FACILITY INSPECTOR – CYBER JOB AID

Sensitive Security Information (when filled out)

Facility:	**FIN:**
MISLE Activity #:	**Date:**
Unit:	**FSO:**
USCG Facility Inspector:	**FSO Phone Number**
USCG Facility inspector:	**USCG Facility Inspector:**

Facility Inspector - Cyber Job Aid – It is recommended that Coast Guard facility inspectors complete this job aid for familiarization with cyber activities at MTSA-regulated facilities. This job aid is not a substitute for applicable legal requirements, nor is it itself a rule. The inspector should consult NVIC 01-20 and applicable sections in NVIC 03-03 (current series) for references.

Preface

There are many resources, technical standards, and recommended practices available to marine industry that can help with the governance of cyber risk. Facilities are encouraged to be familiar with cyber security and cyber risk management guidance such as released by the National Institute of Standards and Technology (NIST). Coast Guard facility inspectors and facility owners/operators should be familiar with those resources to promote a culture of proactive cyber risk management.

This job aid is NOT intended to be regulatory and is only meant to assist facility inspectors in applying the cyber guidance and regulations when conducting facility inspections and reviewing cyber components of a Facility Security Assessment (FSA) and Facility Security Plan (FSP). This job aid addresses items covered by regulation as well as best practices and general cyber security observations. Checking NO on the job aid warrants further discussion with the facility and does not necessarily mean a discrepancy or violation during the inspection or review of the FSA or FSP.

Many MTSA-regulated facilities will have two separate cyber-enabled systems: Information Technology (IT) and Operational Technology (OT) based. IT systems support daily tasks associated with administration, finances, human resources, and other applications that typically support non-operational activities. Examples include computer workstations, laptops, servers, and the Internet. OT equipment supports operational activities within a facility such as chemical processing, cargo handling, and security access control. The inspector should become familiar with how OT systems interact with security access control systems and discuss with the facility. Likewise, possessing knowledge on the convergence of IT and OT systems to support daily operations within facilities is vital to understanding that traditional IT threats (such as ransomware and viruses) can affect OT operations.

Facility Cyber Security Assessments			
33 CFR 105 Reference(s)	**33 CFR 105.305 (d)(2)(v)**		
Has the facility ever conducted a cyber security assessment? *Having a third party or internal audit should address IT and/or OT cyber vulnerabilities within the facility or the organization.*	Y ☐	N ☐	N/A ☐
Are cyber security assessment reports shared with the FSO/AFSO and upper management? *The FSO/AFSO should be aware of the cyber-physical vulnerabilities and administrative network discrepancies that could lead to a security incident.*	Y ☐	N ☐	N/A ☐
If a cyber assessment has been completed, are operations personnel included in the assessment process? *Operations personnel that are knowledgeable on the OT systems within the facility can help identify cyber weaknesses and administrative vulnerabilities on the Industrial Control (ICS) systems.*	Y ☐	N ☐	N/A ☐
Is the physical infrastructure of networks and networked security equipment assessed during the annual physical security inspection?	Y ☐	N ☐	N/A ☐
Do IT staff or cyber security personnel participate in the annual physical security inspection? *If no, IT staff/cyber security personnel are highly encouraged to participate for security program integration and familiarization of FSO duties/responsibilities.*	Y ☐	N ☐	N/A ☐

Do facility IT personnel participate in the required facility security assessment? *If no, IT staff/cyber security personnel are highly encouraged to participate for security program integration and familiarization of FSO duties/responsibilities.*	Y ☐	N ☐	N/A ☐
Cyber Security Administration and Organization			
33 CFR 105 Reference(s)	**33 CFR 105.205(b)** **33 CFR 105.225(b)**		
Does the FSP address cyber security administration and organization? *The cyber/IT portion of the FSP should be written to include (but not limited to) role identifications, incident response, and risk assessments.*	Y ☐	N ☐	N/A ☐
Does the facility document end user acknowledgements? *All users (contractors and employees) should sign and acknowledge responsibilities while operating devices on the networks.*	Y ☐	N ☐	N/A ☐
Are third party users vetted prior to access into a facility network? *The facility should have a vetting process for third party companies that require access into the IT or OT networks. This includes the individuals that will be accessing the systems.*	Y ☐	N ☐	N/A ☐
Are cyber security vulnerabilities addressed during annual physical security audits? *The IT staff should accompany the FSO/AFSO during annual audits and address physical vulnerabilities that compromise the information infrastructure.*	Y ☐	N ☐	N/A ☐

