SHORELINE HUDSON
ACRISURE

Client Advisory 5/25

New U.S. Coast Guard Final Rule for Cybersecurity – Compliance Made Simple – A Step by Step Guide

May 2025

SHORELINE HUDSON
ACRISURE®

Author: Mike Malito
Senior Cybersecurity Consultant – Ports, Maritime, and Trade

About the Author
Mike Malito is a Senior Consultant and Business Development Specialist in ShorelineHudson's Cyber Division, advising clients across the Western Hemisphere on maritime and port cybersecurity. With a background in global technology advisory and advanced degrees in international trade and business, Mike helps organizations strengthen cyber risk management, meet compliance standards, and prepare for emerging regulations, including the upcoming USCG Final Rule, through tools like ShorelineHudson's PortLogix.

Introduction:
Effective July 16, 2025, all US ports, terminals, and Outer Continental Shelf (OCS) facilities subject to the Maritime Transportation Security Act of 2002 (MTSA) must begin a new two-year journey towards cyber compliance. US-flagged vessels will also be required to comply with new cyber standards, though there is a projected implementation delay of 2-5 years. Formally referred to as the Final Rule for Cybersecurity, this regulatory initiative aims to further institutionalize cyber best practices and strengthen protection against increasing cyber threats to maritime operations across the United States. Below are simplified key steps your facility must take to meet these requirements between now and July of 2027.

Step-by-Step Compliance Guide:
Immediate Actions (July 16, 2025):

- **Appoint a Cybersecurity Lead:** Designate an internal cybersecurity leader or interim Cybersecurity Officer (CySO).[1]
- **Incident Reporting:** The Final Rule does not create new cyber incident reporting requirements for current MTSA-regulated facilities that are subject to 33 CFR 6.16-1; however, it did add a definition for "reportable cyber incident" and created a requirement for entities that are pursuant to or not subject to 33 CFR 6.16-1 to report all reportable cyber incidents to the National Response Center (NRC).

[1] Although the Final Rule does not require a CySO to be designated in writing until July 16, 2027, it is strongly recommended to identify someone immediately who will be a go-to for managing compliance and coordinating efforts internally.

Within 6 Months (By January 12, 2026):

- **Staff Training:** Train all personnel and contractors with access to IT and operational technology (OT) systems on cybersecurity awareness, threat detection and recognition of techniques used to circumvent cyber measures, and incident reporting procedures to the CySO. This includes OT-specific cyber training for all personnel whose duties include using OT.
- **Enhanced Training:** Provide specialized training for key personnel with access to IT or remotely accessible OT systems, including contractors. Trainings must be designed around specific roles and responsibilities of key personnel during a cyber incident, including response procedures and how to maintain current knowledge of changing cyber threats and countermeasures.
- **New personnel:** New staff not in place by January 12, 2026 must complete staff and enhanced training (if applicable) within 5 days of gaining system access, and no later than 30 days of hiring.[2]

[2] Once initial trainings are completed, each must be repeated annually.

SHORELINE HUDSON
ACRISURE®

Within 24 Months (By July 16, 2027):

- **Formal Cybersecurity Officer (CySO):** Officially designate a CySO in writing to oversee cybersecurity compliance with the MTSA and communication with authorities. Submit information such as name, title, and contact info, which will be accessible to the Coast Guard 24/7. Names of each vessel and facility for which they are designated CySO must also be submitted to the Coast Guard.
- **Cybersecurity Assessment:** Conduct a thorough assessment of all critical IT and OT systems, equipment, and procedures to identify vulnerabilities, threats, and potential impacts.[3]
- **Cybersecurity Plan:** Develop and submit a comprehensive Cybersecurity Plan to the Coast Guard for approval. This plan should detail security measures including account management, network security, incident response procedures, training, and resilience strategies. This can also be a Master Plan with specific plans for each vessel/facility included.

[3] While it may uncover technical gaps that an Assessment may not, penetration testing is NOT considered a viable replacement to the Assessment component of the Final Rule.

- **Cyber Plan Training:** All personnel must complete training of the Cybersecurity Plan within 60 days of receiving approval.
- **Drills & Exercises:** Conduct cybersecurity drills twice a year and at least one comprehensive cybersecurity exercise each calendar year with no more than 18 months between exercises.
- **Maintain Security Measures:** Regularly update security measures, perform routine maintenance, timely apply patches, and periodically test your cyber defenses.
- **Recordkeeping and Documentation:** Keep clear records of all training, drills, incidents, audits, penetration tests, and cybersecurity assessments for Coast Guard inspection.
- **Annual Reviews:** Annually audit and update your Cybersecurity Plan and ensure continuous compliance.

Conclusion:
Early action and ongoing vigilance are essential. ShorelineHudson is committed to supporting you at every stage of compliance to safeguard your operations from cyber threats.

For detailed support or further questions, please reach out to your ShorelineHudson representative.

Need help with your compliance? To simplify the process, contact:

Mike Mialto
mike.malito@HudsonAnalytix.com

www.shorelinehudson.com