Final Rule: Cybersecurity in the Marine Transportation System Questions

**** In response to questions received from affected stakeholders, and to provide information while future guidance is considered, the Coast Guard is announcing the publication of the Cybersecurity in the MTS final rule Frequently Asked Questions (FAQ). The questions below are representative of those submitted by stakeholders and may have been reworded or combined with others for clarity and organization of topics. They have been grouped under the relevant regulatory cite or the relevant regulatory cite is provided. Nothing in these FAQs represents regulations themselves but support the published regulations. If you have a question that is not reflected here, or you have questions regarding the information presented in the FAQs, please reach out to the Coast Guard at MTSCyberRule@uscg.mil****

General (Last Updated 07/22/2025)

Will the Coast Guard accept and review the submission of a cyber plan in accordance with the final rule right now?

- **Plans are not being approved yet:** The Coast Guard is not currently approving plans for these regulations. We are currently developing review and approval procedures to ensure consistent application of standards for the maritime industry.
- **Previously submitted plans:** If a plan has already been submitted, it will be securely retained until the review and approval process is finalized.

How do I demonstrate compliance with training requirements (101.650(d)) before having an approved cybersecurity plan (effective January 2026)?

- **Documentation:** Use the existing documentation process outlined in the approved FSP/OCS FSP/VSP for other MTSA-related training.
- **Record Keeping:** Ensure training records explicitly state the topics covered that comply with 101.650(d).
- **Qualifications:** The entity providing the training should meet or exceed the knowledge standards for a Cybersecurity Officer (CySO) as outlined in 101.625(e)(2), (5), (8), (10), (11).
- **No Amendment Required:** No FSP/OCS FSP/VSP amendment is needed as long as the cyber training is documented as additional security training within the existing plan.

Does the Coast Guard intend to release guidance clarifying how compliance with cybersecurity requirements will be inspected or enforced?

- The USCG is determining the best way forward to meet stakeholder needs.

Should MTSA facilities/vessels without Operational Technology (OT) be exempt from these cybersecurity regulations?

- No. MTSA regulation implies Transportation Security Incident (TSI) risk regardless of OT presence.
- All regulated entities must conduct the cybersecurity assessment.
- **After** assessment, waivers or equivalence determinations can be requested if warranted.

What is the appeals process for cybersecurity deficiencies?

- First, request reconsideration from the cognizant Captain of the Port (COTP).
- If unresolved, appeals are handled in accordance with 33 CFR 101.420.

101.605(a)

Are Maritime Academies under the Maritime Administration (MARAD) required to adopt the new Coast Guard cybersecurity regulations?

- Applicability depends on whether their operations meet MTSA-regulated entity criteria.
- The rule doesn't expand MTSA applicability but adds cybersecurity requirements to the existing framework.
- If they operate vessels under 33 CFR Part 104 or facilities under 33 CFR Part 105, they *may* be subject to the requirements.
- If a vessel already has a Vessel Security Plan (VSP) and complies with MTSA, it will likely need to comply with the new cybersecurity provision.
- Consult the MARAD/USCG Memorandum of Understanding for further guidance.

101.620 - Owner or operator (Last Updated 07/22/2025)

101.620(b)(3)
Are there specific licensing or certification requirements for the CySO?

- No. For details about CySO requirements, see 33 CFR 101.625(e).

101.625 - Cybersecurity Officer (Last Updated 07/22/2025)

101.625(a)

May a company outsource their CySO to a third-party company?

- Yes. CySO requirements may be met through third-party services.

101.625(b)

Are there any limits to how many vessels/terminals can fall under a CySO?

- No. For details, see 33 CFR 101.625(b).

101.625(d)(6)

What are the cybersecurity inspection expectations?

- **Timing:** Inspections can be combined with other inspections or separate.
- **Format:** In-person review, like existing facility/vessel inspections.
- **CySO Remote Participation:** The CySO may be able to participate remotely at the discretion of the COTP or OCMI.

101.630 - Cybersecurity Plan (Last Updated 07/22/2025)

101.630

What IT/OT systems should be considered in complying with these regulations?

- **Purpose:** The Cybersecurity assessment must identify IT/OT that impact maritime operations or could lead to a TSI. It is not limited to FSP/VSP identified assets.

- **Approach:** Owners/operators should take a holistic approach to include all necessary systems.
- **Questions:** Direct specific IT/OT questions to *MTSCyberRule@uscg.mil*.

101.630

Can similar vessels share one Cyber Plan?

- Yes, owners/operators may submit one Cybersecurity Plan for two or more U.S.-flagged vessels with similar operations.
- The Plan must address any specific cybersecurity risk differences between individual vessels.

101.630(a)

Can the cybersecurity plan be combined with the Vessel Security Plan (VSP) or FSP, and harmonized?

- Yes. For details, see 33 CFR 101.630(a).

101.630(a), (c), (e), (f)

What is the purpose of Audits vs. Assessments?

- **Cybersecurity Plan (CSP) Audits:**
    - Internal verification to ensure CSP/assessment validity or identify amendments.
    - Required annually, or more often with changes (owner/operator, cyber measures).
    - CSP amendments may necessitate separate FSP/VSP amendments if related topics or impacted measures become outdated.
- **Cybersecurity Assessment:**
    - Vital for CSP development: complete assessment first, then tailor plan to identified vulnerabilities.
    - Plan effectiveness rooted in accurate/comprehensive assessment.
    - Not static; threats evolve rapidly, so regular assessment and plan updates are recommended.

101.630(d)

Does the CSP renewal have to align with the current FSP/VSP schedule?

