being unable to open a gate or initiate a business operation for a period that would be noticed outside the organization are examples.
- A *Moderate Event* would result in injuries requiring first aid or medical treatment, damage to property or equipment, sustained impacts to operations requiring work around or impacting 3rd parties, harm to the environment, and endangerment of cargo at a facility, or any circumstance that impairs the safety or fitness for service of a facility or a vessel at a facility.
- A *Major Event* would result in one or more deaths, injuries requiring professional medical treatment beyond first aid, damage to property, damage to or loss of a vessel at a facility, destruction of a facility, or discharge or release of oil or hazardous substance. Major events will generally have significant but acute impacts, or less severe but more sustained effects on the MTS.
- A *Catastrophic Event* would result in high consequence *and* long term effects on the MTS. It is likely to have second and third-order impacts to external stakeholders, companies, and ports.

The Table 1 consequence descriptions are provided for illustrative purposes only and do not, of themselves, determine what systems require what level of protection. Operators should focus further examination on systems with Catastrophic, Major, or Moderate event consequences (those scoring 3, 4, or 5 in **Table 1**) as described in **Table 2** (Appendix A, page 1). Prioritizing systems for which disruption would have the most severe consequences is recommended. Operators may choose to further evaluate systems' vulnerabilities with event consequences in the Minor and Insignificant categories (those scoring 1 or 2) with the goal of protecting business systems, reputation, efficiency, safety, and proprietary information. Good cyber practices and hygiene are recommended throughout organizations.

In addition to systems that score 3, 4, or 5 in **Table 1**, systems that, in whole or part, perform a function required by an FSP, such as running cameras or monitors for a restricted area, should be considered high priority, similar to those scoring 3 or above, and be rigorously examined for vulnerabilities, continuing with this or an equivalent process. Operators should avoid connecting systems with components performing these functions to systems with lower levels of protection. These connections can be vectors for cyber incidents to migrate from system to system and should be limited to those serving a viable and necessary business,

1 A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption. (46 USCS § 70101)

security, or safety purpose. **Table 3** (Appendix A, page 2) will assist operators in determining which systems perform or are related to these critical security and safety functions by examining the purposes and connections of each system.

3.2 Assess Vulnerabilities

Now that critical systems and functions have been identified, examining to what other systems they are connected is critical to gain thorough knowledge of vulnerabilities. This will be done by examining both the connections and functions of each system. To determine which systems should be examined for vulnerabilities, refer to **Table 2** which provides guidance based on the system's assigned consequence score from **Table 1**.

Each major system should be evaluated using the questionnaire in **Table 3,** the Connective Vector Assessment, to determine whether failure or disruption of a seemingly innocuous system might have secondary and more severe consequences.

All "YES" responses from the Connective Vector Assessment in **Table 3** should be evaluated for vulnerability severity in the following step using **Table 4** (Appendix A, page 3), the Cyber Infrastructure Vulnerability Assessment. In some cases, where a connection between systems is deemed unnecessary, "air gapping" the critical system is advisable, minimizing a vulnerability. An "air gap" is a system in which computers are not connected directly to the internet, or to any computers that are connected to the internet (discussed further in Section 5).

Once an organization has identified the systems of highest consequence and eliminated all unnecessary connections, it should examine those systems for infrastructure vulnerabilities using **Table 4**, the Cyber Infrastructure Vulnerability Assessment. Cyber infrastructure vulnerabilities are flaws in a cyber system's design, configuration, maintenance, communication and data links, or software. This vulnerability assessment should be applied to each major system identified by the CRMT as having a consequence score of 3 or higher (**Table 1**). "NO" answers will identify vulnerabilities that could be exploited. "YES" answers indicate that the element of infrastructure has appropriate security measures in place. If the answer is not clearly "YES", or is only partially "YES", it should be marked "NO".

3.3 Vulnerability Severity Assessment

Determining which systems have both an infrastructure vulnerability and a vector by which it could be exploited is a key factor (along with consequence of disruption, covered in Section 3.1) in determining risk. Use **Table 5** (Appendix A, pages 3-5) to assess the severity of vulnerabilities and prioritize systems for mitigation. This will be done by answering the questionnaire for each system with a "NO" answer from the Cyber Infrastructure Vulnerability Assessment (**Table 4**). Systems with the highest TOTAL score (at the bottom of **Table 5)** should be considered the most vulnerable.

Record all vulnerabilities and consequences noted during the assessment for review by the COTP. Maintain records of risk assessment IAW MTSA requirements for an FSA.

4. Protect, Detect, Respond, Recover: Recommended Guidance

Once the CRMT recognizes their cyber risks, the organization can select strategies to reduce that risk. However, adequately protecting digital information and cyber dependent system does not usually entail a straight-forward, sequential implementation of specific mitigation measures. Organizations should implement multiple layers of safeguards across a number of different realms (e.g. contracting, human resource management, education and training, network design, physical security, access control, etc).

