Information Provided by Trident Group America, Inc

THE LAW HAS LANDED:

USCG CYBERSECURITY RULE

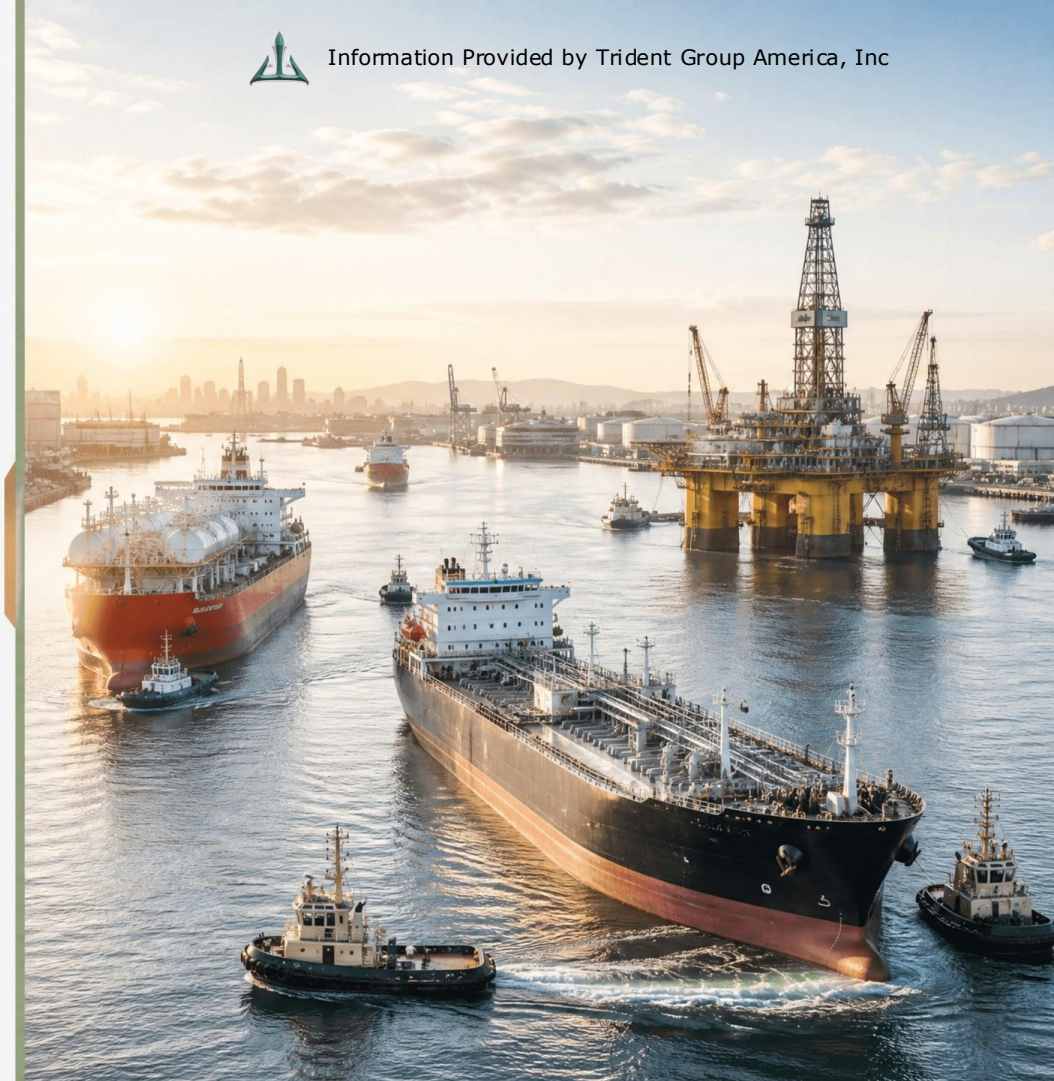
A Practical Quick Guide for Field Compliance and Operational Readiness

WHO MUST COMPLY: THE SCOPE OF REGULATION

Identifying Covered Entities and Practical Commercial Realities

- **MTSA-REGULATED ENTITIES:** The rule applies to U.S.-flagged vessels subject to MTSA 2002, Outer Continental Shelf (OCS) facilities, and MTSA-regulated waterfront facilities.
- **ADDITIVE REQUIREMENTS:** These cybersecurity mandates are additive to existing MTSA physical security plans, not replacements, requiring integrated security management.
- **FOREIGN-FLAGGED IMPACT:** While not directly covered, foreign vessels face intensified Port State Control scrutiny and commercial pressure from MTSA-regulated terminals.
- **SUPPLY CHAIN PRESSURE:** Charterers and cargo owners increasingly require evidence of cybersecurity compliance from all counterparties, making the rule a de facto industry standard.

Information Provided by Trident Group America, Inc



Information Provided by Trident Group America, Inc

PHASE 1: IMMEDIATE INCIDENT REPORTING

Mandatory NRC Notification for All Reportable Cyber Events

1. REPORTING DEADLINE: Effective July 16, 2025, all covered entities must report reportable cyber incidents to the National Response Center (NRC) without delay.

2. REPORTABLE INCIDENTS: Includes events that disrupt operations, compromise critical IT/OT systems, impact safety/security, or trigger incident response plans.

3. CONFIDENTIALITY & INTEGRITY: Any breach affecting the confidentiality, integrity, or availability of critical maritime cyber systems must be formally documented and reported.