Does the facility audit the integrity of information networks throughout the organization? *Internal audits of the integrity of the IT and OT networks are crucial to maintaining cyber resiliency. Examples of audits include (but are not limited to) penetration testing, updating incident response plans, verifying end user compliance with company policies. Penetration testing can include internal phishing tests, examining the overall health of the network (IT and OT) regularly, and ensuring that updates are regularly installed.*	Y ☐	N ☐	N/A ☐
Do security personnel conduct regular audits of facility access credentials? *Security personnel (under the direction of the FSO) should audit site access credentials (if using site access badges in conjunction with TWIC on a set basis to ensure unauthorized personnel do not gain access to the facility.*	Y ☐	N ☐	N/A ☐
Are cyber security audit records retained on a fixed schedule? *The facility should maintain cyber audit records (either conducted by a third party or internally) in conjunction with required physical security audit reports to maintain uniformity.*	Y ☐	N ☐	N/A ☐
Does the FSP have a system in place for revocation of physical and network access in the event of a termination, suspension, or transfer? *Discontinuing physical and network access is important to preventing an intentional insider threat in the event of a change in employment status.*	Y ☐	N ☐	N/A ☐

Does the FSP address unauthorized mobile/personal device connections into operational technology systems? *Connecting personal or unauthorized devices into either IT systems or operational technology systems presents a risk to the physical security of the facility. Malicious software could affect access control systems and software if introduced into the facility network.*	Y ☐	N ☐	N/A ☐
Personnel Training			
33 CFR 105 Reference(s)	**33 CFR 105.205** **33 CFR 105.210** **33 CFR 105.215**		
Is the FSO/AFSO required to complete cyber security awareness training for the company? *Training can include computer-based or in person courses. Training courses are effective cyber defense measures for the FSO/AFSO. These courses can either be provided by the company or third party entities.*	Y ☐	N ☐	N/A ☐
Are contract security staff/Personnel with Security Duties (PSDs) required to complete cyber security awareness training? *Training can include computer-based or in person courses. Contract security staff should have a basic understanding of cyber security threats, delivered through company-specific training entities.*	Y ☐	N ☐	N/A ☐
Is the FSO/AFSO aware of cyber security incident reporting mechanisms internally? *The FSO/AFSO should know which internal entities to notify in the event of a cyber incident.*	Y ☐	N ☐	N/A ☐

Are restrictions placed on access to sensitive files (i.e., security files, operational systems, etc.)? *Files and network folders should be restricted to certain employees and contractors, particularly security and IT records.*	Y ☐	N ☐	N/A ☐
Drills and Exercises			
33 CFR 105 Reference(s)	**33 CFR 105.220**		
Do required drills incorporate cyber security incidents?	Y ☐	N ☐	N/A ☐
Has the facility ever participated in a cyber security exercise?	Y ☐	N ☐	N/A ☐
Does the FSO incorporate IT staff into required drills? *IT staff should be involved in drills and exercises to act as subject matter experts in the event that a cyber security scenario is injected.*	Y ☐	N ☐	N/A ☐
Does the FSO incorporate facility operations personnel in cyber security drills? *Operations personnel that normally operate ICS equipment can help IT staff and security staff identify shortfalls in network security during a drill/exercise and provide subject matter expertise.*	Y ☐	N ☐	N/A ☐
Does the FSO incorporate contract security staff into cyber security drills? *Contract security staff should be included in cyber security drills and exercises to ensure involvement in preventing a cyber security incident at the facility and on access control and other security systems.*	Y ☐	N ☐	N/A ☐
Do drills and exercises guide cyber security development and policy? *Drills and exercises should guide the continual development of cyber security in the FSP.*	Y ☐	N ☐	N/A ☐

Records and Documentation			
33 CFR 105 Reference(s)	**33 CFR 105.225**		
Does the facility keep records of cyber incidents? *Records may be kept in electronic format and should be protected against unauthorized deletion, destruction, or amendment.*	Y ☐	N ☐	N/A ☐
Are records of cyber security audits marked and stored as SSI?	Y ☐	N ☐	N/A ☐
Does IT staff keep and maintain a record of suspicious network activity? *Records of suspicious network activity should be conveyed to the FSO/AFSO for situational awareness, particularly if the activity is discovered on or affects security systems.*	Y ☐	N ☐	N/A ☐
Response to Change in MARSEC Level			
33 CFR 105 Reference(s)	**33 CFR 105.230**		
Are facility IT staff aware of physical security requirements for an increase in MARSEC level? *IT/cyber security staff should be aware of the FSP's requirements and responses to an increase in MARSEC level for network security.*	Y ☐	N ☐	N/A ☐
Do facility IT staff have a site-wide response to an increase in MARSEC level? *The FSO should be proactive in conveying the physical security requirements for MARSEC level increases and likewise address potential cyber vulnerabilities in the facilities' networks with IT staff.*	Y ☐	N ☐	N/A ☐
Does the facility have offsite backup for security systems?	Y ☐	N ☐	N/A ☐