Prevention and protection strategies reduce vulnerabilities and the frequency of successful attacks or adverse events. While high-risk systems should have more robust protection strategies, this does not necessarily require sophisticated technical solutions. For example, physical access control and training may be sufficient for systems where the primary vulnerability is an insider threat. Where risk managers choose technical solutions, they should also recognize their limitations. Many systems are only capable of recognizing and blocking known threats. Unfortunately, malware and associated delivery mechanisms used by malicious actors are becoming increasingly sophisticated, and a strategy that relies exclusively on a perimeter defense designed to filter out known threats is not likely to be successful.

Operators can also reduce risk by taking steps to minimize overall impact or consequences of a cyber incident. Backups, kept at a remote location, can be an excellent way of building cyber resilience and may be appropriate for situations where the cyber failure is disruptive, but does not include immediate security, safety, or environmental impacts. However, these manual backups, while functional, may now be the weakest link, significantly slowing operations. Exercises can help identify the procedures to isolate a suspect system, purge it of malware, and safely resume operations. Including a cyber aspect into an existing security, natural disaster, salvage/recovery, or environmental response plan can help an organization prepare for a cyber incident.

4.1 Protect

4.1.1 Cyber Risk Awareness Program. Facilities should maintain, and enforce a cyber risk awareness program for employees and contractors. The awareness program should ensure that new and existing employees, as well as contractors requiring access to the organization's IT/OT networks, receive job-relevant training and direction related to the organization's cyber risk management policy. This includes enhancing staff's cyber risk awareness (i.e., what can happen as a result of poor cyber practices) and cyber preparedness (i.e., ensuring that staff are doing all they can to improve the organization's cyber integrity). The cyber risk awareness program could include guidance related to the following:

- Internet and email use policy
- Safe use of personal devices (e.g. ensuring work done off-site on personal computers is as safe as possible)
- Safe use of removable media (e.g., USB keys, CD's, external hard drives)
- Safe use and storage of company mobile devices

- Installation and maintenance of software applications
- Safeguarding user information, passwords and digital certificates
- Identification and reporting of cyber and physicial threats (e.g. how to identify and report phishing emails, or what to do if non-company personnel are observed plugging in a unknown device)

4.1.2 Acceptable Use of Cyber Systems. Define and communicate rules regarding the acceptable use of cyber systems. Prior to gaining access to the organization's cyber systems, employees and external party users should be made aware of (and agree to) the constraints and responsibilities associated with the use of these systems. These constraints should be reflected in the organization's cyber risk management policy.

Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help limit installation of unauthorized software and other abuses of administrator privileges.

4.1.3 Access Control.
Establish and implement a process to manage secret authentications (e.g., passwords, tokens, cryptographic keys, etc.). The use of Single Sign Ons (SSO) – an authentication process that permits a user to enter one name and password in order to access multiple applications – is one strategy for managing authentications. SSO can reduce the amount of secret authentication information that users are required to protect and thus can increase the effectiveness of this control (the more authentication-related information users are asked to remember, the more likely they are to forget it or write it down). In order to protect access to critical systems, a secure password management system should:

- Enforce the use of individual user IDs and passwords to maintain accountability
- Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors
- Enforce a choice of quality passwords
- Force users to change their passwords at the first log-on
- Enforce regular password changes and as needed
- Maintain a record of previously used passwords and prevent re-use
- Not display passwords on the screen when being entered
- Store password files separately from application system data
- Store and transmit passwords in protected form (if passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program)

The password management system should reflect that overly complicated passwords, which are changed too frequently, are at risk of being written on a piece of paper and kept near the computer. The value of password protection should be weighed against the risks associated with time-sensitive operations. In cases where rapid access is vital to

operations or safety, risks may be better mitigated with manual backups or other procedures.

In some instances, operational requirements make effective network segmentation a challenge. In such cases, encryption and/or the use of Virtual Private Networks (VPNs) can help organizations better ensure the protection of their critical information. For business-to-business relationships, access control measures could include:

- Clearly identified roles and responsibilities
- Customized warning banners
- Limit on privileges
- Logging of all critical/non-critical transactions by users
- Detailed logs of transactions
- Use of digital signatures
- Filtering of outgoing traffic to prevent spoofing
- Routing of traffic used for Internet access services through a small number of controlled security gateways

The use of firewall and access control lists for traffic through corporate systems such that external parties have access only to the functions needed should also be considered. This is particularly important where suppliers need to upload systems upgrades or perform remote servicing.

For business-to-customer service relationships, all identified security requirements should be addressed before giving customers access to the organization's information or assets. For example:

- Procedures to protect the organization's assets, including information and software, and management of known vulnerabilities;
- Procedures to determine whether any compromise of the assets, e.g., loss or modification of data, has occurred; and
- Restrictions on copying and disclosing information.

