Published on *The National Law Review* https://natlawreview.com

Coast Guard Issues Final Maritime Cybersecurity Rule: Key Requirements and Implementation Timeline

Article By:

Andrew R. Lee

RichardD. Bertram

James A. Kearns

Ilsa H. Luther

On January 17, the US Coast Guard released its much-anticipated final rule on cybersecurity in the US Marine Transportation System, which establishes mandatory minimum cybersecurity requirements for the maritime sector. The new regulations are effective July 16, 2025 and represent the most significant maritime cybersecurity regulations to date. Affected entities should review their existing policies, identify any gaps or deficiencies, and implement compliance procedures.

Jones Walker's *2022 Ports and Terminals Cybersecurity Survey* data was cited in the final rule, helping to shape some of the new regulations.

I. Scope and Applicability

The primary goal of the final rule is to enhance the cybersecurity of the US Marine Transportation System. The new regulations establish minimum mandatory requirements for US flag vessels, Outer Continental Shelf (OCS) facilities, and facilities subject to the Maritime Transportation Security Act of 2002. The rule aims to address the increasing risks posed by cyber threats due to the growing reliance on interconnected digital systems within the maritime industry. It emphasizes both preventing cyber incidents and preparing to respond to them effectively.

The rule applies to:

a. US flag vessels subject to 33 CFR part 104

33 CFR part 104 applies to:

- Cargo vessels greater than 100 gross tons
- Commercial passenger vessels certified to carry more than 150 passengers

- Offshore Supply Vessels (OSVs)
- Mobile Offshore Drilling Units (MODUs)
- Towing vessels more than 26 feet long engaged in towing certain dangerous cargo barges
- Cruise ships and passenger vessels carrying more than 12 passengers on international voyages

b. Facilities subject to 33 CFR part 105

These facilities are covered by the regulation:

- Container terminals
- Chemical facilities with waterfront access
- Petroleum terminals
- Cruise ship terminals
- Bulk liquid transfer facilities
- LNG/LPG terminals
- Barge fleeting facilities handling dangerous cargo
- Facilities that receive vessels carrying more than 150 passengers
- Marine cargo terminals otherwise subject to the Maritime Transportation Security of 2002

c. OCS facilities subject to 33 CFR part 106

These OCS facilities are affected:

- Offshore oil and gas production platforms
- Offshore drilling rigs
- Floating production storage and offloading units (FPSOs)
- Deepwater ports
- Offshore wind energy facilities
- Offshore loading/unloading terminals

II. Core Requirements

The cybersecurity plan must include measures for account security (e.g., automatic account lockout, strong passwords, multifactor authentication), device security (e.g., approved hardware/software lists, disabling executable code), and data security (e.g., secured logging, data encryption). Entities must also create or implement the following:

a. **Cybersecurity Officer** — Each covered entity must designate a Cybersecurity Officer (CySO) responsible for implementing and maintaining cybersecurity requirements. The rule allows for designation of alternate CySOs and permits one individual to serve multiple vessels or facilities, providing welcome flexibility for operators.

b. **Cybersecurity Plans and Assessments** — Organizations must develop and maintain the following:

- A comprehensive Cybersecurity Plan
- A separate Cyber Incident Response Plan
- Regular cybersecurity assessments

Plans must be submitted to the Coast Guard for review within 24 months of the rule's effective date.

c. **Training and Exercises** — The rule mandates the following:

- Cybersecurity training for all personnel using IT/OT systems beginning July 17, 2025
- Two cybersecurity drills annually
- Regular penetration testing aligned with plan renewal cycles

d. **Technical Controls** — Required security measures include the following:

- Account security controls including multifactor authentication
- Device security measures and approved hardware/software lists
- Data encryption and secure log management
- Network segmentation and monitoring
- Supply chain security requirements

III. Implementation Timeline

Key phase-in compliance dates include:

- Rule effective date: July 16, 2025
- Training requirements begin: July 17, 2025
- Initial cybersecurity assessment: Due by July 16, 2027
- Cybersecurity Plan submission: Due by July 16, 2027

The Coast Guard is seeking comments on extending implementation periods for the new requirements by two to five years for US flag vessels. Comments are due no later than March 18, 2025. After review of these comments, the Coast Guard may issue a future rule to allow additional time for US flag vessels to implement the new regulations.

IV. Harmonization with Other Requirements

The Coast Guard has worked to align these requirements with other cybersecurity regulations, including the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Incident Reporting for Critical Infrastructure Act of 2022 reporting requirements. The rule establishes the National Response Center (NRC) as the primary reporting channel for maritime cyber incidents, simplifying compliance for regulated entities.

V. Some Basic Questions and Answers

- **What are the mandatory cybersecurity measures outlined in the rule?** Owners and operators must implement a range of cybersecurity measures that are based on "cybersecurity performance goals" developed by CISA. This includes vulnerability identification of critical IT and OT systems, addressing known exploited vulnerabilities in those critical systems, and conducting penetration testing in conjunction with renewing the Cybersecurity Plan.
- **What constitutes a reportable cyber incident, and to whom do I report it?** A reportable cyber incident is defined as any incident leading to substantial loss of confidentiality, integrity, or availability of a covered system; to disruption to business operations; to unauthorized

access to nonpublic personal information of a large number of individuals; or to operational disruption of critical infrastructure. Such an incident also includes any event that may lead to a "transportation security incident." Such incidents must be reported to the NRC.

- **What is the Coast Guard's approach to compliance and enforcement of this new rule?** The rule takes a performance-based approach, meaning that it focuses on outcomes rather than prescribing specific technical solutions, thus providing some flexibility to the entities in meeting the requirements. However, the rule does not specify the methods of enforcement, and the Coast Guard is currently working with policymakers to define the compliance criteria. The Coast Guard will address those questions at upcoming symposiums. Noncompliance with the rule could lead to penalties, legal action, and financial losses.
- **Is there any flexibility or possibility of waivers in complying with this rule?** Yes. After completing a cybersecurity assessment, owners and operators can seek a waiver or an equivalence determination for the requirements, based on the waiver and equivalency provisions of 33 CFR parts 104, 105, and 106. Owners and operators must also notify the Coast Guard of temporary deviations from the requirements.

VI. Key Takeaways

- Begin preparation now — the 24-month implementation period will pass quickly given the scope of required changes.
- Evaluate current cybersecurity staffing and capabilities against new CySO requirements.
- Review existing security measures against the detailed technical requirements.
- Plan for increased training and exercise obligations.
- Consider whether to comment on the proposed implementation extension for vessels.

Our cross-disciplinary team has extensive experience helping clients navigate complex regulatory requirements. We can assist with:

- Gap analysis against new requirements
- CySO program development
- Cybersecurity Plan creation and review
- Training program development
- Technical compliance assessment

National Law Review, Volume XV, Number 28