LOCH TECHNOLOGIES

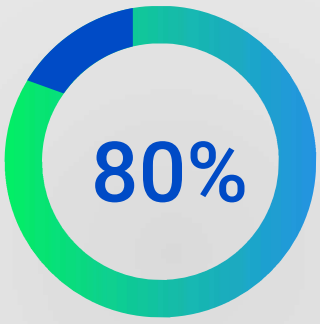
Defend the Digital Dock

Wireless Airspace Defense for U.S. Coast Guard 2025 MTS Cybersecurity Compliance

A Tactical Guide for Maritime Operators to Expose Hidden Wireless Threats and Achieve Full-Spectrum Cyber Resilience

The Growing Problem: The Wireless Blind Spot in Maritime Cybersecurity

Modern ports rely on wireless connectivity—GPS, 4G/5G, Bluetooth, Wi-Fi, CBRS, LPWAN—for everything from vessel navigation to crane operation and logistics. Yet, wireless is the most unmonitored and least secured vector in maritime environments.



80%+ of port-side devices now connect wirelessly

- Traditional IT tools provide no visibility into wireless activity
- GPS spoofing, rogue LTE modems, Bluetooth skimmers, and RF jammers are being used for cyber-physical disruption
- These threats can interfere with OT systems, leading to operational downtime, lost cargo, and even vessel collisions

Business Impact: Downtime, Fines, and Non-Compliance

Risk	Impact on Operations
Rogue Access Points	Enable covert intrusion into OT systems
GPS Spoofing	Causes navigation errors, vessel grounding, cargo delays
Unmanaged Wireless/IoT Devices	Creates backdoors for attackers via BYOD or third-party devices
RF Jamming or Signal Interference	Interrupts port logistics, ship communications, and safety systems
Lack of Continuous Monitoring	Results in failure to meet 33 CFR 106 cybersecurity mandates
No Forensic Data	Makes it impossible to investigate, respond, or demonstrate compliance during audits

Regulatory Urgency: USCG's 2025 Cybersecurity Rule (33 CFR 106)

Effective July 16, 2025, all MTSA-regulated facilities must implement:

- Baseline Cyber Risk Assessments
- Continuous Cybersecurity Monitoring
- Incident Response Plans
- Documentation and Audit Readiness
- Enforcement of Cybersecurity Procedures & Controls

These requirements explicitly extend to wireless and RF-based cyber threats—an area unmonitored by most maritime cybersecurity stacks today.

The LOCH Solution: Full-Spectrum Cyber Visibility

LOCH Technologies' AirShield (wireless) and NetShield (wired) platforms provide a unified cybersecurity defense across Ethernet, Wi-Fi, Cellular, GPS, Bluetooth, CBRS, LPWAN, and beyond.

LOCH TECHNOLOGIES

Together, they offer:

01 **Real-Time RF Detection:** From rogue APs to fake GPS towers

02 **Zero Trust Enforcement:** Across all wireless communications

03 **SIEM/SOAR/CMDB Integrations:** For response and compliance logging

04 **Cloud + On-Prem Deployment:** Built for critical infrastructure flexibility

Mapping LOCH to the USCG 33 CFR 106 Cybersecurity Requirements

USCG Rule	LOCH Capability	Mapped Compliance Area
106.230 – Cyber Risk Assessment	AirShield discovers and classifies all RF-connected devices across Cellular, Wi-Fi, Bluetooth, GPS, LPWAN, CBRS	Asset Visibility
106.235 – Cybersecurity Procedures & Controls	Zero Trust policy enforcement, real-time anomaly detection, GPS spoof/jam detection	Zero Trust Implementation
106.240 – Incident Response Plan	AI-driven threat detection, RF forensic logging, SIEM/SOAR integration	Incident Response
106.245 – Documentation & Compliance	Centralized dashboards, audit-ready reporting, CMDB/NAC integrations	Audit Readiness
106.250 – Continuous Monitoring	Persistent RF monitoring from 300 MHz–6 GHz, alerts across Wi-Fi, 4G/5G, GPS, CBRS, BLE	Continuous Wireless Monitoring
Implicit – Vulnerability Management	Identification of rogue devices, misconfigured wireless assets, tampered IoT hardware	Risk Mitigation
Implicit – Supply Chain Threat Detection	Exposes embedded threats in third-party wireless equipment	Supply Chain Risk Management

Side-by-Side Comparison: LOCH vs. Traditional Cyber Tools

Capability	LOCH (AirShield + NetShield)	Legacy Cyber Tools
Wireless Threat Visibility	Yes – 300 MHz to 6 GHz RF detection	No
Shadow IoT Discovery	Yes – cellular/BLE/LoRa/Zigbee/CBRS	No
Real-Time Threat Detection	Continuous 24/7	Periodic or reactive
Zero Trust for Wireless	Enforced via policy + alerts	Not supported
GPS Spoofing Detection	Integrated	Not detected
Audit-Ready Compliance	Dashboards, logs, reports	Manual or partial

Sector-Proven Value

LOCH's wireless airspace defense is actively deployed across mission-critical and high-security environments, helping organizations detect invisible wireless threats, enforce Zero Trust, and achieve compliance.

Seaports & Maritime: Detected rogue LTE modems, GPS spoofing attempts, and unsecured wireless PLC broadcasts; enforced wireless isolation zones to protect cargo operations and logistics systems.

Airports & Aviation: Identified fake cellular towers and Bluetooth skimmers near passenger terminals; secured airside operations from drone incursions and RF interference targeting navigation systems.

Defense & SCIFs: Enforced RF isolation in secure facilities; uncovered covert Bluetooth modules and unauthorized surveillance devices within classified areas.

Healthcare: Detected HIPAA violations from shadow IoT devices; monitored WMTS, MedRadio, and HL7 traffic for unauthorized access and RF anomalies.

Retail & Hospitality: Blocked PoS skimmers, RF jammers, and rogue APs; ensured PCI compliance and protected guests from wireless eavesdropping and surveillance.

What Happens If You Don't Act?

- You'll miss 80% of the devices in your port environment
- Your cyber risk assessments and incident response will be non-compliant
- You'll have no forensic trail to support audits or incident investigations
- You could face fines, cargo delays, and operational shutdowns

"Wireless has created the world's largest attack surface—each device an entry point for threats." – LOCH Technologies, Feb 2025

Summary: Why LOCH is Critical for MTS Compliance and Cyber Defense

Feature	Benefit to MTS Operators
Full RF Visibility	Detect threats across 300 MHz – 6 GHz
Unified Wired + Wireless Security	Converged threat detection for OT + IT systems
Real-Time Alerting	Detect rogue access, GPS spoofing, jammers
Compliance Mapping	Built-in support for 33 CFR 106, NIST, MTSA, NERC CIP
Flexible Deployment	Passive RF sensors, SaaS or on-prem control
Proven Results	Deployed in maritime, defense, healthcare, and retail