Specific access control measures could include:

- Use of virus checking software on the gateways to the Internet
- Scanning files and stored information for viruses, trojans and other forms of malware
- Data/file integrity verification using algorithms such as hash/checksums, certificates
- Routing of traffic used for Internet access services through a small number of controlled security gateways
- Limit permissions of web applications when accessing backend databases
- Network segmentation and security tiers within a Demilitarized Zone (DMZ) – a *network* design where publicly accessible servers are placed on a separate,

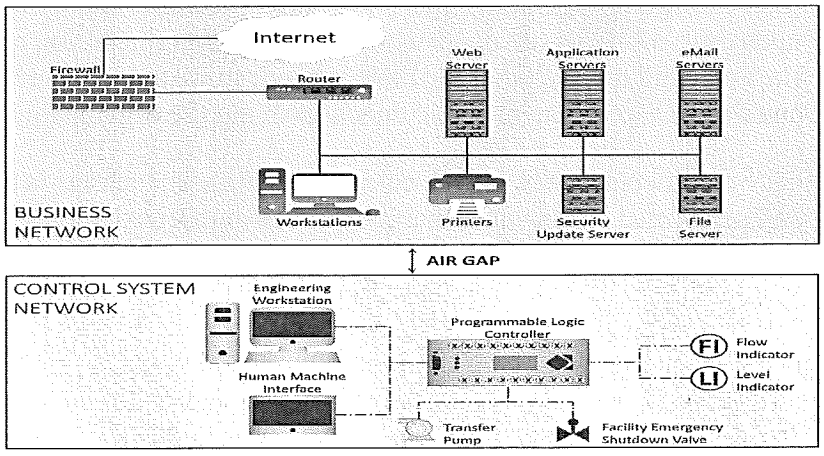
isolated *network* segment – to prevent direct connection paths to corporate data assets
- Secure user registration to ensure that access credentials are only issued to authentic users – such as using an independent Registration Authority for the process
- Authentication using digital certificates, passwords, biometrics or smartcards
- Firewalls and access control lists to prevent unauthorized user access
- Role based access control to limit the function the user is permitted to perform
- Review web application logs for attack identification and containment

4.1.4 Network Segmentation. One method of managing the security of large networks is to divide them into separate network zones (i.e., domains) or organizational units. The most common approach for managing such an approach is through network segmentation and segregation.

While network segregation and segmentation can involve the physical separation of networks, it generally relies on the use of firewalls and/or Virtual Local Area Networks (VLANs) to segment the organization's network(s) into multiple zones with varying security requirements. Both tools – of which there are a variety of options, each with its own capabilities/uses – can be layered and/or used in combination to increase network security. Firewalls and VLANS should be configured (e.g. through access lists) to enforce access management rules set by the organization.

Most accepted national standards recommend segregating functional systems into separate network zones using such methods as air gapping. **Figure 1** illustrates an "air gap" between business and control systems networks.

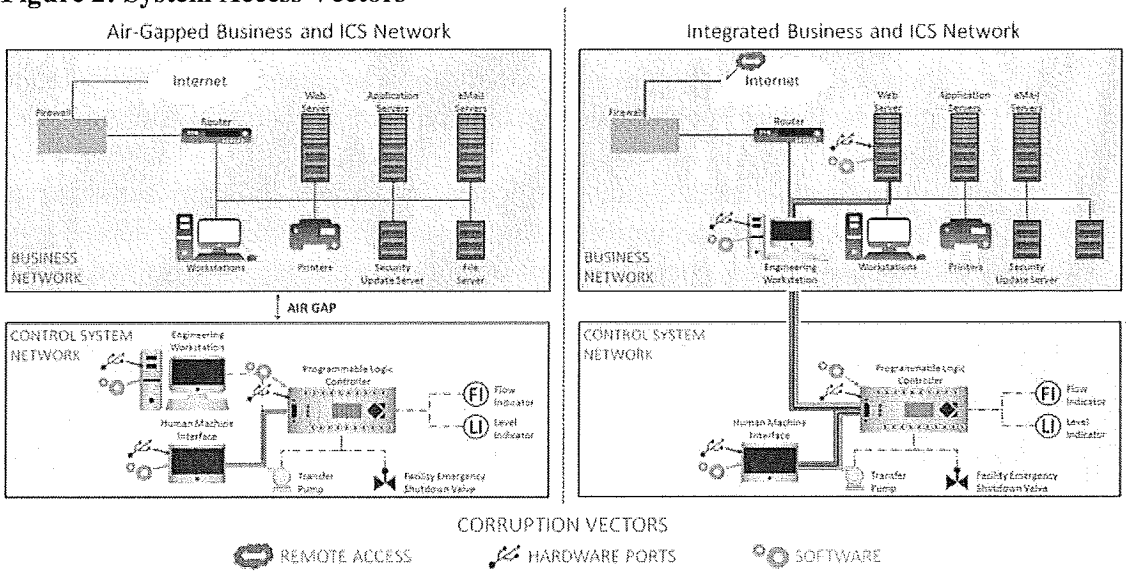
Figure 1: System Segregation, "Air Gapping"



Minimize connections between business and operational technology. Evaluate connected systems based on the highest consequences and vulnerabilities to either system.

