Title	Cybersecurity Training Verification Job Aid				
Serial	MCP-WI-001	Orig. Date	09 Jan 2026	Rev. Date	N/A
Signature Authority	C. N. Parham Chief, Office of Maritime Cybersecurity Policy				
Disclaimer:	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.				
References:	a) 33 CFR 101.640 and 101.650(d) 33 CFR Part 101 Subpart F -- Cybersecurity b) CG-5PC Policy Letter 01-25 (9 October 2025) Policy Letter-5-PC_01-25				
Enclosures:	CYBER TRAINING VERIFICATION JOB AID (09 January 2026)				

A. <u>Purpose.</u> The enclosed Cyber Training Verification Job Aid (09 January 2026) equips Coast Guard Vessel and Facility inspectors with key questions and answers to verify cybersecurity training requirements detailed in references (a & b). It provides a foundational framework for addressing common cybersecurity concerns and includes targeted queries for effective inspection procedures. It is expected that these questions will be incorporated into the existing inspection regiment. This guide provides a starting point and is not intended to limit inspector and COTP/OCMI discretion. Inspectors should consult the unit Marine Transportation System Specialist-Cybersecurity (or District if unit not available) for expertise as needed.

B. <u>Questions.</u> This guidance will also be posted and updated on the Coast Guard Maritime Cybersecurity Resource Website. Questions concerning this work instruction and guidance should be directed to the Office of Maritime Cybersecurity Policy, (CG-MCP) at MTSCyberRule@uscg.mil . Changes to this guidance will be issued by CG-MCP as necessary.

C.N. Parham

C. N. PARHAM
Chief
U.S. Coast Guard Office of Maritime
Cybersecurity Policy
By direction

CYBER TRAINING VERIFICATION
JOB AID

Entity:	VIN/FIN:
MISLE Activity #:	Date:
Vessel/Facility Security Officer (VSO/FSO):	Cybersecurity Officer (CySO) if designated:
USCG Inspector:	CySO Contact Information:
USCG Inspector:	USCG Inspector:

Preface

This job aid guides an inspector through pertinent questions to help verify cybersecurity training requirements under 33 CFR 101 Subpart F for vessels, facilities and OCS facilities <u>during inspections before July 16, 2027</u>. This training compliance checklist will be incorporated into a cybersecurity inspection job aid to be promulgated for use after that date. This job aid is not a substitute for applicable legal requirements, nor is it itself a rule. The inspector should consult 33 CFR 101.640 and 101.650(d), and CG-5PC Policy Letter 01-25 as references.

It is understood that these verifications are being added to existing vessel, facility, and OCS facility inspections. <u>If operational tempo or unit needs preclude the ability to include all job aid questions during the inspection, focus on those questions denoted by "*" and note it in the MISLE narrative.</u>

CG-835s should be considered a primary tool to capture compliance issues/deficiencies for all items in this job aid.

This guide provides a starting point and is not intended to limit inspector and COTP/OCMI discretion; <u>inspectors should consult the unit MTSS-C (or District if unit not available) for expertise and guidance</u>. For further policy assistance, contact MTSCyberRule@uscg.mil.

Section I. Cybersecurity Training Program (33 CFR § 101.650(d))

These questions verify the establishment and content of the required cybersecurity training program.

Yes	No	N/A	

☐	☐
	 *see appendix
		☐	1. ***Scope of Training:** Do you have a cybersecurity training program in place for all personnel, including contractors (part-time, full-time, temporary, and permanent), who have access to Information Technology (IT) or Operational Technology (OT) systems in/on this vessel/facility/OCS facility?
			      a. Did the owner/operator identify who was required to receive the training in 101.650(d)(1)?
			      b. Did the owner/operator identify "Key Personnel," and did they receive additional specialized or recurring training in 101.650(d)(2)?

☐	☐ *see appendix	☐	2. ***Training Deadline:** Was the initial required cybersecurity training completed for all relevant existing personnel by January 12, 2026? (Note: If not by the deadline, but it is completed any time prior to the time of inspection, issue a corrected-on-the-spot 835 for tracking purposes.)

