U.S. COAST GUARD Homeland Security

FACILITY INSPECTOR - CYBER JOB AID
Revision 2

Facility:	**FIN:**
MISLE Activity #:	**Date:**
Unit:	**Facility Security Officer (FSO):**
USCG Facility Inspector:	**FSO Phone Number**
USCG Facility inspector:	**USCG Facility Inspector:**

Facility Inspector - Cyber Job Aid – It is recommended 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 (current series) 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, nor does it create any regulatory requirements 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 a crossover of existing MTSA regulations over to general cyber security practices to give the inspector an idea of the cyber security reference. During the Facility Security Assessment (FSA), the facility should address cyber security vulnerabilities applicable to the facility using an internal, documented cyber security method and/or the current series of NVIC 01-20. Selecting the "NO" checkbox on the job aid does not mean a discrepancy or violation during the inspection or review of the FSA or FSP but warrants further discussion with the facility. The inspector should never issue a Notice of Violation (NOV) based solely on information provided in this job aid.

Many MTSA-regulated facilities will have two or more, function-independent, but connected 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, etc. These networks may also be referred to as Process Control Networks (PCNs) or Industrial Networks. The inspector should become familiar with how OT systems interact with security access control systems and discuss this with knowledgeable personnel within the facility. Likewise, understanding how the convergence of IT and OT systems support daily operations within facilities is vital to understanding how traditional IT threats (such as ransomware and viruses) can affect facility operations.

To further knowledge about facility cyber security, the FSO should invite the IT/cyber security staff to participate (at the facility discretion) in the annual physical security inspection to encourage interaction between the USCG Facility Inspectors and to address any cyber security-related questions identified during the inspection process. Additionally, the FSO and facility IT/cyber security staff should interact with the regional Area Maritime Security Committee (AMSC) to discuss cyber security concerns and obtain best practices from other participants and receive cyber security bulletins from government resources.

By no means should this job aid be used as a regulatory document during the inspection process.

Administrative Controls			
Has the facility implemented an internal cyber security policy or governance? **Reference:** 33 CFR 105.400, 33 CFR 105.405	Y ☐	N ☐	N/A ☐
Has the facility incorporated cyber security into the Facility Security Assessments? Supporting Factors: - *Does the Facility Security Assessment (FSA) include cyber vulnerabilities?* - *Does the recent CG-6025 address mitigations for identified cyber security vulnerabilities?* **Reference:** 33 CFR 105.305(c)(1)(v); 105.405(a)(17)	Y ☐	N ☐	N/A ☐
Does the FSP incorporate cyber security into facility security administration and organization? Supporting Factors: - *Do IT/cyber security personnel regularly interact with the FSO?* - *Does the organization have a competent representative (FSO or otherwise) to satisfy FSO cyber security responsibilities?* - *Do annual security audits incorporate cyber components and the facility IT/cyber security staff?* - *Are suspicious cyber activities and Breaches of Security (BoS) documented?* - *Are security personnel aware of Suspicious Activity (SA) and Breach of Security (BoS) reporting requirements as per the CG-5P Policy Letter 08-16 (current series)?*	Y ☐	N ☐	N/A ☐

- *Are sensitive digital records, associated to and/or a part of the FSP, protected (e.g., encryption) and marked as Sensitive Security Information (SSI)? Examples include facility maps, digital copies of BoS records, etc.)* - *Does the FSP include cyber-breach incident response policy and procedures?* - *Does the facility notify the National Response Center (NRC) in the event of a significant cyber incident?* **Reference:** 33 CFR 105.400; 105.405			
Does the facility incorporate IT staff into security drills? Supporting Factors: - *Involving IT staff in drills and exercises would reinforce a working relationship between the FSO and IT/cyber security staff and greatly improve interoperability in the event of a real-world cyber security event.* **Reference:** 33 CFR 105.220	Y ☐	N ☐	N/A ☐
Does the facility require cyber security training awareness for personnel with access into information systems? Supporting Factors: - *Examples of training include annual computer-based training.* - *Are contractors or other third-party vendors with access to information systems required to complete cyber security training?* **Reference:** 33 CFR 105.205; 105.210; 105.215	Y ☐	N ☐	N/A ☐