Properly air-gapped and segregated systems may still be vulnerable to insider threats, third parties, and technical failure. **Figure 2** shows all the potential ports and access points in an air-gapped control system compared to systems that are not segregated into separate networks.

Figure 2: System Access Vectors



4.1.5 Protect Equipment. Define and implement practices and procedures that establish a protective perimeter and layered defenses around critical equipment.

4.1.5.1 Install, maintain, and update anti-virus/anti-malware systems across the corporate network. Employees and contractors should be aware that anti-malware software does not remove their responsibilities within the organization's cyber risk management policy.

4.1.5.2 Establish safe and secure processes to track and manage system updates (i.e., configuration management). Ensure procedures that provide comprehensive updates to all hardware and software installations (including routers, switches, firewalls and other elements of the network infrastructure) are properly managed and documented system-wide, thus improving the organization's security posture.

4.1.5.3 Ensure that remote access of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. Leverage the use of VPNs with strong authentication systems and effective segmentation and segregation to allow for secure remote access.

Extra precaution should be given to remote maintenance, as this function often requires access to sensitive network areas. Remote maintenance of organizational assets should be approved, logged, and performed in a manner that prevents unauthorized access.

4.1.5.4 Ensure physical access control to areas where cyber assets are stored or used. The physical location of the IT/OT infrastructure within a site (e.g., on board a waterfront facility) is important to consider, particularly with a view to restricting access and maintaining physical security of the network installation and access to control points.

Protect sites containing critical IT/OT equipment or to operate critical cyber dependent systems, from unauthorized access. Authenticate the identity of visitors and instruct them on security requirements and emergency procedures. Supervise all visitors and grant them access only for specific times and authorized purposes. Record the date and time of entry and departure of visitors.

4.1.5.5 Protect power and telecommunication cabling servicing from interception, interference, or damage. Segregate power cables from communications cables to prevent interference.

4.1.5.6 Ensure that cyber assets are not taken off-site without prior authorization. Perform spot checks to detect unauthorized removal of assets and to detect installation of unauthorized devices.

4.1.5.7 Organizations should consider options for securing obsolete IT systems and hardware (i.e. legacy systems). To protect against risks resulting from the use of legacy systems, where adequate security measures cannot be implemented, organizations should consider the following:

- Life cycle management (migrating to new systems)
- Customized support from vendors/specialists

Similarly, organizations should consider how best to handle obsolete IT/OT hardware, which are no longer maintained by the manufacturer (e.g., computers, servers, hard disks, removable media).

4.1.5.8 Establish and implement controls regarding access to cyber systems from off-site (e.g. tele-working), or at remote sites (e.g. field office). Organizations allowing remote activities should issue a policy that defines the conditions and restrictions of off-site activities. In addition, organizations should ensure the security of personal computers, mobile phones, or other devices, used to access cyber systems (e.g. home working or travel outside the normal work location).

In addition to general security controls applicable to all devices that access an organization's cyber systems, the organization should ensure that mobile device-specific risk management considerations are also taken into account. For example, consideration should be given to the following:

- User training
- Physical security of mobile devices (i.e., off-site use and protection of devices)
- Relatively weaker wireless security protocols.
- Inactivity timer lock policy
- Disabling of unused wireless interfaces, services and applications to mitigate against unauthorized access.

- Remote asset management, including:
  - Disabling/locking lost and stolen devices
  - Periodic secure backups
  - Centralized management for asset tracking and policy compliance
- Avoiding default configurations
- Strong authentication (e.g. password protection, biometric ID)
- Enabling logging options
- Firewalls
- Content filtering
- Acceptable use policies for enterprise-owned devices (i.e., restricting personal use)
- Encrypting stored and transmitted (wireless) data
- Secure synchronization procedures Secure VPN for remote access connections
- User consent for location use
- Disabling of unused wireless interfaces, services and applications
- Up-to-date patching of OS
- Anti-virus updating and alerts
- Software downloads only from enterprise software distribution system (avoiding installation of unlicensed software)
- Use of digital signatures to verify download sources
- Remote asset management (disable/lock device)
- Periodic secure backup
- Centralized management for asset tracking and policy compliance
- Establish and implement rules governing the installation of software. Cyber attacks are often propagated through the installation of malware disguised as legitimate software. Organizations should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect) to minimize the likelihood of a compromise to the organization's information security posture.
- Applying the principle of *least privilege* in determining which users are able to install software. This principle suggests that only those who need access should have access.
- Establish, communicate and enforce procedures for the management of removable media (e.g. USB keys, external hard drives, CD, etc). Using removable media to transfer data from uncontrolled systems to controlled systems represents a major risk for the introduction of malware. The organization's cyber risk management policy should include direction concerning the use of removable media (e.g., measures to improve the protection of the devices, procedures to ensure the integrity/security of the device, and restrictions regarding their use).

