

**CISA Tabletop Exercise Package**

**Maritime Ports**

[Enter Organization Name]

## <Insert Date>

## Updated November 2023

## Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc151377240)

[Exercise Overview 5](#_Toc151377246)

[General Information 6](#_Toc151377247)

[Module 1 8](#_Toc151377248)

[Module 2 11](#_Toc151377249)

[Appendix A: Additional Discussion Questions 13](#_Toc151377250)

[Appendix B: Acronyms 16](#_Toc151377251)

[Appendix C: Case Studies 17](#_Toc151377252)

[Appendix D: Cybersecurity Risks to Port Components 18](#_Toc151377253)

[Appendix E: Contacts and Resources 19](#_Toc151377254)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 10:30 a.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <Organization> in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the resilience of <Organization> during and following a cyber incident impacting the maritime sub-sector. 2. Evaluate <Organization’s> ability to continue operations during and after a cyberattack. 3. Identify areas for improvement in cyber incident response plans. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A zero-day vulnerability leads to a cyberattack impacting port and maritime transportation operations. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An overview of the cybersecurity risks to maritime port components presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include but are not limited to the information technology (IT)/information security staff, emergency management staff, Facility Security Officer, and port dispatchers.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include personnel without a direct role in incident response, senior leadership, and port partners.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces several events, including a joint advisory from CISA, the U.S. Coast Guard Cyber Command (CGCYBER), and the Federal Bureau of Investigation (FBI), and indicators of a potential network compromise.
  + **Module 2:** This module includes operational impacts to port operations, media inquiries, and the successful exploitation of vulnerabilities to an information system.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

# Module 1

### Day 1

A cyberattack against a large U.S. port is reported across major national news outlets. A web server at the port was breached via an exploited vulnerability in the port’s <authentication infrastructure>. The malicious actors obtained the log-in credentials for a type of popular password management software that allowed entry onto port networks. A CISA, CGCYBER, and FBI joint advisory notes that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability.[[2]](#footnote-3) The advisory further identifies this incident as part of an ongoing campaign targeting U.S. ports, transportation companies, and other transportation sector organizations using known exploited vulnerabilities (KEVs) in unpatched legacy systems to gain network entry. CISA, CGCYBER, and the FBI urge organizations to ensure password software is not directly accessible from the internet and strongly recommends domain-wide password resets.[[3]](#footnote-4)

### Day 3

Multiple people are forcefully logged out of their accounts. They report their passwords have been changed by someone else and they cannot reset it as their security question answers were changed.

### Day 9

Vessel Traffic Controllers in the Harbormaster’s Office (HMO) notice a vessel appearing to start into the port via the <Vessel Traffic Information System (VTIS)>. Controllers attempt to contact the vessel; however, it does not respond. Controllers in the HMO notice the vessel no longer appears on <VTIS>. Visual inspections verify there was no vessel traversing the port.

### Day 10

A security researcher contacts your organization informing you that a trusted Managed Service Provider (MSP) in the Maritime Transportation Sector was recently the target of a significant cyber incident. You do not use this vendor but do employ other MSPs.

Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cybersecurity threats to your organization?
2. What cybersecurity threat information does your organization receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated across your organization and by whom?
   3. What actions would your organization take following an alert like the one presented in the scenario?
   4. What mechanisms exist for your organization to share information across the subsector?
3. How does your organization assess risks in conjunction with maritime partners?
4. Describe the risks/advantages to maintaining legacy equipment/systems.
   1. How do you manage technology that is no longer supported by the manufacturer?
   2. What supply chain concerns do you have regarding legacy equipment/systems?
   3. Describe your organization’s equipment decommissioning process.
   4. Describe your organization’s equipment security commissioning process.
5. Describe your organization’s patch management plan.
   1. What processes are used to evaluate and maintain an allowed list of patches?
   2. How does risk inform decisions regarding allowed hardware, firmware, and software?
   3. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
6. How is your network configured (e.g., network segmentation, least privilege access, multi-factor authentication, etc.) to defend against malicious actors?
7. What tools (e.g., threat hunting, security audits, etc.) do you leverage as part of a proactive cybersecurity strategy?
8. What Indicator of Compromise (IOC) feeds does your organization use?
9. How does your organization baseline network activity?
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
10. What is the role of cybersecurity in the review and selection of third-party vendor support?[[4]](#footnote-5)
    1. What cybersecurity language, (e.g., cybersecurity training and cyber incident notification requirements), is included within third-party vendor contracts?
    2. How do you evaluate the cybersecurity posture of your vendors?
    3. How often are contracts reviewed?
11. What level of access do your third-party vendors have to your organization’s network?[[5]](#footnote-6)
12. How often are third-party access rights and data logs reviewed?
13. How do your service level agreements address cyber incident notifications?[[6]](#footnote-7)