- **Owner/operator Choice:** That decision is left to the company about whether to request alignment of submission dates.
- **CSP Schedule:** Initial approval date sets the CSP's 5-year schedule.
- **Alignment:** On request, the Coast Guard will work with submitters to align approval dates, where able, between the FSP/VSP and their CSP.

101.635 - Drills and exercises (Last Updated 07/22/2025)

101.635(b), (c)

Cybersecurity Drills (bi-annual) vs. Exercises (annual): What's the difference?

- **Cybersecurity Drill:** Tests individual aspects of the cybersecurity plan.
- **Cybersecurity Exercise:** Full test of the cybersecurity plan.

101.635(a), (b), (c)

Can more than one facility/vessel get credit for the same cybersecurity drill and exercise?

- Yes, an owner/operator **may** conduct a drill that spans more than one facility/vessel simultaneously.
- However, all requirements per 33 CFR 101.635 **must be met for each specific facility/vessel** involved.
- The same scenario may be used for multiple facilities at different times, provided it remains applicable to each.
- Each successive drill should test a different part of the security plan, as feasible.

101.635(a), (b), (c)

Can IT phishing tests or simulated cyber incidents count as drills?

- Yes, phishing awareness emails, such as simulated link-click response can potentially count as drills.
- However, they should not be the only types of drills conducted.
- Drills should vary the elements of the plan tested over time.

- Real-world events can also serve as drills/exercises.

101.635

Can cybersecurity drills and exercises be combined with physical security drills and exercises?

- **Yes**, cybersecurity drills and annual exercises can be combined with existing MTSA-required physical security drills/exercises.
- For combined exercises, the scenario must:
- Fully test both the Cybersecurity Plan (CSP) and the Physical Security Plan (FSP/VSP/OCS FSP).
- Meet all requirements of each respective regulatory provision.

101.650 - Cybersecurity measures (Last Updated 07/22/2025)

101.650(d)

What cybersecurity training requirements will be mandated for personnel in maritime operations?

- For details about cybersecurity training requirements, see 33 CFR 101.650(d).

101.650(d)

What defines "access" for IT/OT cybersecurity training?

- The ability and means to:
    - Communicate with or interact with a system.
    - Use system resources to handle information.
    - Gain knowledge of system information.
    - Control system components and functions.
- Typically granted via user credentials and permissions.
- Can be **physical access** (for example, plugging in a USB) or **logical access** (for example, logging into a network).

- **Personnel with unrestricted physical access** to IT/OT equipment housing areas are considered to have "access" for this requirement, even without logical access.

101.650(d)(2)

What defines "Key Personnel"?

"Key Personnel" may be defined by the owner/operator based on the operational conditions and cybersecurity risks, but in general are individuals whose duties involve:

- A direct role or leadership in cyber incident response and/or disaster recovery.
- Being critical to the operations of the covered IT/OT systems.
- Other personnel as designated by the owner/operator.

Identification of these positions/persons is up to the owner/operator and must be documented by position and/or name in the security plan.

101.650(e)(1)

What are the expected frequency of mandatory cyber assessments/audits?

- **Cybersecurity Assessments:**
  - **Initial:** No later than July 16, 2027.
  - **Frequency:** Annually thereafter.
  - **Sooner if:** Change in ownership.
  - **Purpose:** Inform plan development/maintenance by identifying risks and vulnerabilities.
  - **Note:** Assessment must be conducted *before* developing the Cybersecurity Plan.
- **Cybersecurity Audits (Internal):**
  - **Frequency:** At least annually.
  - **More frequently if:** Change in owner/operator, or modifications to cybersecurity measures (per 33 CFR 101.630(f)).
  - **Purpose:** Identify issues or changes since the last audit and initiate Cybersecurity Plan (CSP) amendments.

101.650(e)(1)

Can a fleet of vessels with identical IT/OT footprint be covered by a single Cybersecurity Assessment (CSA)?

- Yes, however, if there is any deviation in configuration on one or more vessels, a Cybersecurity Assessment (CSA) is **required for each individual vessel**, addressing its unique IT/OT footprint.

101.650(g)

Does the Coast Guard have capabilities and resources that can aid companies in their response to cyber incidents?

- Yes, the USCG can provide guidance and assistance.
- **Resources:**
  - Sector Marine Transportation System Specialist -Cyber (MTSS-C), stationed in local COTP Zones.
  - U.S. Coast Guard's Cyber Protection Team (CPT).
  - Coast Guard Maritime Industry Cybersecurity Resource Website: Coast Guard Maritime Industry Cybersecurity Resource Website
- **How to Request Assistance:**
  - During an NRC report.
  - Directly through the Sector Command Center.
  - Through the MTSS-C.
  - Via email: maritimecyber@uscg.mil .

101.660 - Cybersecurity compliance documentation (Last Updated 07/22/2025)

Can TSA CIP/CAP compliance fulfill new cybersecurity requirements?

- If regulatory overlap exists, entities may identify where requirements are being simultaneously satisfied and bring this to the attention of the Coast Guard during submission or inspection.

Part 160 – Ports and Waterways Safety – General (Last Updated 07/22/2025)

"Cyber incident" (160.202) vs. 101.615 definitions?

- The use of the term "cyber incident" in the definition of “hazardous condition” in 33 CFR 160.202 **is treated the same** as the definition of "cyber incident" in 33 CFR 101.615.

Do foreign vessels have to report cyber incidents via ENOA and to NRC/COTP?

- **Yes, hazardous conditions** (now including cyber incidents) must be reported on the Notice of Arrival (NOA) per 33 CFR 160.206.
- **Immediate notification** to the nearest COTP or OCMI is required for any hazardous condition (33 CFR 160.216).