- Where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept.
- Conduct continuous vulnerability assessments and remediation. Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

4.1.6 **Deploy and Update Intrusion Prevention Systems.** These types of systems are recommended to detect anomalies and prevent potential malicious actions.

4.2 Detect

Even with a well-defined cyber risk management policy and program, unauthorized intrusions and compromises of critical systems remain a possibility. Therefore, it is necessary to put in place applications and processes to detect these intrusions.

4.2.1 **Monitor Traffic.** Establish and implement procedures to monitor network traffic, physical security, and the activities of external parties and personnel to ensure integrity and availability of cyber systems. Ensuring systems are in place to effectively monitor the IT/OT systems (from cyber, physical and personnel security threats) should be a key element of an organization's cyber risk management policy.

4.2.2 **Reporting Responsibilities.** Define and communicate roles and responsibilities related to the reporting of suspicious and observed cyber incidents and weaknesses. All employees and contractors using the organization's IT/OT systems and services should be required to note and report any observed or suspected cyber incident or weaknesses to a point of contact, as specified in the cyber risk management policy and either referenced or incorporated into the FSP, as quickly as possible. The reporting mechanism should be as easy, accessible and available as possible.

Report breaches of cybersecurity and cyber suspicious activity in accordance with current regulations, policy and guidance.

4.2.3 **Keep Logs.** Create, keep, protect, and regularly review event logs recording user activities, exceptions, faults and cyber events. It is important that logs be protected against tampering and unauthorized access. To help identify significant events for security monitoring purposes, consider copying appropriate log entries automatically to a second log, or the use of other tools to perform file analysis. To ensure accuracy of event logs and subsequent reports, the clocks of all relevant IT/OT systems within an organization should be synchronized.

4.2.4 **Run Tests.** Run penetration testing of the organization's critical IT/OT infrastructure, if feasible. Penetration tests of critical IT/OT infrastructure can detect whether the actual cybersecurity level matches the level set forth in the cyber risk management policy. Penetration tests performed by external experts employ attacks using both cyber and social engineering-based elements.

4.2.5 **Deploy and Update Intrusion Detection Systems.** Deploy intrusion detection and protection systems as appropriate. Ensure the software is properly installed, configured, maintained, and updated. Network Intrusion Detection Systems (IDS) work by monitoring and analyzing network traffic, then generating and disseminating suspicious activity alerts in real time. Organizations may also choose to incorporate Intrusion Prevention Systems (IPS). IPS, an extension of the IDS, monitors, logs and reports on network activity and attempts to block malicious traffic with the potential to compromise critical systems once detected. The majority of IDS and IPS are attack Signature Based, comparing known threats against observed events to identify possible incidents. Therefore, the value of the system is only as good as the attack signature database against which events are analyzed. IDS may also leverage Anomaly Based Detection, which compares definitions of what activity is considered normal against observed events to identify significant deviations *at the system level*. Anomaly-based systems rely on profiles representing the normal behavior of such things as users, hosts, network connections, or applications. Profiles are developed by monitoring the characteristics of typical activity over a period of time.

Finally, IDS may also use more complex Protocol Analysis, which attempts to identify deviations between what are generally accepted activities *at the application level* against observed events.

Given the differing characteristics and complexities of different IDS/IPS, at a minimum, the following factors should be considered when selecting intrusion detection software:

- Timeliness of updates
- Effectiveness of internal distribution
- Implementation
- System impact

It is also important to note that technology alone is not sufficient to detect system intrusions. Organizations should ensure that the evaluation, selection, installation, operation, and maintenance of intrusion detection software are performed by qualified technical staff. For example, IDS should be configured to closely monitor traffic taking place within network zones housing critical information. This support should be integrated in the organization's cyber risk management policy.

4.3 Respond

Even with strong access controls and a well-designed cyber network that may include sophisticated anti-virus software, and intrusion detection and protection systems, compromises could occur. Response procedures are therefore necessary. An incident response plan will detail the response priorities, roles, and responsibilities of personnel, procedures and communication process necessary to effectively respond to a cyber incident. A planned response to an incident can aid in minimizing disruption/damage, recover compromised data and preserve evidence for legal action.

4.3.1 **Investigate Notifications.** Ensure that notifications from monitoring systems are investigated in a timely manner. If monitoring reveals an anomaly, organizations should be able to quickly determine whether the cause is a security incident, a hardware or software problem, or an increase in client demand.

