U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard
Washington, DC 20593-7501
Staff Symbol: CG-5PC
Phone: (202) 372-1107

16601
CG-5PC
Policy Letter 01-25
October 9, 2025

From: Robert C. Compher, CAPT
COMDT (CG-5PC)

To: Distribution

Subj: CYBERSECURITY TRAINING FOR PERSONNEL WITH ACCESS TO INFORMATION TECHNOLOGY OR OPERATIONAL TECHNOLOGY SYSTEMS

Ref: (a) Title 33, Code of Federal Regulations (CFR), Part 101.650 (d)

1. Purpose. This policy provides guidance for the cybersecurity training required by reference (a) which has a January 12, 2026, deadline for completion.

2. Action. The Coast Guard will use this policy to aid in the verification of training requirements outlined in reference (a).

3. Directives Affected. None.

4. Disclaimer. This policy letter is not intended to, nor does it, impose legally binding requirements on any party. The regulatory requirements in reference (a) remain in effect and are unchanged by this policy letter.

5. Background. 33 CFR Part 101, Subpart F – Cybersecurity became effective on July 16, 2025. This subpart set minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities to safeguard and ensure the security and resilience of the Marine Transportation System (MTS). Reference (a) requires owners/operators of U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR parts 104, 105, and 106 to complete the specified training by January 12, 2026.

6. Applicability. This policy letter applies to all personnel with access to U.S.-flagged vessel, facility, and OCS facility Information Technology (IT) and/or Operational Technology (OT) systems, including contractors, whether part-time, full-time, temporary, or permanent. Enclosure (1) provides a quick reference for the various training requirements and associated timeframes.

7. Definitions. Below are two definitions to be used as supplemental guidance in addition to the definitions found in 33 CFR § 101.615.
    a. *Access* means the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. Access is typically granted based on user credentials and permissions, ensuring only authorized individuals can interact with the system. Access can be gained through physical access to a device (for example, plugging in a USB drive) or logical access (for example, logging into a network). Personnel with unrestricted physical access to spaces or areas housing IT and/or OT equipment, regardless of logical access, are considered to have access for the purposes of this section.
    b. *Key Personnel* are determined by the owner/operator but, in general, are individuals whose duties involve:
        i. Direct involvement in cyber incident response and/or disaster recovery after a cyber incident;
        ii. Cybersecurity responsibilities or oversight for the operations of IT or remotely accessible OT systems and/or
        iii. Other roles as designated by the owner/operator.

    Examples of personnel whom the owner/operator may designate as key personnel may include, but are not limited to:
        i. Company leadership, Company Security Officer (CSO), Facility/Vessel Security Officer, or other individuals with oversight responsibility;
        ii. Personnel with elevated system access, administrative privileges, or system maintenance duties;
        iii. Designated Cybersecurity Officer (CySO), or other personnel tasked with direct cybersecurity plan (CSP) responsibilities; and/or
        iv. OT engineers, operators, or technicians with elevated system access, administrative privileges, or system maintenance duties.

    Considering the examples above, operational conditions, and cybersecurity risks, owners/operators are expected to document their reasoning or justification for how key personnel are defined. In addition to the topics required by 33 CFR § 101.650(d)(2), key personnel must also receive the training required by 33 CFR § 101.650(d)(1).

8. Training Implementation. Cybersecurity training must address the subject matter categories outlined in 33 CFR § 101.650(d)(1) and (d)(2). Training should be tailored to suit the unique operations of each owner/operator and may be combined with training required by 33 CFR § 104.225, 33 CFR § 105.215, and 33 CFR §106.220. All personnel with access to the IT or OT systems are expected to comply with reference (a).
    a. As owners or operators designate a CySO, they shall ensure the CySO has the appropriate knowledge as outlined in 33 CFR § 101.625(e), and any necessary training for the CySO addresses the same.

b. During the interim period before a CSP is approved, when a CySO may not yet be assigned:
   i. Training on relevant provisions of the CSP (33CFR § 101.650(d)(1)(i)) may be deferred until such time that the CSP is approved and CySO is assigned (See Enclosure (1)), but no later than 16 July 2027.
   ii. The knowledge level of the individual, group, and/or third-party entity implementing, developing, or approving the training should meet or exceed the knowledge standards for a CySO as outlined in 33 CFR § 101.625(e).
   iii. The training requirement on procedures for reporting a cyber incident to the CySO (33 CFR § 101.650(d)(1)(iv)) may be modified to cyber incident reporting procedures currently in effect under the FSP/VSP/OCS FSP.

c. Upon designation of a CySO and approval of the CSP, the CySO must review the existing training to ensure it is tailored to the entity's operations, taking into account the types of IT and OT systems and equipment that personnel have access to at their specific vessel, facility, or OCS facility.

