



USCG Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI)



| | | | | | |
|-------------|---|------------|---------|-----------|-----|
| Category | Commercial Vessel Compliance (Domestic and Foreign Vessels) | | | | |
| Title | Vessel Cyber Risk Management Work Instruction | | | | |
| Serial | CVC-WI-027(1) | Orig. Date | 27OCT20 | Rev. Date | N/A |
| Disclaimer: | <p>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 part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at CG-CVC@uscg.mil who is responsible for implementing this guidance.</p> | | | | |
| References: | <p>(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems"</p> <p>(b) U.S. Coast Guard Cyber Strategy, June 2015</p> <p>(c) International Safety Management (ISM) Code</p> <p>(d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(1))</p> <p>(e) Title 33 Code of Federal Regulations (CFR) Part 96</p> <p>(f) Chapter IX, Management of the Safe Operation of Ships, International Convention for the Safety of Life at Sea (SOLAS), 1974</p> <p>(g) Title 33 Code of Federal Regulations (CFR) Subchapter H</p> <p>(h) National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018</p> <p>(i) Navigation and Vessel Inspection Circular (NVIC) 04-05: "Port State Control Guidelines for the Enforcement of Management for the Safe Operation of Ships (ISM Code)"</p> <p>(j) "Guidelines for Port State Control Officers on the International Safety Management (ISM) Code," MSC-MEPC.4/Circ.4</p> <p>(k) USCG Oversight of Safety Management Systems on U.S Flag Vessels, (CVC-WI-003(1))</p> <p>(l) Maritime Safety Committee / Facilitation Committee Circular 3 "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3</p> <p>(m) USCG Assistant Commandant for Prevention Policy (CG-5P) Policy Letter 08-16 "Reporting Suspicious Activity and Breaches of Security"</p> | | | | |

- A. **Purpose.** Reference (a) calls for Safety Management Systems required under the ISM Code to address cyber risks. This work instruction (WI) provides guidance regarding the U.S. Coast Guard (USCG) commercial vessel compliance program's approach to assessing the cyber risk on vessels to ensure vessels do not pose a risk to the Marine Transportation System (MTS) due to a cyber event.
- B. **Action.** Marine Inspectors (MIs) and Port State Control Officers (PSCOs) should be familiar with reference (b) and use the guidance provided in this WI to evaluate how well a vessel's Safety Management System (SMS) complies with references (a) and (c-f). Additionally, this WI provides guidance to MIs when assessing cyber risk management onboard non-SMS U.S. vessels. Lastly, this WI discusses use of COTP orders and CG-835Vs to control vessels that have been affected by a cyber incident, and responding to a reported or probable cyber incident affecting the seaworthiness of a vessel.

U.S. flagged vessels subject to reference (c) are required to evaluate cyber risk and establish procedures to respond to a cyber-attack as per reference (d). Starting January 1, 2021, all vessels with a Safety Management System (SMS) pursuant to reference (a) should address cybersecurity risk

with respect to references (c) and (e). The January 2021 requirement also applies to vessels that voluntarily comply with reference (e).

- C. Background. As maritime operations become more reliant on the systems integrated through automation, cyber risk is an area of increasing concern in the Marine Transportation System. The USCG recognizes that not all shipping companies and ships are alike, and therefore the SMS provides shipping companies the ability to tailor a structured system to address evolving cybersecurity vulnerabilities unique to a company/vessel's specific management and operations.
1. MSC-FAL.1/Circ 3. Reference (l) contains high-level recommendations to maritime stakeholders on assessing maritime cyber risk management. This IMO circular refers to several standards to help identify and mitigate cyber risks, including five functional elements consistent with the NIST Framework:
 - a. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
 - b. Protect: Implement risk control processes and measures, and contingency planning to protect against cybersecurity events and ensure continuity of shipping operations.
 - c. Detect: Develop and implement activities necessary to detect a cybersecurity event in a timely manner.
 - d. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
 - e. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cybersecurity event.
 2. Other international organizations (ISO/IEC), including shipping associations (BIMCO), have provided maritime cybersecurity guidance and best practices for industry stakeholders. A MI/PSCO may encounter a vessel managing cyber risk using these standards in lieu of the NIST framework.
- D. Definitions.
1. *Company Security Officer (CSO)*. The person designated by the Company as responsible for the security of the vessel, including implementation and maintenance of the vessel security plan, and for liaison with their respective Vessel Security Officer and the USCG (reference g).
 2. *Cybersecurity*. The prevention of damage to, unauthorized use, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. This includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, communications systems and control systems required for safe shipboard navigation and operations (annotated from reference m).
 3. *Cybersecurity Event*. A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation (reference h).
 4. *Cybersecurity Incident*. Actions taken through the use of a computer networks that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (reference m).
 5. *International Safety Management (ISM) Code*. The International Management Code for the Safe Operation of Ships and Pollution Prevention, Chapter IX of the Annex to the International Convention for the Safety of Life at Sea (SOLAS), 1974 (references c and e).