# Module 2

### Day 13 – Morning

All gate ID card readers begin to malfunction. Some gates are abnormally slow to open while others will not open at all. As a result, trucks attempting to deliver and pickup cargo are unable to enter or exit the terminals, causing major delays at gates and backups on local roadways.

### Day 13 – Afternoon

Incoming vessels report they are not receiving information from the port on their assigned terminals. HMO controllers discover that they have lost access to <VTIS> and cannot identify vessels or their intended destination.

The lack of access to <VTIS> results in significant backups on the waterways.[[7]](#footnote-8)

### Day 14

Local news media begins to report on the delays at the port. Some news organizations are claiming to have insider information that the port is currently experiencing a significant cyberattack.[[8]](#footnote-9)

### Post Cyber Incident

A post incident forensic investigation reveals that the port’s legacy systems were left unpatched, and threat actors used one of the exploited vulnerabilities mentioned in the <Day 1> alert from CISA, CGCYBER, and the FBI. Once the vulnerability was exploited, attackers were able to move laterally through other port systems.

## Discussion Questions

1. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
   1. What guidance does the plan include on assessing the severity of the incident?
   2. How does incident severity level dictate response?
   3. How are critical systems and processes incorporated within your CIRP?
2. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
   1. What additional resources outside of your organization would be necessary for responding to the cyber incident?
   2. What are the processes or procedures for requesting additional resources?
   3. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
3. How would you attempt to mitigate the issue with the gate card readers?
   1. What are the impacts of gate malfunctions on port operations?
   2. How long can the port operate with gates and card readers malfunctioning?
   3. Describe the process to implement manual override of the gates/readers and perform verifications on incoming/outgoing personnel and cargo.
4. What are the impacts on the port when <VTIS> is malfunctioning?
   1. What navigational backups can be utilized by the port and incoming/outgoing vessels?
5. What external organization(s) would you be engaged with?
   1. Are there any regulatory reporting requirements?
6. Describe your organizational processes to respond to the media reports and inquiries.
   1. What pre-scripted messages do you have for cyber incidents?
   2. How would public messaging be coordinated and disseminated during a cyber incident?
   3. How do you preserve and reinforce the public’s confidence and trust in your organization during a significant cyber incident?
7. What plans and policies are in place for recovery and restoration of critical infrastructure operations and services?
   1. What are your priorities regarding recovery efforts?
8. Based on discussion, what changes will you implement to increase the resilience of your organization?
   1. Describe the “lessons learned” and corrective action processes you use.
   2. What measures will you take to secure your network from a similar incident happening in the future?

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional page, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated into your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
3. What were the most recent results and action items that followed?
4. Describe your organization’s review process for your CIRP.
5. How often is the CIRP reviewed?
6. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
7. How are updates to the plan communicated to relevant employees?
8. Discuss your supply chain concerns related to cybersecurity infrastructure.
9. How are IT and business continuity functions coordinated with physical security?
10. How is the integrity of your critical data protected and validated?
11. What mission essential functions are impacted by the incidents described in the scenario?
12. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
13. If primary communications are compromised, how do you provide information to internal and external entities?
14. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Employee Accounts & Privileges

1. Describe your organization’s bring your own device (BYOD) policy.
2. Describe your organization’s employee off-boarding process.
3. Is this process coordinated with IT and Human Resources (HR)?
4. What additional actions are taken if the employee’s termination is contentious?
5. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication key, system administrator’s handbook/manual, keys, identification cards, etc.)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training have employees received regarding reporting requirements and your CIRP?
4. What cybersecurity incident escalation criteria are defined in your CIRP?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When is leadership notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is the integrity of your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are the key factors in the decision to keep the port open (e.g., change in Maritime Security [MARSEC] level)?
2. Who makes the decision?
3. How do the HMO and Port PD coordinate and share information about incidents and threats to the port?
4. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
5. At what point in the scenario would you contact law enforcement?
6. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
7. How would a breach of <vendor> affect your organization if they have access to your information?