Physical and Technical Controls			
Does the facility practice access control measures on information systems? Supporting Factors: - *Does the facility have an inventory of hardware/software assets used throughout the MTSA regulated footprint of the facility?* - *Does the facility restrict access to sensitive security information (data) and operational technology?* - *Does the facility remove network access for former employees, temporary personnel, contractors, and guests (e.g., off-boarding policy)?* - *Does the facility require credentialing (such as usernames/passwords) for access to SSI or operational technology networks?* - *Does the facility use network traffic control devices (firewalls, Intrusion Detection/Protection Systems) to prevent unauthorized network activity?* - *Are servers and network equipment that control operational technology, and/or contain SSI, secured from physical access?* - *Are the networks configured to minimize the likelihood of unauthorized movement from IT networks to Restricted/Secure Area networks? (Such as firewalls and other network separations)* **Reference:** 33 CFR 105.255	Y ☐	N ☐	N/A ☐
Is cyber factored into physical security measures? Supporting Factors: - *Are physical network infrastructure, which are connected to facility networks and/or sensitive security information (data), physically protected from individuals not cleared for restricted/secure area access?*	Y ☐	N ☐	N/A ☐

- *Are devices and networks that contain sensitive security information (data) (or are involved in process control) located in areas labeled "Restricted Area" or "Secure Area"?* **Reference:** 33 CFR 105.260			
Has the facility incorporated cyber security capabilities into measures for monitoring? Supporting Factors: - *Does the facility monitor networks connected to process control or traditional business networks containing SSI?* **Reference:** 33 CFR 105.275	Y ☐	N ☐	N/A ☐
Does the facility incorporate hardware and software into equipment maintenance? Supporting Factors: - *Are critical systems regularly patched or maintained?* - *If no, does the facility record the vulnerability via CG-6025 or alike, and provide a means of mitigating the vulnerability that would be remedied by the patch (patch management policy)?* **Reference:** 33 CFR 105.250	Y ☐	N ☐	N/A ☐
Does the facility consider cyber in their policy for interfacing with vessels and segmented networks? Supporting Factors: - *Is cyber security referenced during the Declaration of Security (DoS) process?* - *Does the facility have established procedures for vessels that connect to a shoreside network (e.g., guest network)?*	Y ☐	N ☐	N/A ☐

- *Does the facility discuss the discovery and reporting of Suspicious Activities/Breaches of Security pertinent to cyber security with the vessel?* **Reference:** 33 CFR 105.240, 33 CFR 105.245			

Appendix A

Terms

- **Assessment:** Evaluation using "best practices" in cyber security to include internally derived assessments, third party assessments, and/or recognized cyber security standards (such as the NIST Cyber Security Framework)
- **Audit:** Evaluation of compliance to a "standard" using internally derived checks and/or third party to verify the effectiveness of the cyber security stance of the facility.
- **Network Monitoring:** Continual checking, supervising or critically observing network activity and status in order to identify changes from expected parameters.
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.

Resources

- Maritime Transportation Security Act (MTSA) of 2002, Public Law 107-295 (codified as amended at 46 U.S.C. 70101-70125)
- Navigation and Vessel Inspection Circular No. 01-20 (series), Guidelines forAddressing Cyber Risks at MTSA Regulated Facilities
- Navigation and Vessel Inspection Circular No. 03-03 (series), Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of2002 (MTSA) for Facilities
- Navigation and Vessel Inspection Circular No. 09-02 (series), Guidelines for theArea Maritime Security Committees and Area Maritime Security Plans for U.S. Ports
- CG-5P Policy Letter 08-16 (series), Reporting Suspicious Activity and Breaches of Security National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)