☐	☐	☐	3. ***Training Content:** Does the training include these topics:
			      a. Recognition and detection of cybersecurity threats and all types of cyber incidents;
			      b. Techniques used to circumvent cybersecurity measures;
			      c. The procedures for reporting a cyber incident;
			      d. OT-specific cybersecurity training for all personnel whose duties include using OT.
			 (Note: Evidence may be found in the required training records' description of training, or in a stand-alone document/outline.)

☐	☐	☐	4. **New Hire Training:** Do new personnel (including contractors) complete the required cybersecurity training within 5 days of gaining access or within 30 days of hire?

Section I Notes:

_____

_____

_____

Section II. Training Records (33 CFR 101.640)

These questions verify that the required training documentation is maintained and accessible.

Yes	No	N/A	

☐	☐	☐	1. ***Training Record Detail:** Does the documentation for each training session include all of the following:
			      a. The date and duration of the session?
			      b. A description or outline of the training demonstrating topics provided in 101.650(d)(1) and (2)?
			      c. A complete list of all attendees?

☐	☐	☐	2. ***Record Maintenance:** Are cybersecurity training records maintained in accordance with 33 CFR 101.640 (and 33 CFR 104.235, 105.225, 106.230 as applicable)?

Section II Notes:

_____

_____

_____

Section III. Untrained Personnel Access Controls (33 CFR 101.650(d)(3) and (4))

These questions verify the safety measures for personnel who have not yet completed the required training.

Yes	**No**	**N/A**	
☐	☐	☐	1. **Untrained Access Policy:** Do you have a process for managing personnel who require access to IT or OT systems but are unable to complete the required cybersecurity training?
☐	☐	☐	2. **Supervision Measures:** Are specific methods such as physical accompaniment or continuous monitoring/escorting used to mitigate risk for personnel with system access who are unable to complete the required cybersecurity training?
☐	☐	☐	3. **Remote Escort (if applicable):** Is there a specific individual or team that manages the remote escorting process, and are there processes or procedures in place for remote escorting of untrained personnel?
☐	☐	☐	4. **Contractor/Third-Party Provided Training for their personnel accessing your systems (if applicable):** If you have not trained contractors and/or third party personnel with the entity training program, have you reviewed and accepted the third-party training program for currency of information and compliance with 33 CFR 101.650(d)/Policy Letter 01-25 paragraph 13(b) as meeting the requirements for accessing your networks and/or systems?

Section III Notes:

_____

_____

_____

Appendix

If the answer to Question 1 and/or Question 2 in Section I is "no", the "Main Questions" below must be asked by the inspector and findings and responses to these questions documented in MISLE under the deficiency narrative. This appendix is a guide to assessing the entity's compliance posture, potential risks, and commitment to cybersecurity best practices while still demonstrating a focus on understanding challenges and finding solutions. All other questions below are provided as samples for an inspector to use to understand the situation and inform compliance actions/decisions and are not an inclusive list of what may be asked.

Note: COTPs should engage with their District and Area Prevention and Legal Staffs, as well as CG-MCP, before imposing any operational controls or enforcement actions on regulated entities that have not met the requirements under 33 CFR Part 101.650(d) beyond a CG-835.

Main Questions:

- **What specific challenges are you facing in completing cyber training requirements?**
- **What specific steps are being taken to address the challenges?**
- **What percentage of your workforce remains to be trained?**
- **Are there any 'key personnel' that have not yet completed the training?**
- **Based on your current progress and planned actions, what is the realistic timeframe for achieving 100% completion of cyber training for all personnel?**

Understanding Challenges:

- Are there any resource constraints, scheduling conflicts, or technical issues hindering your ability to complete the training?
- Has the company explored alternative training delivery methods (e.g., online, in-person, blended learning) to overcome these challenges?
- Are there accessibility concerns impacting training completion for certain personnel?

Assessing Progress:

- What percentage of personnel have completed the training under 101.650(d)(1)? Key personnel under 101.650(d)(2)?
- What is the average completion rate for personnel who have started the training program?
- Are there any documented instances of personnel failing the training and requiring re-training?

Clarifying Completion Plans:

- Can you provide a detailed plan, including key milestones and responsible parties, outlining how you intend to achieve full compliance with the cyber training requirements?
- What contingency plans are in place should unforeseen issues arise to delay the completion date?
- How will you track and monitor progress against this timeframe, and who is responsible for reporting on these metrics?

Notes

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____