## Recovery

1. How does your organization determine a cyber incident is over?
2. Who makes this decision?
3. What post-incident activities would your organization conduct?
4. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
5. What is the risk associated with re-activating critical business processes and systems?
6. How long and costly is the process to completely rebuild these systems?
7. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. How often does your organization exercise its CIRP?
3. How do your organization’s training and exercise efforts address both physical and cyber risks?
4. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior staff/leadership?
3. What is your role during a cyber incident?
4. What information do you need to support your decision-making process?
5. What are the gaps in your cybersecurity workforce?
   1. How does your organization recruit, develop, and retain cybersecurity staff?
6. What state, local, tribal, territorial, or regional partners do you enlist for cybersecurity personnel support?

## Public Information

* + - 1. What training is provided to employees regarding reporting any contact with the media to the appropriate public information personnel?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What are the potential legal issues based on the scenario?
3. What legal documentation should your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| APT | Advanced Persistent Threat |
| CGCYBER | U.S. Coast Guard Cyber Command |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| BYOD | Bring Your Own Device |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HMO | Harbormaster’s Office |
| IOC | Indicators of Compromise |
| IT | Information Technology |
| KEV | Known Exploited Vulnerability |
| MARSEC | Maritime Security |
| MSP | Managed Service Provider |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| TLP | Traffic Light Protocol |
| USCG | United States Coast Guard |
| VTIS | Vessel Transportation Information System |

# Appendix C: Case Studies

## Ransomware Attack Against Japanese Port

On July 4, 2023, a major Japanese port suffered a ransomware attack that impacted the central computer system. The centralized system is responsible for operating five cargo terminals at the port. The attack against Japan’s busiest port prevented it from receiving any shipments for two days. “LockBit 3.0”, a pro-Russian cyber gang, claimed responsibility for the ransomware attack.[[9]](#footnote-10) The port authority decided to not pay the ransom, but rather shutdown operations and restore the affected systems to normal functionality. During restoration some terminals chose to resort to manual operations to mitigate impacts. This was the first reported ransomware attack against the port and generated concerns for the local economy and supply chain. Cascading impacts included manufacturing delays across the country, most notably at the Toyota Motor Corporation.

## Zero-Day Vulnerability in Password Management Software

On August 19, 2021, unidentified hackers broke into a web server at a large U.S. port using a previously unidentified (zero-day) vulnerability in a password management software. The hackers planted malicious code on the server, which allowed further access to the IT system. Approximately 90 minutes into the breach, the hackers stole all of the log-in credentials for a type of Microsoft software that organizations use to manage passwords and access their networks. Port cybersecurity staff isolated the server and cut off access to the network in response to the breach.[[10]](#footnote-11) This attack was part of an ongoing set of hacks targeting defense contractors, transportation firms, and other U.S. based organizations.

## Shipboard Network Malware Attack

In February 2019, a vessel traveling from international waters to a major U.S. port experienced a cyber malware attack affecting its shipboard network. The malware degraded the functionality of the onboard computer system but did not impact essential controls. The impacted network was used to conduct official business, update electronic charts, manage cargo information, and communicate with onshore resources.[[11]](#footnote-12) This attack revealed the risks inherent in a common practice of transferring cargo data at the pier via USB drives, which are then plugged into ship computers without scanning for malware. In response to the attack, the U.S. Coast Guard issued a maritime security advisory warning others to implement basic cybersecurity protocols to prevent similar incidents from occurring. The advisory encouraged vessels to segment networks, install basic anti-virus software, and create a patch and update management plan.

# Appendix D: Cybersecurity Risks to Port Components

## IT and Operational Technology (OT) Systems Connectivity

OT systems are defined as systems, devices, and communications links used to control physical processes at ports, including cargo handling equipment and pumps. Connectivity between OT systems and IT systems can lead to the manipulation of OT networks via compromised IT networks and other internet connected devices. Boundary protection is the electronic division between OT and enterprise networks. If boundary protection is not developed thoroughly, access to OT networks can be manipulated via enterprise networks and other internet connected devices. Inadequate boundary protection can also make it difficult to detect unauthorized activity on systems. To mitigate threats against network boundaries, limit the number of external networks to the system, implement a managed interface for each external telecommunication service, deny network communications traffic by default, detect, and deny outgoing communications traffic posing a threat to external systems, and enforce adherence to protocol formats.