Communications			
33 CFR 105 Reference(s)	**33 CFR 105.235**		
Does the facility understand cyber Breach of Security and Suspicious Activity incident reporting requirements? *Reference: COMDT (CG-5P) Policy Letter 08-16 – Reporting Suspicious Activity and Breaches of Security*	Y ☐	N ☐	N/A ☐
Are cyber incidents reported to company management for future mitigation policies?	Y ☐	N ☐	N/A ☐
Procedures for Interfacing with Vessels and Segmented Networks			
33 CFR 105 Reference(s)	**33 CFR 105.240** **33 CFR 105.245**		
Is cyber security awareness included as part of the Declaration of Security (DOS) process? *The FSO (or designate) should address cyber security concerns such as connecting to onshore networks with the VSO in the DOS process.*	Y ☐	N ☐	N/A ☐
Does the FSO (or designee) discuss reporting suspicious cyber activity with a visiting vessel? *The FSO (or designee) should be proactive in discussing cyber incident prevention measures with the Vessel Security Officer (VSO).*	Y ☐	N ☐	N/A ☐
Are visiting vessels required to connect to a facility based network system? *Operations and IT staff should communicate vulnerabilities and weaknesses discovered in shore-to-ship network connections (if available).*	Y ☐	N ☐	N/A ☐
Are visiting vessels able to connect to facility wireless networks? *Facilities should not have open wireless networks, but instead have a password-enabled system to ensure no breaches of security occur over the network.*	Y ☐	N ☐	N/A ☐

Security Systems and Equipment Maintenance			
33 CFR 105 Reference(s)	**33 CFR 105.250**		
Are access control systems and software updated on a set schedule?	Y ☐	N ☐	N/A ☐
Do access control systems receive software/firmware updates?	Y ☐	N ☐	N/A ☐
Does the FSO/AFSO or any other facility employee have the ability to remotely access security systems? *Remote access should not be discouraged. Instead, proper security protocols should be in place to mitigate the chance of a cyber incident. Examples include strong passwords, use of a Virtual Private Network (VPN), and using trusted networks. The FSO/AFSO should team with IT staff to ensure maximum protection for remote access requirements.*	Y ☐	N ☐	N/A ☐
Are contractors or third party vendors vetted prior to introducing any devices to systems supporting the security program?	Y ☐	N ☐	N/A ☐
Security Measures for Access Control			
33 CFR 105 Reference(s)	**33 CFR 105.255**		
Are devices and controllers for access control points kept locked in tamper-proof casings within the MTSA-regulated footprint (i.e., turnstile controllers)?	Y ☐	N ☐	N/A ☐
Are contract security staff routinely checking access control devices and controllers at entry points?	Y ☐	N ☐	N/A ☐
Does the facility have designated personnel who monitor digital access control networks?	Y ☐	N ☐	N/A ☐
Are access control servers kept locked in restricted areas in the facility?	Y ☐	N ☐	N/A ☐
Are security camera servers or supporting equipment kept locked in restricted areas in the facility?	Y ☐	N ☐	N/A ☐
Are access control computers, access control equipment, and access control records kept on backup power?	Y ☐	N ☐	N/A ☐

Does the facility employ fire protection systems for the information infrastructure?	Y ☐	N ☐	N/A ☐
Are access control points and equipment on backup power?	Y ☐	N ☐	N/A ☐
Are security staff able to connect to outside connections that are not password protected or encrypted (i.e., open Internet) on devices supporting access control?	Y ☐	N ☐	N/A ☐
Does the facility keep a record of vendors/visitors that require access into the networks on the facility?	Y ☐	N ☐	N/A ☐
Are there different levels of access for credentialing software?	Y ☐	N ☐	N/A ☐
Do workstations automatically lock during inactivity?	Y ☐	N ☐	N/A ☐
Security Measures for Restricted Areas			
33 CFR 105 Reference(s)	**33 CFR 105.260**		
Are spaces containing digital infrastructure locked or have access control systems in place? *Examples include server rooms, control rooms, access control equipment boxes, and central computer operating terminals.*	Y ☐	N ☐	N/A ☐
Are spaces containing digital infrastructure marked as restricted areas?	Y ☐	N ☐	N/A ☐
Are site-wide alarm computers physically secure?	Y ☐	N ☐	N/A ☐
Is there a key control program in place throughout the facility for restricted areas containing digital infrastructure?	Y ☐	N ☐	N/A ☐
Can facility contractors access restricted areas containing digital infrastructure?	Y ☐	N ☐	N/A ☐

