REGULATORY AT-A-GLANCE

Cybersecurity Compliance Action Guide

What maritime and energy operators need to know about the U.S. Coast Guard's cybersecurity requirements, including deadlines and next steps.

WHY THIS MATTERS

Ports handle roughly 80% of world trade, and the U.S. maritime sector is now a documented target for nation-state actors, ransomware operators and APT groups. The USCG's MTSA cyber rule moves cybersecurity from an IT concern to a safety, operational and boardroom priority. Non-compliance risks operational disruption, financial penalties, regulatory action and reputational damage.

New regulatory requirements for the marine transportation system (MTS) demand immediate attention, advises ABS Consulting, a safety and risk management subsidiary of world-leading classification society American Bureau of Shipping (ABS).

Now that the U.S. Coast Guard's (USCG) minimum cybersecurity requirements have taken effect as of July 2025, vessel and facility owners and operators are navigating uncharted waters, notes ABS Consulting Senior Director Michael DeVolld, a retired USCG Officer who established a cybersecurity program at USCG Cyber Command.

Who must comply? If a company operates U.S.-flagged vessels over 500 gross tonnes carrying more than 12 passengers or manages facilities subject to the Maritime Transportation Security Act (MTSA) of 2002, the USCG's 2025 enforced Cyber Rule applies to them.

Whether running container ports, oil and gas facilities, cruise terminals or ferry operations, the Coast Guard's cybersecurity requirements cover both inland and deepwater environments.

"Companies need to get comfortable with reporting transparently—what affects one, ultimately affects all," DeVolld says. "With this transparency, they can then prioritize critical system protection inside and out by continually investing in their people and building cybersecurity capabilities over time."

DeVolld has spent months working with ports, vessel operators and terminal facilities across the country. He says many executives still think of cybersecurity as an IT problem, rather than what it really is—an existential business risk. Cybersecurity for operational environments "demands C-suite ownership and serious capital allocation," he says.

TechEDGE shares in brief what industry stakeholders in the marine and energy space should know about the path toward full MTSA compliance by 2027.

Maritime Cyber Rule Compliance Timeline

What's required to secure the nation's critical maritime transportation system and offshore energy assets on the Outer Continental Shelf (OCS)? Four milestones mark the journey.

DATE	MILESTONE	WHAT IT REQUIRES
February 2024	**Rule Issued**	USCG updates cybersecurity requirements for Maritime Transportation Security Act (MTSA)-regulated facilities. Cybersecurity must be integrated into Facility Security Plans (FSPs) and Vessel Security Plans (VSPs). Compliance planning begins.
July 16, 2025	**Final Rule Effective**	Minimum cybersecurity requirements are now in force. All qualifying cyber incidents must be reported to the National Response Center.
January 12, 2026	**Training Deadline**	All employees must complete cybersecurity training. New hires must complete cybersecurity training within 30 days of gaining system access. Existing personnel who are granted access to new IT or OT systems must complete training within 5 days. Annual refresher training is required for all personnel. Specialized training required for OT users and incident-response personnel.
July 16, 2027	**Full Compliance**	Written designation of a Cybersecurity Officer (CySO). Cybersecurity Assessment completed (and annually thereafter, or sooner on change of ownership). Cybersecurity Plan submitted to USCG for approval.

Who Must Comply

The rule applies to U.S.-flagged vessels, Outer Continental Shelf facilities and other facilities subject to MTSA regulations.

U.S.-Flagged Vessels	Operators of vessels subject to MTSA regulations, including cargo ships, passenger vessels and specialized maritime transport.
Outer Continental Shelf Facilities	Offshore drilling platforms, FPSOs, production facilities and related OCS infrastructure under USCG jurisdiction.
Ports & Terminals	Public and private terminal operators, including container, energy, chemical and bulk facilities subject to MTSA.
Other MTSA-Regulated Entities	Marine facilities and operators captured under MTSA scope, including those supporting the broader energy and chemicals value chain.

Five Core Requirements

The final rule establishes a minimum cybersecurity standard for MTSA-regulated entities. The five pillars below capture what owners and operators must put in place.

1

Cybersecurity Officer (CySO)

Designate a CySO in writing. This individual owns the cybersecurity program for the facility or vessel and is the point of accountability for USCG engagement.

2

Cybersecurity Assessment

Complete a cyber risk assessment within 24 months of the effective date, then annually. Sooner if there is a change in ownership. The assessment informs the cybersecurity plan.

3

Cybersecurity Plan

Develop and submit a written cybersecurity plan to the USCG for approval. The plan integrates with existing FSPs and VSPs.

4

Training

Train all employees on threat recognition, detection, reporting and countermeasures. Provide specialized training for OT users and focused training for incident-response personnel. New hires: 30 days. New-system access: 5 days. Annual refreshers required.

5

Incident Reporting

Report all qualifying cyber incidents to the National Response Center. Maintain an incident-response plan capable of containing and recovering from an event without halting operations.

Immediate Action Checklist

A focused set of next steps for operators still closing gaps against the 2027 full-compliance deadline:

☐ Confirm or formally designate your Cybersecurity Officer (CySO) in writing.

☐ Map the scope of MTSA-regulated assets (facilities, vessels, OCS infrastructure) and identify cyber-relevant OT and IT systems within each.

☐ Verify that all employees have completed the required cybersecurity training, including specialized OT modules. Confirm new-hire and new-access training triggers are documented.

☐ Commission or update your Cybersecurity Assessment as the foundation of your program, not a checkbox exercise.

☐ Draft or revise your Cybersecurity Plan, integrated with FSPs and VSPs, and plan for USCG review.

☐ Establish the reporting workflow for qualifying cyber incidents to the National Response Center, with clear escalation and roles.

☐ Conduct a tool rationalization review to reduce technology debt and clarify which platforms provide evidence for compliance.

☐ Brief the board: frame cyber as a critical business risk, not an IT line item, and secure ongoing executive sponsorship.

Cost of Non-Compliance

- Operational disruption from cyber incidents that could have been prevented or contained.
- Financial losses from business interruption, ransomware and recovery costs.
- Regulatory penalties and enforcement action from the USCG.
- Reputational damage with customers, partners, insurers and investors.
- Elevated insurance premiums or denial of cyber coverage.

ABOUT ABS CONSULTING

Named one of Forbes' World's Best Management Consulting Firms, ABS Consulting is a recognized leader in operational technology (OT) cybersecurity and safety, risk and compliance frameworks. Backed by more than 160 years of maritime safety heritage at ABS, the firm’s Cyber Practice has worked directly with the U.S. Coast Guard and supports MTSA-regulated entities across the maritime and energy value chain.

Sources:

1. United States Coast Guard: Cybersecurity in the Marine Transportation System

2. ABS Consulting's insight paper, "Cyber Risk Management: From Final Rule to Fully Trained: Practical Direction for Meeting the U.S. Coast Guard's Maritime Cybersecurity Requirements," authored by Michael DeVolld.

This action guide is a summary reference and does not constitute legal advice.