To better inform the subsequent response, investigators should be able to ascertain:

- When did the cyber breach occur and is it ongoing?
- Where did it originate? Internally or externally?
- How and why did the cyber incident occur? For example, did a malicious intruder exploit a network vulnerability, or did an employee accidentally exercise poor cyber hygiene?
- What was compromised (e.g., intellectual property, data, network operations, etc.)? (consider primary effects and secondary effects)

Communication on the incident should involve pertinent internal and external stakeholders in accordance with legal reporting requirements.

4.3.2 **Plan Thoroughly.** Develop, manage, execute, and regularly exercise contingency response and incident management plans. The plan should be concise and accessible to those with responsibilities defined in the plans. The purpose and scope of each specific plan should be defined, agreed by the organization and top management, and understood by those who will invoke the plan. Reference other relevant plans or documents within the organization, particularly business continuity plans, security plans, and oil/hazardous material incident response plans. Cyber response plans should include details regarding response-related considerations, including:

- Roles and responsibilities (e.g., who has decision-making authority, when to call in external experts, as well as who to communicate with);
- Incident thresholds and activation triggers;
- Incident handling and escalation procedures (e.g. order of operations, consider the following process:

1. Detect intrusion
2. Isolate system
3. Shut down system (if necessary)
4. Purge intrusion
5. Verify system safe
6. Restart

- Incident response priorities/capabilities for organizational information systems
- Steps to ensure integrity of post-incident investigations and forensics (avoiding decisions that may inadvertently compromise evidence and/or make recovery work more difficult); and
- Procedures for determining the impact of the incident.

Update contingency response and incident management plans to address cyber as a vector to trigger other events, disrupt computer networks used in response to other incidents or to disrupt maritime operations. It is important that response plans be available in non-electronic formats as some types of cyber incidents can include the deletion of data, and/or the disabling of system functions/communication links. Exercise cyber response plans as part of MTSA and other existing contingency plans. It is recommended that operators hold these exercises at the strategic level involving senior management, as well as at the tactical level involving key operational personnel.

4.3.3 **Limit Consequences.** Include controls to deal with loss of computer based systems and cyber networks, such as a denial of service attack. The plan should address actions necessary to minimize, if not eliminate, propagation of the incident. The action could be, but not limited to:

- Isolation functions
- Software management (e.g. patching vulnerabilities)
- Strengthened controls to prevent reoccurrence

Conduct a post-incident analysis which summarizes the impact of the incident, including cost, and identifies measures to prevent a similar incident. Define and apply procedures for the identification, collection, acquisition and preservation of information related to the cyber incidents. Consider the use of external experts who are skilled in conducting interviews and retracing the behaviour of people who had access to protected information. These external experts may help to ensure no digital evidence is overlooked and can assist at any stage of a digital forensics investigation or litigation. Capture lessons learned and evaluate vulnerabilities discovered while responding to and/or investigating the cyber incident for possible changes to related cyber risk policies.

4.4 Recover

No amount of planning or investment can make an organization's cyber systems completely secure. New threats and unanticipated vulnerabilities could emerge, potentially allowing critical systems and functions to be compromised or disrupted. The ability to restore a system via backup data or software is an important element in cyber recovery planning. Effective cyber recovery processes can aid in minimizing financial loss, maintain customer and public confidence, and prevent future cyber incidents.

Taking steps to put in place backups and alternative methods of carrying out core business and supporting functions allows an organization to continue operations and maintain continuity of safety and security processes despite a cyber attack. These redundancies and mitigation measures will prove valuable not only in the event of a cyber incident, but also during the recovery phase of a non-cyber safety or security event.

Facility operators should ensure that they have identified the sources of any backup data or software needed to restore critical functions in a timely manner. Storage areas (e.g. lockers/closets) may need additional capabilities such as dehumidifiers or water resistant closures to protect electronic equipment stored in the maritime environment.

4.4.1 **Back Up Information.** Create, manage, and periodically test backup copies of information, software and system images per cyber risk management policy. Provide adequate backup facilities to ensure that all essential information and software can be recovered following a disaster, cyber attack, or media failure.

4.4.2 **Protect Back Up Storage.** Ensure that backups are adequately protected via physical security or encryption when they are stored, as well as when they are moved across the network. Require the creation of multiple backups over time, so that, in the event of malware infection, restoration can be from a version that is believed to predate the original infection. Consideration should be given to the protection of remote backups and cloud services. Ensure that key systems have at least one backup destination that is not automatic and should be initiated by an operator.