6. *Major non-conformity*. An identifiable deviation, which poses a serious threat to personnel or vessel safety or a serious risk to the environment and requires immediate corrective action. The lack of effective and systematic implementation of an ISM Code requirement is also considered a major non-conformity (reference c and e).
7. *Non-conformity*. An observed situation where objective evidence indicates the non-fulfillment of a specified requirement (reference c and e).
8. *Objective Evidence*. Quantitative or qualitative information, records or statements of fact pertaining to safety or to the existence and implementation of a SMS element based on observation, measurement or test and which can be verified (reference c and e).
9. *Safety Management System (SMS)*. A structured and documented system enabling company and vessel personnel to effectively implement the responsible person's safety and environmental protection policies (reference c and e).
10. *Vessel Security Assessment (VSA)*. An analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, consequences and existing protective measures, procedures and operations (reference g).
11. *Vessel Security Plan (VSP)*. A plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes and persons on board at the respective Maritime Security (MARSEC) levels (reference g).
12. *Vessel Security Officer (VSO)*. The person onboard the vessel who is accountable to the Master and designated by the Company as responsible for the security of the vessel, including implementation and maintenance of the vessel security plan, and for liaison with their respective Company Security Officer and the Facility Security Officer (FSO) (reference g).

E. Discussion.

1. Per reference (d), as a Flag Administration, the USCG expects that U.S. flagged vessels and companies will incorporate cyber risk management into their SMS. Additionally, as a port state, pursuant to reference (a), companies with foreign flagged vessels that call on ports in the U.S. should ensure cyber risk management is appropriately addressed in their SMS no later than the first annual verification of the company's Document of Compliance (DOC) after January 1, 2021.
2. This WI also contains guidance regarding those vessels that are not required to implement and maintain a SMS, but are required to maintain a VSP as per reference (g). MIs should keep in mind that a VSP might include measures taken to mitigate cyber related vulnerabilities that the ship would be required to follow in order to meet 33 CFR part 104.
3. For the purposes of this WI, USCG vessel compliance activities are only directed towards cyber risk management on systems that are critical to the safe operation and navigation of the vessel. Stand-alone computers or other systems which do not affect the safe operation or navigation of the vessel are not to be inspected or examined.

F. Vessels subject to the ISM Code (U.S. & Foreign Vessels).

1. Basic Cyber Hygiene. The MI/PSCO shall identify when basic cyber hygiene procedures are not in place onboard. These include, but not limited to the following:
 - a. Poor cyber hygiene
 - 1) Username / Password openly displayed
 - 2) Computer system appears to require a generic login or no login for access

- 3) Computer system does not appear to automatically log out after extended period of user inactivity
- 4) Heavy reliance on flash drive/USB media use
- b. Shipboard computers readily appear to have been compromised by ransomware/excessive pop-ups
- c. Officers/crew complain about unusual network issues and reliability impacting shipboard systems
- d. Unit/vessel screener received potential ‘spoofed’ email from master/crew onboard.

If these observations are not directly linked to statutory requirements or are not technical or operational-related deficiencies, the MI/PSCO does not have clear grounds to conduct a more detailed inspection. However these vulnerabilities should be discussed directly with the master. In addition, these discussions shall be annotated in the MISLE inspection narrative and documented with a deficiency entered into MISLE marked “Worklist Item/Do Not Show in PSIX” for data analysis.

2. Guidance for assessing cybersecurity onboard a vessel subject to the ISM Code. During the course of a normal inspection/examination, the MI/PSCO should evaluate whether or not a cybersecurity event was a factor in the failure of a system required for the safe navigation or operation of the vessel.

Example: While aboard a ship for a PSC exam the 2nd Officer explains that the ECDIS is not operational after a recent electronic chart update. The PSCO asks the 2nd Officer what is the procedure to update the ECDIS? The 2nd Officer explains that the ECDIS is updated via a flash drive loaded with updates from a shipboard computer (this scenario continues throughout the work instruction).

Up to this point the PSCO is still trying to determine why a piece of equipment required for the safe navigation of the vessel is not operating properly. SOLAS Regulation V/27 requires all nautical charts necessary for the intended voyage shall be adequate and up to date. Since the ECDIS is not operational, the applicable SOLAS Regulation is not met.

