Coast Guard Cybersecurity Requirements for the Marine Transportation System Facilities

Summary

The U.S. Coast Guard (USCG) has issued a final rule that makes cybersecurity requirements mandatory for all U.S.-flagged vessels and maritime transportation system (MTS) facilities, including ports, energy terminals, and other installations. It mandates security controls across all critical IT and Operational Technology (OT) assets, emphasizing protection of IT-OT interfaces and OT networks due to their critical role in safety-of-life and operational continuity. Enforcement actions may include deficiency notices, detention, denial of entry, or Captain of the Port (COTP) orders to restrict vessel movement.

Bottom line: compliance is no longer voluntary guidance, it is a legal obligation with direct operational and regulatory consequences.and cooperation with competent authorities to address cyber threats effectively.

Compliance Timeline (At a Glance)

Date	Requirement
July 16, 2025	Rule effective. All reportable cyber incidents must be reported to the National Response Center immediately upon occurrence.
Jan 12, 2026 (and annually)	Cybersecurity training for all relevant personnel per 33 CFR 101.650.
July 16, 2027	Designation of a Cybersecurity Officer (CSO); Cybersecurity assessment completed; Cybersecurity plan submitted for approval.

Compliance Requirements

The rule expects a defensible program spanning the following domains, with specific expectations for OT:

Account security

- Lockouts after repeated failed logins; strong password standards
- Multi-factor authentication (MFA) on applicable systems
- Least privilege for admin/privileged accounts
- Immediate deprovisioning for personnel who depart or change roles

Device & asset security

- Accurate inventory of IT/OT assets and current network maps
- Identification of critical assets and interfaces (e.g., IT/OT gateways, vendor remote access, wireless links)

Data security

- Secure logging: privileged access to logs, integrity protection, retention supporting investigations
- Encryption in transit and at rest; protect sensitive data and OT protocol traffic where feasible

Network segmentation

- Segregate IT and OT; constrain lateral movement with layered controls (zones/conduits, allow-lists, jump hosts, brokers)
- Address complexities from diverse device types and vendor remote support

Vulnerability management & patching

- Prompt remediation of Known Exploited Vulnerabilities (KEVs) on critical IT/OT systems
- Where patching is impractical on OT, employ documented compensating controls and track risk until remediation

Xage Capabilities Mapping to USCG Requirements

Xage helps maritime operators comply with USCG cybersecurity requirements by providing consistent, centralized policy enforcement across diverse vessels and facility networks. The Xage Fabric Platform enables unified management of access controls, segmentation and policy enforcement, while generating detailed audit evidence—including who accessed what, when, and how policies changed—to support compliance verification and incident investigations.

xage SECURITY

USCG Requirement	Xage Capabilities
 **Account security (identity & access enforcement)**	Xage enforces MFA, strong password and credential policies, and least-privilege access across users and systems. It automates lockouts on failed logins and immediate credential removal for personnel departures, ensuring continuous compliance with account security requirements.
 **Device & asset security**	Xage provides continuous asset discovery and interactions map for OT systems. This ensures visibility of all connected devices, identification of unmanaged assets, and detection of new connections.
 **Data security**	Xage provides end-to-end encryption for sensitive data in transit, maintaining integrity across IT and OT networks. Its secure logging framework captures and protects logs with privileged access controls and integrity checks to meet evidentiary and regulatory standards.
 **Network segmentation**	Xage enforces Zero Trust segmentation between IT and OT environments with zone conduits and policy-based isolation. It manages vendor and remote access through secure brokers and allow-listed communications, preventing unauthorized lateral movement across network zones and assets.
 **Vulnerability management & patching**	Xage delivers compensating controls and virtual patching capabilities that immediately mitigate KEV-related risks when direct patching is not possible. It applies protocol mediation, dynamic allow-listing, and just-in-time controls to protect vulnerable OT assets until full remediation can be safely performed.

Offline Continuity & Enforcement

Xage provides secure access and protection for any asset without requiring an internet connection, maintaining full identity and access functionality even in denied, disrupted, intermittent, or limited (DDIL) environments. Access and privilege controls remain active even if a remote site or edge device loses connectivity to the central network.

To learn more about Xage Fabric's Zero Trust capabilities for IT and OT environments, read our whitepaper: **Unified Zero Trust Access and Protection for Operational Technology (OT) and Cyber Physical Systems (CPS).**