CyberSurv℠
AI DRIVEN CYBERSECURITY SOLUTIONS

DATA SHEET

MARITIME CYBERSECURITY SERVICES

Inspection-Ready Cyber Compliance for Maritime Facilities and Operators

Overview

Cybersecurity is now a formal requirement under U.S. maritime security regulations.

33 CFR Part 101 Subpart F establishes mandatory cybersecurity expectations for maritime facilities and vessels regulated under MTSA, extending compliance beyond physical security into cyber risk management, governance, workforce training, and incident response.

While many maritime organizations maintain strong physical security programs under 33 CFR 105, most were not designed to demonstrate cyber inspection readiness. Missing elements often include documented cyber risk assessments, policies, training records, incident response plans, and ongoing evidence of cyber hygiene.

CyberSurv's Maritime Cybersecurity Services deliver practical, defensible, and inspection-ready cyber compliance aligned to Subpart F, without operational disruption or mandatory technology replacement.

What CyberSurv Delivers

CyberSurv helps maritime facilities and operators meet Subpart F through a structured, security-first approach that produces inspection-ready evidence as a natural outcome of operations. Services are delivered and tracked through a secure cyber operations platform that provides centralized visibility, documentation, and audit-ready reporting.

Subpart F–Aligned Services

- **Maritime Cyber Risk Assessment** - Identification of cyber systems supporting maritime operations, including IT, OT, access control, cargo, and safety systems. Risk assessments are aligned to maritime threat realities and documented to support Coast Guard inspection and annual review requirements.
- **Cyber Governance & Policy Development** - Development of maritime-appropriate cybersecurity policies and procedures, including access control, authentication standards, third-party risk controls, and defined roles and accountability.
- **Workforce Cybersecurity Readiness -** Maritime-specific cybersecurity awareness training and role-based instruction, supported by inspection-ready training records

and reporting.

- **Cyber Incident Response & Recovery -** Cyber incident response plans aligned with Facility Security Plans, including response procedures, reporting workflows, and recovery coordination. Tabletop exercises are available to validate readiness.
- **Ongoing Cyber Hygiene & Monitoring -** Continuous oversight of cyber risk conditions with documented findings, trend visibility, and compliance evidence maintained within a centralized platform.

How CyberSurv Supports Maritime Operations

CyberSurv services are designed to integrate cleanly into existing maritime security programs and complement physical security teams and maritime security consultants. Key principles include:

- **Security-First Execution** - Real risk reduction, not checklist compliance
- **Inspection-Ready by Design** - Documentation generated through normal operations
- **Vendor-Neutral Advisory** - No forced technology replacement
- **Operationally Practical** - built for real maritime environments

Why This Matters for Maritime Compliance

Attackers do not exploit compliance gaps, they exploit weak credentials, misconfigured access, unpatched systems, and vendor trust relationships. CyberSurv focuses on reducing these risks while ensuring organizations can clearly demonstrate compliance during inspection, audit, or investigation.

Ideal Clients

- Port Authorities
- Terminal Operators
- Maritime Facility Operators
- Maritime Logistics Providers
- Offshore and Energy Maritime Operators
- Maritime Security and Compliance Consultants

About CyberSurv

CyberSurv is a veteran-led cybersecurity and AI-enhanced security services firm helping regulated and critical infrastructure organizations achieve continuous cyber hygiene, inspection readiness, and operational cyber resilience.

EMPOWER. INNOVATE. FORTIFY.

CONTACT US TODAY FOR A FREE CONSULTATION
info@cybersurv.com | (877) 940-4344 | www.cybersurv.com