(Example continued) The PSCO continues by querying the 2nd Officer if the flash drive was scanned for viruses/malware prior to connecting to the ECDIS, and they state “no.” At this point, poor cyber hygiene may have occurred and the PSCO has established clear grounds to conduct a more detail exam including the cyber risk management portion of the SMS.

3. More Detailed Inspection (Expanded Exam). If clear grounds are established, the MI/PSCO should conduct a more detailed inspection consistent with the applicable guidance for a foreign or U.S. vessel in accordance with reference (j) or (k), respectively. Based on objective evidence, the MI/PSCO may discover and can issue deficiencies based on the portion of the SMS that is not being effectively implemented with respect to cyber risk management. A more detailed inspection does NOT automatically mean that an ISM deficiency exists. MI/PSCO should NOT direct the ship to create any checklists or procedures with respect to cyber risk management. A MI aboard a U.S. vessel may review internal audits and corrective action reports while conducting a more detailed inspection.

(Example continued) The PSCO reviews the cyber security portion of the vessel’s SMS. The SMS requires all thumb drives to be scanned for malware prior to connection to a ship’s

computer/system. Since the 2nd Officer has already stated that the thumb drive was not scanned, there exists an ISM deficiency.

4. Deficiencies. If objective evidence is identified indicating that the vessel failed to implement its SMS with respect to cyber risk management, the MI/PSCO should direct the vessel to take the following actions:
 - a. For U.S. Vessels:
 - 1) MIs should follow the guidance in reference (k) which sets forth guidance for assessing the effectiveness of a company's SMS on U.S. flag vessels
 - b. For Foreign vessels:
 - 1) If cyber risk management has not been incorporated into the vessel's SMS by the company's first annual verification of the DOC after January 1, 2021, a deficiency should be issued with action code 30 – *Ship Detained*, with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.
 - 2) When objective evidence indicates that the vessel failed to implement its SMS with respect to cyber risk management, then the PSCO should issue a deficiency for both the operational deficiency and an ISM deficiency with an action code 17 – *Rectify Prior to Departure* and require the vessel to conduct an internal audit, focused on the vessel's cyber risk management, within 3 months or, prior to returning to a U.S. port after sailing foreign.
 - 3) When objective evidence indicates there is a serious failure to implement the SMS with respect to cyber risk management that directly resulted in a cybersecurity incident impacting ship operations (e.g. diminished vessel safety/security, or posed increased risk to the environment), after gaining concurrence from the OCMI, the PSCO should issue a deficiency for both the operational deficiency and an ISM deficiency with action code 30 – *Ship Detained* with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.
 - c. With the exception of U.S. vessels described in a.1 above, deficiencies issued with respect to ISM and cybersecurity should be assigned deficiency code 15113 (Other ISM) on the respective deficiency form (PSC Form B) and entered into MISLE marked "Worklist Item/Do Not Show in PSIX" and include the word 'CYBERSECURITY-ISM' at the beginning to aid with data analysis.

G. Non-SMS U.S. Vessels subject to MTSA.

1. VSA. A vessel owner or operator must consider cybersecurity vulnerabilities when conducting the vessel's VSA in accordance with 33 CFR 104.305. Cybersecurity vulnerabilities should be addressed per 33 CFR 104.305(d)(2)(v) and 33 CFR 104.305(d)(2)(vi).
2. Questions for MIs to ask during Maritime Transportation Security Act (MTSA) Verifications.
 - a. *Does your VSP address measures taken to address cybersecurity vulnerabilities?*
 - If yes: *Are these measures in place?*
 - 1) If yes: No further action/questions.
 - 2) If no, then ask: *Have you communicated that issue to your CSO?*
 - i. If yes: No further action/questions required.
 - ii. If no: Issue deficiency as per paragraph G.3 below.

- If no, then ask: *Has the vessel experienced any cybersecurity events¹ within the past 12 months?*

1) If yes, then ask: *Have you reported these cybersecurity incidents to your CSO?*

- i. If yes: Reasonably verify reporting to CSO, then no further action.
- ii. If no: Issue deficiency as per paragraph G.3 below.

2) If no: No further action/question required.

3. Issuing Deficiencies for cyber-related issues. As per the guidance in the paragraph above, MIs should issue a deficiency (Code 50; 30 days to rectify) on an CG-835V directing the VSO to submit cyber-related issues to the CSO as per 33 CFR 104.215(e). Deficiencies issued as described above with respect to MTSA and cybersecurity should be assigned deficiency code 16107 (Other Maritime Security) on the CG-835V and MISLE. The MI shall ensure that the “Security Violation” is checked for the deficiency in MISLE to prevent inadvertent release of Sensitive Security Information (SSI). The deficiency description in MISLE must include ‘CYBERSECURITY-MTSA’ at the beginning to aid with the data analysis.

