

MTSA Cybersecurity Compliance for OT Environments

What are the MTSA Cyber Regulations?

The U.S. Coast Guard is modernizing its Maritime Transportation Security Act (MTSA) regulations to address growing cybersecurity risks across the maritime sector. These updates, enforced by the **U.S. Coast Guard through NVIC 02-24**, establish mandatory cybersecurity requirements that must be incorporated into Facility and Vessel Security Plans (FSP/VSPs).

Why do these Regulations Matter in OT?

For industrial environments, this marks a critical shift: Operational Technology (OT) systems, such as DCS, SCADA, PLCs, and safety systems, must now be evaluated and protected as part of maritime security compliance. These regulations aim to enhance cyber resilience, reduce operational risk, and safeguard critical infrastructure from evolving digital threats.

Compliance Timeline

Phase 1 January 2026

Cyber Incident Reporting and OT-Specific Training

January 2026

- Align cyber incident reporting plan with NVIC 02-24
- Appoint cybersecurity officer
- Establish cybersecurity governance
- Develop and implement OT training modules
- Complete and document training activities
- Draft facility/vessel OT risk assessment plan
- Update cyber incident reporting plan
- Outline cybersecurity plan
- Launch OT-focused risk assessments
- Conduct technical control gap analysis

Phase 2 July 2026

Conduct Risk Assessment and Deploy OT Technical Controls

July 2026

- Continue site-specific OT risk assessments
- Identify and submit requests for waivers and equivalent measures
- Implement required OT technical controls (segmentation, firewalls, remote access)
- Finalize and enhance cybersecurity plan based on assessment results

Phase 2 - 3

MTSA Network (Cyber) Boundary

- Any IT or OT system used by the vessel/facility that if compromised or exploited could result in a transportation security incident (TSI)
- Including systems whose ownership, operation, or maintenance may be delegated to third parties

Phase 3 January - July 2027

USCG Approval, Validation and Ongoing MTSA Cyber Compliance

January 2027


- Approve and submit final cybersecurity plan
- Finalize and validate incident reporting plan
- Complete deployment of all technical controls
- Conduct OT-appropriate penetration testing

July 2027


- Conduct cybersecurity plan audits, updates, and required documentation
- Perform annual OT risk assessments and penetration testing
- Deliver recurring training and tabletop exercises

THE CHAMPION ADVANTAGE

 **Deep OT Expertise**
Specialized in securing Industrial Networks, Safety Systems and Control Systems

 **Regulatory-Ready Approach**
Designed to streamline U.S. Coast Guard review and reduce rework during inspections

 **Minimal Disruption**
Protects uptime and drives value while meeting regulatory deadlines

 **Trusted by Industry Leaders**
Supporting critical infrastructure clients across diverse verticals including oil & gas, terminals, chemicals, and more

Go beyond compliance.
Together we'll build resilient, secure, and future-ready operations.