9. Access by Untrained Personnel.
   a. Personnel who are unable to receive cybersecurity training may access IT and/or OT if they are physically accompanied or monitored by personnel with the required training, in accordance with reference (a). This physical accompaniment and/or monitoring is intended to mitigate risk and limit potential damage by untrained users by restricting their access to the minimum necessary and ensuring their actions are observed. Examples of untrained personnel who may fall under this category include, but are not limited to, technicians responding for a short period, or stevedores and longshoremen who are not anticipated to have recurring, long-term access to IT and/or OT at a specific location, personnel supporting a maintenance event or "turnaround," and other personnel who have temporary or infrequent "access" as defined in Section 7(a) .
   b. The owner/operator may also allow an untrained person to access the IT and/or OT remotely for an operational necessity or exigent circumstance in accordance with 33 CFR § 101.650(d)(3). If a trained person cannot physically monitor or accompany the untrained person, then remote access may be granted using remote "escorting" (monitoring by a trained person and/or automated systems) using the concept of least privilege with additional control measures in place to ensure system/network integrity. The owner/operator should ensure personnel responsible for implementing and monitoring these remote "escorting" measures possess the knowledge to understand the scope of access granted, recognize actions that could compromise system integrity, and have the authority to immediately terminate the session, if necessary. Options for remote "escorting" may include, but are not limited to:
      i. periodic reviews of access logs during the session;
      ii. session recording;

iii. automated systems that provide real-time security monitoring and notification to detect unauthorized activity by untrained personnel (if chosen, should include session recording); and/or
iv. remote control/shadowing by personnel who are trained in accordance with 33 CFR § 101.650(d)(1).
(1) Remote access to OT by untrained personnel must include remote control/shadowing by a trained application system engineer/owner;

Considering the examples above, operational conditions, and cybersecurity risks, owners/operators are expected to document the processes or procedures for physical accompaniment or monitoring of untrained personnel as well as the processes, procedures, and/or automated systems utilized for remote "escorting" of untrained personnel.

10. Training Documentation. Owners/operators must maintain training records and documentation in accordance with 33 CFR § 101.640. This documentation will be used by the Coast Guard to verify that the cybersecurity training meets the basic requirements outlined in 33 CFR Part 101, Subpart F. Records documenting training under 33 CFR § 101.650(d)(1) and (2) may be kept in hard copy and/or electronic format (including in a Learning Management System) and must include the following data at a minimum: the date of each session, duration of session, a description or outline of the training demonstrating how personnel are trained in the topics provided in 33 CFR § 101.650(d)(1) and (2), and a list of attendees.
    a. A plan amendment is not required if cybersecurity training is documented as additional security training under the existing FSP/VSP/OCS FSP. In addition to documenting the minimum training data listed above, the following information should be documented:
        i. How key personnel are defined;
        ii. How training is delivered, which may utilize a combination of delivery options, as noted in Section (12);
        iii. The processes or procedures for physical accompaniment or monitoring of untrained personnel as well as the processes, procedures, and/or automated systems utilized for remote "escorting" of untrained personnel;
        iv. Contractor training records, if applicable, as outlined in Section (13).

    Until such time as the CSP is approved, the information above in (i)-(iv) can either be included as a section under 33 CFR § 104.225, 33 CFR § 105.215, or 33 CFR § 106.220 or as standalone document kept with the FSP/VSP/OCS FSP.

11. Training Requirements.
    a. All personnel with "un-escorted" access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must have cybersecurity training in the following topics:
        i. Relevant provisions of the Cybersecurity Plan;

(1) As determined by the owner/operator. This requirement may be deferred until such time that the CSP is approved and CySO assigned (See Enclosure (1)), but no later than 16 July 2027. Examples of relevant provisions may include the requirements found in 33 CFR § 101.630 (c) (1 through 14).
(2) Cybersecurity content from approved Facility and Vessel Security Plans that will be incorporated into the Cybersecurity Plan should be included in the training.

ii. Recognition and detection of cybersecurity threats and all types of cyber incidents;
(1) This may include information on the most likely cybersecurity threats based on operational conditions and cybersecurity risks and may include topics such as ransomware, insider threats, supply chain security, phishing / social engineering, and state-sponsored attacks.

iii. Techniques used to circumvent cybersecurity measures;
(1) This may include information on the most likely techniques to circumvent cybersecurity threats based on operational conditions and is closely related to (ii). Examples may include topics such as using another person's access credentials, attempting to bypass cybersecurity measures, or introduction of malware via a USB.

iv. Procedures for reporting a cyber incident to the CySO;
(1) This may be accomplished by referencing a telephone number, email address, or other notification process where personnel can report a cyber incident or other suspicious cybersecurity activities.

v. OT-specific cybersecurity training for all personnel whose duties include using OT.
(1) This information may focus on general OT-related cybersecurity issues, but should emphasize the types of OT that are present at the subject vessel/facility/OCS facility.
(2) This may include information on the most likely techniques to circumvent cybersecurity threats based on operational conditions and may include topics such maintaining secure physical access into OT environments (such as Control Rooms) and being alert to unusual OT system conditions.

b. Key personnel with access to the IT or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must also have cybersecurity training in the following additional topics:

i. Understanding their roles and responsibilities during a cyber incident and response procedure;
(1) This may be accomplished by referencing the types of roles, responsibilities, and resources that may be required to respond to a cyber incident and can then reference or direct key personnel to

consult existing cybersecurity response or remediation plans for more detailed response information.

ii. Maintaining current knowledge of changing cybersecurity threats and countermeasures.