Security Measures for Handling Cargo			
33 CFR 105 Reference(s)	**33 CFR 105.265**		
Do facility operators require portable media (i.e. hard drives, flash drives, etc.) exchanges during cargo handling? *Uncontrolled use of removable/portable media can increase the risk of malware being transferred to critical network systems.*	Y ☐	N ☐	N/A ☐
Does the facility allow wireless connections between ship and shore for cargo handling?	Y ☐	N ☐	N/A ☐
Are interconnections shared between vessels and shoreside systems?	Y ☐	N ☐	N/A ☐
Does the facility allow remote access for cargo handling?	Y ☐	N ☐	N/A ☐
Would the facility restrict interconnections for MARSEC level increases?	Y ☐	N ☐	N/A ☐
Security Measures for Delivery of Stores			
33 CFR 105 Reference(s)	**33 CFR 105.270**		
Does the facility require any third-party access to IT systems for the delivery of stores?	Y ☐	N ☐	N/A ☐
Does the facility have processes in place to protect electronic files associated with the scheduling and delivery of stores?	Y ☐	N ☐	N/A ☐
Are remote-controlled gates or doors used in the secure-restricted portion of the facility for store delivery?	Y ☐	N ☐	N/A ☐
Security Measures for Monitoring			
33 CFR 105 Reference(s)	**33 CFR 105.275**		
Does the facility monitor networks that contain operational security equipment for unauthorized activity? *Examples of operational security equipment include cameras, access control systems, intrusion detection systems, and credentialing applications.*	Y ☐	N ☐	N/A ☐

Are physical security measures in place to monitor physical access to central servers or controllers that support OT throughout the facility?	Y ☐	N ☐	N/A ☐
Facility Security Plan (FSP) – Cyber Annex			
33 CFR 105 Reference(s)	**33 CFR 105.400(a)(3)**		
Does the FSP address cyber security?	Y ☐	N ☐	N/A ☐
If the facility has a cyber annex to their FSP, proceed to the below questions			
Is the cyber security annex marked as SSI?	Y ☐	N ☐	N/A ☐
Does the cyber security annex to the FSP include incident response roles?	Y ☐	N ☐	N/A ☐
Is the FSO/AFSO familiar with the cyber security elements in the FSP or cyber security annex?	Y ☐	N ☐	N/A ☐
Is cyber security referenced in drills/exercises section?	Y ☐	N ☐	N/A ☐
Audits and Security Plan Amendments			
33 CFR 105 Reference(s)	**33 CFR 105.415(b)**		
Are cyber security audits conducted at a set frequency?	Y ☐	N ☐	N/A ☐
Does the FSO/AFSO participate in cyber security audits?	Y ☐	N ☐	N/A ☐
Are corrective action plans written after cyber security audits?	Y ☐	N ☐	N/A ☐
If a cyber annex to the FSP is kept at the facility or by facility corporate offices, is the annex updated to reflect vulnerabilities found during previous cyber incidents?	Y ☐	N ☐	N/A ☐

Appendix A

Terms

- **Assessment:** Evaluation against "best practices"
- **Audit:** Evaluation of compliance to a "standard"
- **IP Address:** Label assigned to a network device that communicates with the Internet Protocol
- **Network Scan:** Method of interrogating network devices over the "wire"
- **Penetration (pen) testing:** Method of testing a computer, network, web application for vulnerabilities
- **Security Integrator:** Third party vendor that provides security equipment and performs maintenance to a facility
- **Vulnerability:** A flaw in the system that can be open to attack/failure

Acronyms

- **AFSO:** Alternate Facility Security Officer
- **CBT:** Computer-Based Training
- **CISA:** Cybersecurity and Infrastructure Security Agency
- **FSO:** Facility Security Officer
- **ICS:** Industrial Control Systems
- **IT:** Information Technology
- **NIST:** National Institute of Standards and Technology
- **OT:** Operational Technology
- **PSD:** Personnel with Security Duties
- **SSI:** Sensitive Security Information
- **VSO:** Vessel Security Officer

Resources

- Maritime Transportation Security Act (MTSA) of 2002, Public Law 107-295
- Navigation and Vessel Inspection Circular No. 01-20 (current series), Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities
- Navigation and Vessel Inspection Circular No. 03-03 (current series), Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities
- Navigation and Vessel Inspection Circular No. 09-02 (current series), Guidelines for the Area Maritime Security Committees and Area Maritime Security Plans for U.S. Ports
- CG-5P Policy Letter 08-16, Reporting Suspicious Activity and Breaches of Security
- National Institute of Standards and Technology (NIST) SP 800-53, Rev 4