4. ENFORCEMENT SHIFT: This phase marks the end of voluntary reporting, with the USCG now tracking incidents to build a comprehensive national maritime threat picture.

PHASE 2: MANDATORY PERSONNEL TRAINING

Ensuring Workforce Readiness and Cybersecurity Awareness

- **DEADLINE PASSED:** The January 12, 2026 deadline for initial training has passed; all personnel with IT/OT system access must now be fully trained and certified.
- **TWO-TIERED STRUCTURE:** Training includes general awareness for all staff and role-specific technical training for those managing remotely accessible OT systems.
- **NEW HIRE PROTOCOL:** All new personnel must complete required cybersecurity training within 30 days of gaining access to any covered vessel or facility systems.
- **ANNUAL REFRESHERS:** Compliance requires documented annual refresher training to ensure personnel remain current on evolving threats and reporting procedures.

Information Provided by Trident Group America, Inc

PHASE 3: THE 2027 COMPLIANCE MILESTONE

Preparing for the Most Substantive Regulatory Deliverables

1. JULY 16, 2027 DEADLINE: Requires the simultaneous delivery of a designated Cybersecurity Officer, a completed Assessment, and a USCG-approved Plan.

2. SEQUENCING CONSTRAINT: The Assessment must be completed first to inform the Plan's content, and the Officer must be designated to oversee both processes.

3. REVIEW BUFFER: Operators must account for an unknown USCG review period; waiting until mid-2027 to submit will likely result in a compliance gap.

4. OPERATIONAL URGENCY: For operators who haven't started, the timeline is tighter than it appears due to the complexity of OT system inventories and network mapping.

Information Provided by Trident Group America, Inc

Information Provided by Trident Group America, Inc

THE CYBERSECURITY OFFICER (CySO)

Accountability, Qualifications, and Structural Flexibility

1. DESIGNATED ACCOUNTABILITY:

The CySO is the individual responsible for the compliance architecture, overseeing implementation and certifying the Plan's adequacy.

2. FUNCTIONAL QUALIFICATIONS:

Must possess knowledge of cyber administration, relevant laws, risk methodologies, and procedures for drills and exercises.

3. STRUCTURAL FLEXIBILITY:

A single CySO can cover multiple vessels or facilities, and the role can be filled by full-time staff, collateral duty, or contracted consultants.

4. AUTHORITY & RESOURCES:

Regardless of employment status, the CySO must have sufficient authority and resources to fulfill the role's substantive legal requirements.

Information Provided by Trident Group America, Inc

THE CYBERSECURITY ASSESSMENT

The Foundational Evaluation of IT and OT Environments

1. **COMPREHENSIVE SCOPE:**
   Not a simple audit; it's a full evaluation of IT/OT systems, network interconnections, and the effectiveness of existing security controls.

2. **CRITICAL SYSTEM INVENTORY:**
   Must identify all systems whose compromise would affect vessel safety, cargo integrity, or core operational capabilities.

3. **TECHNICAL EVALUATION:**
   Includes assessing access controls (MFA), network segmentation, patch management, and the reliability of backup/recovery procedures.

4. **EVIDENCE-BASED:**
   Requires documented proof of network diagrams, remote access inventories, and test evidence that default credentials have been removed.

Information Provided by Trident Group America, Inc

THE CYBERSECURITY PLAN (CySP)

Translating Assessment Findings into Operational Security

1. **SIX FUNCTIONAL DOMAINS:** The Plan must cover access protection, incident detection/ reporting, response/recovery, supply chain governance, training, and drills.

2. **SUBMISSION & CERTIFICATION:** Must be submitted to the USCG by **July 16, 2027,** constituting the operator's formal certification of regulatory compliance.

3. **RECURRING OBLIGATIONS:** Plans must be renewed every five years, with mandatory penetration testing required in conjunction with each renewal cycle.

4. **ANNUAL AUDIT REQUIREMENT:** Operators must conduct internal cybersecurity audits at least annually to ensure the Plan remains effective and up to date.

Information Provided by Trident Group America, Inc

COMMON IMPLEMENTATION GAPS

Critical Areas Where Early Implementation Often Fails in the Field

1. **NETWORK SEGMENTATION:**
   The most technically challenging requirement; separating legacy OT systems from IT networks often requires significant modification.

2. **THEORETICAL PLANNING:**
   Many incident response plans are created for compliance but fail when tested against realistic, high-pressure operational scenarios.

3. **VENDOR GOVERNANCE:**
   Managing third-party and supplier access to critical systems remains a major vulnerability that assessments often overlook.

4. **DOCUMENTATION VS. CAPABILITY:**
   The USCG requires actual security capability, not just the documentation of intended measures; performance is the metric.

CONCLUSION: A NEW ERA OF MARITIME SECURITY

Moving from Voluntary Guidance to Mandatory Federal Accountability

1. **ENFORCEABLE STANDARDS:**
   The USCG rule represents a permanent shift in maritime security, making cybersecurity as mandatory as physical safety.

2. **PROACTIVE INVESTMENT:**
   Successful compliance requires treating the rule as a genuine security investment rather than a last-minute documentation project.

3. **CONTINUOUS VIGILANCE:**
   With 828 maritime cyber incidents in 2025 alone, the threat environment provides the ultimate motivation for robust implementation.

4. **OPERATIONAL RESILIENCE:**
   Building a compliant cybersecurity posture ensures long-term operational legality and resilience against evolving global threats.

Information Provided by Trident Group America, Inc