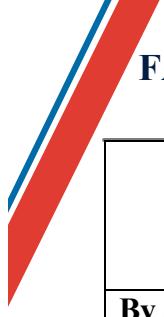


FACT SHEET: U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System

- **On January 17, 2025, the U.S. Coast Guard published a new final rule that establishes baseline cybersecurity requirements to protect the marine transportation system (MTS) from cyber threats.**
- **The Coast Guard is also requesting comments on the implementation periods for U.S.-flagged vessels.**
- **Who do the new regulations apply to?**
 - This final rule applies to the owners and operators of U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities required to have a security plan under 33 CFR parts 104, 105, and 106.
 - This subpart does not apply to any foreign-flagged vessels subject to 33 CFR part 104.
- **What is the effective date**
 - This final rule is effective July 16, 2025.
- **What are the compliance timeframes?**
 - The following table outlines the timing of this final rule's requirements:

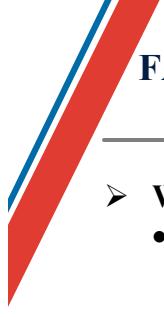
Effective Dates	Provisions
Immediately Upon July 16,2025	Entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1, begin ensuring that all reportable cyber incidents are reported to the National Response Center (NRC). § 101.620(b)(7).
By January 12, 2026	<p>All personnel must complete the training specified in § 101.650(d)(1)(ii) through (v), which includes recognition and detection of cybersecurity threats and all types of cyber incidents, techniques used to circumvent cybersecurity measures, procedures for reporting a cyber incident to the Cybersecurity Officer (CySO), and operational technology (OT)-specific cybersecurity training (for all personnel whose duties include using OT).</p> <p>Key personnel must also complete the training specified in § 101.650(d)(2) about their roles and responsibilities during a cyber incident and response procedure and how to maintain current knowledge of changing cybersecurity threats and countermeasures.</p> <p>Additional training requirements include the following:</p> <ul style="list-style-type: none">○ Training for new personnel not in place at the time of the effective date of this final rule must be completed within 5 days of gaining system access, but no later than within 30 days of hiring and annually thereafter.○ Training for personnel on new information technology (IT) or



FACT SHEET: U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System

	OT systems not in place at the time of the effective date of this final rule must be completed within 5 days of system access and annually thereafter.
By July 16, 2027	<p>Owners and operators must designate, in writing, the CySO. § 101.620(b)(3) and (c)(1).</p> <p>Owners and operators must conduct the Cybersecurity Assessment within 24 months of the effective date of this final rule and annually thereafter (or sooner than annually if there is a change in ownership). § 101.650(e)(1).</p> <p>Owners and operators must submit the Cybersecurity Plan to the Coast Guard for approval within 24 months of the effective date of this final rule. § 101.655.</p>
After Receiving Approval of the Cybersecurity Plan	<p>Owners and operators must conduct cybersecurity drills at least twice each calendar year. Owners and operators must also conduct cybersecurity exercises at least once each calendar year, with no more than 18 months between cybersecurity exercises. § 101.635(b)(1) and (c)(1).</p> <p>All personnel must complete the training specified in § 101.650(d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan.</p> <p>Each owner or operator must ensure that the cybersecurity portion of their Plan and their penetration test results are available to the Coast Guard upon request. § 101.660.</p>

- **Why is the Coast Guard requesting comments on the implementation period for U.S.-flagged vessels?**
- The Coast Guard received several public comments asking us to extend the implementation period for different periods ranging from 36 to 48 months beyond the 12 to 18 months proposed in the notice of proposed rulemaking (NPRM). Some commenters suggested that U.S.-flagged vessels would require more time than facilities to implement the requirements in this final rule.
 - The Coast Guard invites the public to comment by March 18, 2025, on whether we should delay the implementation periods for U.S.-flagged vessels for a period of 2 to 5 years beyond what is specified in this final rule. For a more detailed discussion, please see Section VII of the final rule. Comments submitted should include information supporting the specific period from 2 to 5 years that the commenter suggests. (See the ADDRESSES portion of the final rule preamble, under *Comment period for solicited additional comments*, for instructions on submitting comments.)
 - After reviewing any comments and supporting information received, the Coast Guard may issue a future rulemaking to implement this additional delay to provide time for U.S.-flagged vessels to comply with these requirements.



FACT SHEET: U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System

➤ **Where can I find the regulatory text?**

- Regulatory text can be found at www.regulations.gov (type USCG-2022-0802 in the search box and click “Search.”)

➤ **Where should I send questions?**

- For submitting comments regarding the implementation period for U.S.-flagged vessels, go to www.regulations.gov, type USCG-2022-0802 in the search box, and click “Search.” Next, look for this document in the **Search Results** column, and click on it. Then click on the **Comment** option.
- For further information about this rulemaking, email MTSCyberRule@uscg.mil.
- For facility-related questions, call Commander Brandon Link, Office of Port and Facility Compliance, at 202-372-1107.
- For vessel-related questions, call Commander Christopher Rabalais, Office of Design and Engineering Standards, at 202-372-1375.