(1) This may be accomplished by referencing reliable sources key personnel may use to stay apprised of the changing cybersecurity landscape, such as information pages from Cybersecurity and Infrastructure Security Agency (CISA), sector specific Information Sharing and Analysis Center (ISAC), or other third-party sources.

12. Training Delivery. Training approved by the owner/operator or CySO may incorporate a range of delivery approaches (or a combination of approaches), including, but not limited to, virtual, in-person, or self-paced instruction. The owner/operator should determine the training provider, with options including in-house employees, contractors, or third-party entities. The training requirements in 33 CFR § 101.650(d) are performance-based, and the Coast Guard does not endorse specific training programs or content. The owner/operator is responsible for selecting training that satisfies their operational needs and meets regulatory requirements. If the owner/operator utilizes existing cybersecurity training materials, then the owner/operator should be able to demonstrate how existing training module(s) or content address each regulatory topic. This could be accomplished, for example, by cross-referencing existing training(s) to the topics in 33 CFR 101.650(d)(1) and 33 CFR 101.650(d)(2).

13. Contractor Training. Prior to authorizing IT and OT system access for a contractor or third-party employee at the vessel, facility, or OCS facility, the owner/operator should:

a. Train the contractor using the owner's/operator's training, or monitor or accompany in accordance with 33 CFR § 101.650(d)(3); or

b. Evaluate the third-party entity's existing cybersecurity training program for regulatory compliance and specific alignment to 33 CFR § 101.650(d)(1)(i)-(v) and 33 CFR § 101.650(d)(2)(i)-(ii). Based on this evaluation, the owner/operator may deem the training adequate to mitigate human factor cybersecurity risks associated with the use of their systems and meet compliance.

i. If the owner/operator accepts the third-party entity's training program, the owner/operator should maintain a record of this decision and keep the record of the decision with the VSP/FSP/OCS FSP until the CSP is approved. This record should include the date of evaluation, scope of the review, consideration of regulatory requirements, and the rationale for acceptance. Training records for each impacted third-party employee should also be maintained. All records should be available for Coast Guard inspection upon request.

ii. If this option is chosen, the owner/operator must review the third-party training program for currency of information and compliance with 33 CFR § 101.650(d) at least annually and produce or access contractor training records for Coast Guard inspection upon request.

14. Questions. Questions concerning this policy letter and guidance should be directed to the Office of Maritime Cybersecurity Policy, (CG-MCP) at MTSCyberRule@uscg.mil. Changes to this policy will be issued as necessary.

#

Enclosure: (1) Reference Table for Training Requirements

Dist: (1) COMDT (CG-CVC)
(2) COMDT (CG-ENG)
(3) COMDT (CG-MSC)
(4) COGARD CYBERCOM
(5) LANT-543
(6) PAC-543
(7) CGD-NE (dp)
(8) CGD-E (dp)
(9) CGD-SE (dp)
(10) CGD-H (dp)
(11) CGD-SW (dp)
(12) CGD-NW (dp)
(13) CGD-O (dp)
(14) CGD-A (dp)

Cybersecurity Training for Personnel						
Training Requirments 33 CFR 101.650(d)		***All Personnel***	***Key Personnel***	***Untrained Personnel***	***Compliance Date***	
(1)(i):	Relevant provisions of the CSP	See paragraph 8 of this policy letter	See paragraph 8 of this policy letter	*MUST BE ESCORTED*	Initial Training: W/in 60 days of CSP approval	<u>New Personnel:</u> Training for newly onboarded personnel must be completed w/in 5 days of gaining system access, but NLT 30 days of hiring & then annually thereafter. <u>New IT/OT Systems:</u> Training for personnel on new IT or OT systems must be completed w/in 5 days of gaining system access & then annually thereafter
(1)(ii):	Recognition and detection of cybersecurity threats and all types of cyber incidents	Yes	Yes		Initial Training: NLT Jan 12, 2026	
(1)(iii):	Techniques used to circumvent cybersecurity	Yes	Yes		Initial Training: NLT Jan 12, 2026	
(1)(iv):	Procedures for reporting a cyber incident to the CySO	See paragraph 8 of this policy letter	See paragraph 8 of this policy letter		Initial Training: W/in 30 days of designation of CySO, but NLT July 16, 2027	
(1)(v):	OT-specific cybersecurity training for all personnel whose duties include using OT	Yes	Yes		Initial Training: NLT Jan 12, 2026	
(2)(i):	Roles and responsibilities during a cyber incident and response procedure	No	Yes		Initial Training: NLT Jan 12, 2026	
(2)(ii):	Maintaining current knowledge of changing cybersecurity threats and countermeasures	No	Yes		Initial Training: NLT Jan 12, 2026	