H. Considerations for all reportable marine casualties. When attending a vessel for a damage survey, in-service inspection or port state control exam following a report of a marine casualty (as defined by 46 CFR 4.05-1) the MI/PSCO or Investigating Officer (IO) should always consider the possibility of the incident being related to a cybersecurity event in cases where system/equipment failure have no obvious causes. MIs/PSCO/IO should utilize the procedures outlined above to assist with this determination. The MI/PSCO/IO should determine if there was a failure of a system required for the safe navigation or operation of the ship, and then determine if it was a cybersecurity event. After making this determination, the MI/PSCO/IO ensure that the owner or operator promptly report the incident to the National Response Center (NRC) or the Department of Homeland Security National Communications and Cybersecurity Information Center (NCCIC) to initiate a coordinated federal response.

I. Reporting of cybersecurity events. See reference (m) when determining if a cybersecurity event and/or incident needs to be reported by the vessel owner/operator to the NRC or NCCIC.

J. Responding to a cybersecurity event / cybersecurity incident / marine casualty. The OCMI may request CGCYBER Cyber Protection Team (CPT) support through the District/Sector Command Center when the cybersecurity incident has impacted the MTS (i.e. vessel unable to move from loading terminal, casualty that limits or prevents movement of other vessel traffic on the waterway). The CPT can be contacted via the CG Cyber Command watch at (202) 372-2904 or at CyberWatch@uscg.mil. A MI/PSCO should be prepared to attend a vessel when a cybersecurity event onboard has been deemed a cybersecurity incident (see definition above). An onboard attendance to the vessel may be necessary to evaluate whether vital systems for safety, security, and environmental protection have been affected by a cybersecurity incident or remain functioning as required. If these systems were impacted, then the MI/PSCO should take actions to ensure these vital systems are fully restored.

K. Captain of the Port (COTP) Order. The COTP order is most appropriate and effective tool for control of a U.S. or Foreign Flagged vessel experiencing a cybersecurity incident that impacts

¹ Examples of cybersecurity events include: Intrusions into telecommunications equipment, computer, and networked systems linked to security plan functions (e.g. access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS. Also, instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers that are linked to security plan functions.

systems necessary for the safe operation of the vessel. The COTP should issue the order in the same manner that a COTP order would be issued for inoperable essential shipboard equipment with an unknown cause (e.g. loss of propulsion or steering reported to the USCG prior to troubleshooting issue). The COTP order imposes the minimal vessel control actions necessary to limit the vessel's effect on the MTS or facility until the issue has been identified and corrective measures put in place. For example, if the vessel's propulsion system was potentially involved in a cybersecurity incident, the COTP order could direct the vessel to proceed to the nearest anchorage, utilize tug escort, or accept a master attestation indicating vital systems are operational for mooring/anchoring/cargo operations. COTPs should also consider the extent of the cyber event onboard when imposing vessel control actions. A cyber event that affects shipboard control systems is much more serious than a cybersecurity event onboard affecting a non-integrated shipboard computer/device (e.g. malware, virus, ransomware). For example, a ransomware affecting shipboard computers used for communicating with the shoreside company, arranging logistics and cargo operations may not require a COTP order for tugs or to direct the vessel to anchor. However, it may be appropriate to prohibit shoreside connections until the extent of the cyber event has been determined.

- L. COTP Order vs. CG-835V. For the purposes of safeguarding the MTS, the COTP order is the most effective and primary tool for controlling a vessel experiencing a cybersecurity incident. A CG-835V may be issued to a U.S. vessel to require repairs or corrective action to a specific regulation.
- M. Training. MIs/PSCOs shall view and understand the basic maritime cybersecurity principles in the [Maritime Cybersecurity Webinar posted on the CG-FAC website](#). Additionally, MIs/PSCOs should have a basic understanding of reference (h), particularly how the framework would apply in the maritime setting.
- N. Appeals. The appeal procedure for decisions made by the Officer in Charge of Marine Inspections (OCMI) is outlined in 46 CFR Subpart 1.03. The appeal procedure for decisions made by COTP, under 33 CFR Subchapter H, should follow the appeal procedures outlined in 33 CFR 101.420.
- O. Questions. All questions and comments regarding this policy can be sent to the Office of Commercial Vessel Compliance at CG-CVC@uscg.mil (U.S. Flag Vessels) or PortStateControl@uscg.mil (Foreign Flag Vessels).

M. EDWARDS
Captain, U.S. Coast Guard
Chief, Office of Commercial Vessel Compliance
By direction