*Additional Resources*

* NIST Guide for Security Focused Configuration Management of Information Systems (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>)
* NIST SP 800-53, Rev. 5.1.1.: “System and Communications Protection (SC) – Boundary Protection”(<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-07>)
* Layering Network Security Through Segmentation (<https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>)

IT and OT Physical Access Control

Both OT and IT physical access control to limit potential malicious activity are critical in a port environment. The compromise of OT systems could cause changes to cargo movements, interrupt port operations, and cause physical damage to equipment and safety risks for personnel. To mitigate threats against physical access control locations, develop, document, and disseminate a physical and environmental protection policy, maintain a list of individuals with authorized access to the facility where systems reside, enforce physical access authorization, control physical access, monitor physical access, maintain visitor access logs, and protect equipment from damage and destruction.

*Additional Resources*

* NIST Cybersecurity Framework, v2.0 (via NIST CSRC CPRT), PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk (<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA-06>)
* Interagency Security Committee (ISC) Best practices for Facility Access Control (<https://www.cisa.gov/resources-tools/resources/isc-best-practices-facility-access-control>)

## Positioning, Navigation, and Timing (PNT)

Position, Navigation, and Timing plays an essential role in many maritime functions such as vessel navigation and port logistics. Loss of PNT services would disrupt vessel movements in the port and complex logistics systems at port facilities. Loss of PNG could also lead to collisions and allisions, resulting in potential damage to fixed infrastructure, pollution, release of hazardous material, fires, loss of life, vessel sinking and blocking of a navigable channel. Suspected PNT degradation, disruptions, and other issues or anomalies should be reported to the U.S. Coast Guard Navigation Center (<https://www.navcen.uscg.gov/>).

*Additional Resources*

* CISA Positioning, Navigation, and Timing (<https://www.cisa.gov/topics/risk-management/positioning-navigation-and-timing>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* USCG National Response Center (contact: 1-800-424-8802, <https://nrc.uscg.mil/>)
* Federal Bureau of Investigation (FBI)
* Field Office Cyber Task Forces (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)

Maritime Preparedness Resources

* Coast Guard Maritime Industry Cybersecurity Resource Center (<https://www.uscg.mil/MaritimeCyber/>)
  + Maritime Cybersecurity Assessment and Annex Guide (MCAAG) ([https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment](https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf?ver=NE11YUspj_kNa3xRoMd0TQ%3d%3d))
* Port Facility Cybersecurity Risks (<https://www.cisa.gov/resources-tools/resources/port-facility-cybersecurity-risks>)
* Maritime Transportation System Resilience Assessment Guide (<https://www.cisa.gov/resources-tools/resources/marine-transportation-system-resilience-assessment-guide>)

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
* NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Cybersecurity Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Additional Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (<https://www.isao.org/information-sharing-groups/>)
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. See, e.g. CISA Cybersecurity Advisory “APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus,” <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-259a>. [↑](#footnote-ref-3)
3. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s Cybersecurity and Privacy Reference Tool, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-4)
4. NIST CSF 2.0 via CPRT, “GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship CPG Checklist,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-07>. [↑](#footnote-ref-5)
5. NIST CSF 2.0 via CPRT, “PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA-01>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship CPG Checklist,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-07>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?keyword=incident%20response%20plan> [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “RS.CO-03: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-9)
9. Alicia Hope, “Largest Japanese Port Suffered a Russian Ransomware Attack Halting Cargo Operations,” *CPO* Magazine, July 13, 2023, <https://www.cpomagazine.com/cyber-security/largest-japanese-port-suffered-a-russian-ransomware-attack-halting-cargo-operations/>. [↑](#footnote-ref-10)
10. Sean Lyngaas, “Hackers breached computer network at key US port but did not disrupt operations,” *CNN*, September 23, 2021, <https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html>. [↑](#footnote-ref-11)
11. Jeff Stone, “After ‘significant’ malware attack, U.S. Coast Guard issues maritime security advisory,” *Cyberscoop*, July 9, 2019, <https://cyberscoop.com/coast-guard-significant-malware-attack/>. [↑](#footnote-ref-12)