4.4.3 **Maintain/Establish Redundancies.** Ensure that redundancies are in places for critical systems. Identify safety, security, and operations requirements to identify and prioritize cyber systems with high availability requirements. Where the availability cannot be guaranteed using the existing systems architecture, redundant systems should be considered. Where applicable, redundant cyber systems should be tested to ensure they work as intended. Train workers on engaging manual systems to re-establish or maintain operations. In many cases, non-cyber measures and process can serve as effective redundancies and can limit an organization's vulnerabilities in a high-threat cyber environment. For instance, in the event of a cyber incident that compromises the transfer pumps at a bulk liquid facility a manual float switch can be used on a bulk liquid tank to cut power to a fill pump to prevent overfilling the tank. Additional security guards could be

used to monitor access to restricted areas in the event that cyber dependent access control and monitoring systems are compromised.

4.4.4 **Perform Exercises.** Develop, manage, execute (as appropriate), and regularly exercise recovery plans for cyber incidents that compromise critical systems. Recovery plans (i.e. business continuity plans and disaster recovery plans) should be concise and accessible to those with responsibilities defined in the plans. The purpose and scope of each specific plan should be defined, agreed to by the CRMT and senior management, and understood by those who will invoke the plan. Any relationship to other relevant plans or documents within the organization, particularly to business continuity plans, should be clearly referenced and the method of obtaining and accessing these plans described. The following is a non-exhaustive list of elements that should be contained in organizational recovery plans:

- the critical cyber dependent services to be recovered;
- the timelines in which they are to be recovered;
- the recovery levels needed for each critical service activity; and,
- the circumstances under which each plan can be invoked.

4.4.5 **Integrate Cyber Recovery into Enterprise Recovery Plan.** Include cyber risk management within the business continuity and disaster recovery management processes. Existing business continuity or resumption plans can be implemented to restore operations and maintain essential mission functions to supplement and/or restore computer networks. Cyber networks should be tested prior to resuming full operational capability to verify the problem is isolated and the network is not vulnerable to a similar, or the same, threat.

4.4.6 **Communication.** Communicate status of cyber networks and impact on business operations to internal and external stakeholders. Public relations personnel may be needed to communicate impacts and resumption of operations to the general public.

Cyber Risk Evaluation Tables

Table 1: Consequence Evaluation Guide (Encl. 2, section 3.1)

Language Descriptor	Effect on MTS	Physical Consequences	Effects beyond MTS	Score
Catastrophic Event	High Consequence Event AND Long Term or Significant Effect on MTS	Multiple Permanent Injuries and/or Deaths	Significant impact beyond MTS, economic disruption, harm to national security	5
Major Event	High Consequence Event OR Long Term Significant Effect on MTS	Few Permanent Injuries and/or Deaths	Short term *or* localized disruption beyond MTS	4
Moderate Event	Moderate Consequence, Moderate Term Effect on MTS.	Injury requiring medical treatment or first aid, and/or Death	Minor or short term localized economic disruption	3
Minor Event	Minor Disruption: Local/Short Term Disruption	Business disruption noticeable outside organization	Negligible	2
Insignificant Event	None	Business Disruption	None	1

Table 2: Consequence Score Action (Encl. 2, section 3.2)

Consequence Score	Recommended Assessment Action
4-5	Continue rigorous evaluation of vulnerabilities within this system; establish redundant control/protection/detection measures. Do not establish connections to systems w/lower level of protection w/out a compelling need and risk review and mitigation.
3	Continue rigorous evaluation vulnerabilities within this system; establish credible and effective control/protection/detection measures. Avoid establishing connections to higher consequence systems w/out compelling business needs and appropriate controls.
1-2	Document. Conduct evaluation of vulnerabilities and establish controls sufficient to business needs. Avoid establishing connections to higher consequence systems w/out compelling business needs and appropriate controls.

Table 3: Connective Vector Assessment (Encl. 2, sections 3.2 and 3.3)

Does this system support or impact or is it linked to systems that support or impact:	Yes	No
• Security measures to prevent or deter unauthorized access to restricted areas?		
• Security measures for monitoring personnel in restricted areas?		
• Security measures to protect vessels using and serving the facility?		
• Security measures for facility restricted areas or spaces containing: - Security & surveillance equipment - Lighting system controls - Intrusion detection systems - Water supplies/pumps/manifolds, - Dangerous goods or hazardous substances - Cargo pumps and control stations - Cargo spaces/storage - Sensitive security information - Ventilation & air conditioning systems, including their access points - Telecommunications		
• Security measures for facility-specific restricted areas or spaces containing: - Shore areas immediately adjacent to each vessel moored at the facility - Certain dangerous cargoes - Manufacturing or processing areas and control rooms		
• Systems containing cargo documentation?		
• Security measures to protect cargo and vessel stores at the facility (including measuring, tracking, or moving cargo)?		
• Systems that identify cargo approved for loading, restrict entry of unauthorized cargo, or ensure the release of cargo only to authorized carriers/recipients?		
• Security or monitoring measures for delivery of stores and bunkers?		
• Identification, monitoring, screening, tracking, or direction of guests or passengers?		
• Sensors, alarms, or notification systems for a security or safety incident?		
• Emergency communications with outside parties?		

