

Maritime Transportation Security Act (MTSA) Compliance Assessment

2023

DeepShield Systems, Inc.

Assessment Period: January 1, 2023 - December 31, 2023

Document Reference: MTSA-CA-2023-001

1. Executive Summary

This Maritime Transportation Security Act (MTSA) Compliance Assessment evaluates DeepShield Systems, Inc.'s ("DeepShield") adherence to MTSA requirements as they relate to the company's maritime cybersecurity solutions and services provided to regulated facilities and vessels. This assessment was conducted by DeepShield's Legal and Compliance Department in conjunction with external maritime security counsel.

2. Scope of Assessment

1. This assessment covers:

- DeepShield's OceanGuard(TM) Maritime Cybersecurity Platform
- DeepShield Port Security Management System
- Vessel Security Plan (VSP) Integration Services
- Facility Security Plan (FSP) Compliance Modules
- Maritime Operations Center (MOC) Security Solutions

2. Relevant MTSA Provisions:

- 33 CFR Part 104 (Vessel Security)
- 33 CFR Part 105 (Facility Security)
- 33 CFR Part 106 (Offshore Facility Security)
- Navigation and Vessel Inspection Circular (NVIC) 01-20

3. Compliance Status

1. Product Certification

DeepShield's maritime security products have maintained current certification under:

- USCG Type Approval for Maritime Security Systems

- Certificate Number: USCG-MSS-2023-478
- Validation Period: March 15, 2023 - March 14, 2024

2. Security Plan Integration

DeepShield's solutions demonstrate compliance with:

- Facility Security Plan Requirements (33 CFR 105.405)
- Vessel Security Plan Requirements (33 CFR 104.405)
- Cybersecurity Framework Integration (NVIC 01-20)

4. Risk Assessment Findings

1. Critical Infrastructure Protection

- Implementation of MTSA-compliant access control systems
- Integration with existing physical security infrastructure
- Automated threat detection and response capabilities
- Real-time maritime domain awareness features

2. Cybersecurity Controls

- Multi-layer authentication protocols
- Encrypted communications channels
- Secure system architecture
- Regular penetration testing and vulnerability assessments

5. Compliance Gaps and Remediation

1. Identified Gaps

- Minor documentation updates required for new NVIC guidance
- Enhanced audit trail functionality needed for certain legacy systems
- Additional training modules required for updated regulations

2. Remediation Timeline

- Documentation Updates: Completed by Q1 2024
- System Enhancements: Implementation by Q2 2024
- Training Program Updates: Roll-out by Q3 2024

6. Certification and Testing

1. Third-Party Validation

- Annual security assessment conducted by MaritimeSec Associates, LLC
- Penetration testing performed by CyberMarine Security Partners
- Compliance verification by USCG-approved independent validators

2. Testing Protocols

- Quarterly security control testing
- Monthly vulnerability assessments
- Bi-annual full-system security exercises

7. Regulatory Reporting and Documentation

1. Required Reports

- Annual Security Assessment Report (SAR)
- Quarterly Compliance Updates
- Incident Response Reports (as needed)
- Security Exercise Documentation

2. Record Retention

All documentation maintained in accordance with 33 CFR 104.235 and 105.225

8. Legal Attestation

The undersigned hereby certifies that this assessment has been conducted in accordance with applicable MTSA requirements and represents a true and accurate evaluation of DeepShield Systems, Inc.'s compliance status as of the date of this document.

9. Signatures and Approvals

EXECUTED this 15th day of December, 2023

/s/ Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

/s/ James Morrison

James Morrison

VP of Engineering

DeepShield Systems, Inc.

/s/ Robert Kessler

Robert Kessler

Chief Financial Officer

DeepShield Systems, Inc.

10. Disclaimer

This assessment is confidential and proprietary to DeepShield Systems, Inc. It has been prepared solely for internal use and regulatory compliance purposes. While every effort has been made to ensure accuracy, this document should not be relied upon as legal advice. Regulatory requirements are subject to change, and compliance status must be continuously monitored and updated.