(Source: NIST SP800-82-4.2.6)

Table 4: Cyber Infrastructure Vulnerability Assessment (Encl. 2, sections 3.2 and 3.3)

	YES	NO
Are installed security capabilities enabled and checked?		
Is there incorporation of security into architecture and design?		
Are there safeguards against system reprogramming?		
Are there safeguards against and warnings for spoofing?		
Is manipulation of control data logic prevented?		
Is there sufficient backup power?		
Is there an identity authentication policy?		
Are there incident detection and response plans and procedures?		
Have unsecured physical ports been eliminated?		
Are vendor software patches developed after a vulnerability is identified?		
Are vendor software patches installed after a vulnerability is identified?		
Is data accessible only to personnel with a legitimate business need?		
Is malware protection installed and up-to-date?		
Are critical configurations stored and backed up properly and regularly?		
Is there redundancy in critical system functions (avoiding single point failure)?		
Are logs of software alterations, suspicious activity, cyber attacks/ incidents, and system modifications maintained?		
Are there backup or shut-down options in case of loss of environmental control?		
Are you able to isolate, contain, or shut down compromised operations or systems in the event of a cyber-related disruption?		
Is operational data and configuration information removed from systems before they are decommissioned?		

(Source: NIST SP800-82-4.2.6)

Table 5: Vulnerability Severity Assessment (Encl. 2, section 3.3)

Access Point	Analysis Questions	N/A =0	0	1	2	3	Selected Score
Hardware Ports: Serial USB Ethernet	*Is physical access to these ports limited to personnel with a legitimate business purpose?* *Are the drives and storage devices used with these ports used exclusively for business purposes?*	N/A	No ports physically accessible	Few ports accessible to select personnel with approved hardware only	Several ports available for use by loosely trained/ vetted personnel	Substantial access with few controls	
Remote Access: Router Vendor Network Satellite Provider Network Wireless Access Points Wireless Protocols	*Who has access to wireless ports?* *Are guests permitted to access wireless ports, particularly on their own devices?* *Are wireless ports password protected?* *Are only approved devices able to access wireless networks?*	N/A	No wireless access	Guest and corporate access points are logically separated; limited number of users and access points,	Significant number of users and access points	All employees have access; guests have substantial access	
Software Software Defects and Bugs Configuration	*Are user-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools) in use?* *Are internally hosted and developed (or vendor developed but user modified) applications supporting critical activities?* *Is Open Source Software (OSS) in use?*	N/A	No user-developed software No user-modified software No OSS	Few instances of OSS, user developed or modified software, supporting non-critical functions	Large incidence of user-developed, user-modified, or OSS supporting non-critical functions	Large incidence of user-developed, user-modified, or OSS supporting critical functions	
ISP Connections	*What ISP connections link to ICS, security, or business systems?* *Are ISP configurations overly complex?* *Are policies on ISP use sufficiently restrictive and adhered to?*	N/A	No ISP connections to ICS, security systems, or relevant business systems	Minimal connections to ICS, security systems, or relevant business systems Low complexity	Several connections to ICS, security systems, or relevant business systems	connections to ICS, security systems, or relevant business systems	

Table 5 (cont.) Access Point	Analysis Questions	N/A =0	0	1	2	3	Selected Score
Changes in Cyber Environment : Network Infrastructure Critical applications	*How often are changes made which may impact ICS/OT systems occurring?* *Is security a consideration when making changes?* *Are old ports, terminals, etc. secured?*	N/A	Stable Environment	Infrequent or Minimal Changes	Frequent adoption of new technologies	High Volume of significant change to critical systems	
External Devices Personal Company owned but personally maintained allowed to connect to the network	*Are the devices used to update or collect data secure?* *Are the minimum number of portable devices in use?* *Are devices assigned to an individual with a specific business purpose, training, and accountability?*	N/A	No portable devices allowed to connect to the network	Only one device type allowed to connect, limited data exchange, selected employees	Multiple device types, used to update software,	Significant number of device types, including personally owned devices, allowed to access the network.	
Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	*How many vendors maintain equipment on the network?* *Do my employees know/recognize individuals sent by vendors?* *How complex is their access method? Is their reach limited to the system they are working on?* *Are devices used by vendors connected to my network secure?*	N/A	No third parties and no individuals from third parties with access to systems	Limited number of third parties and limited number of individuals from third parties with access; low complexity in how they access systems	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems	Significant number of third parties and significant number of individuals from third parties with access; high level of complexity in terms of how they access systems	
The total of all scores represents an overall vulnerability score for this system.						**TOTAL:**	

(Source: NIST SP800-82-4.2.6)