SINGAPORE MARITIME AUTHORITY SECURITY AUDIT REPORT

Audit Reference: SMA-2023-0472

Date of Report: December 15, 2023

Entity Audited: DeepShield Systems, Inc.

1. EXECUTIVE SUMMARY

This security audit report documents the comprehensive assessment conducted by the Singapore Maritime Authority (SMA) of DeepShield Systems, Inc.'s maritime cybersecurity solutions deployed across Singapore's critical maritime infrastructure. The audit was performed between October 1-30, 2023, pursuant to Maritime Cybersecurity Code 2021 (MCC 2021) requirements.

1.1 Audit Scope

- DeepShield Maritime Defense Platform v4.2.1
- OT Network Monitoring Systems
- Maritime-SCADA Integration Modules
- Port Authority Integration Systems
- Emergency Response Protocols

1.2 Key Findings

The audit confirms DeepShield Systems' substantial compliance with MCC 2021 requirements, with identified areas for enhancement in Section 4. No critical security vulnerabilities were detected.

2. SYSTEM ARCHITECTURE ASSESSMENT

2.1 Core Platform Architecture

DeepShield's Maritime Defense Platform demonstrates robust security architecture with:

- Multi-layered authentication protocols
- Encrypted communication channels (AES-256)
- Redundant failover systems
- Real-time threat monitoring capabilities

2.2 Network Segmentation

Implementation of network segregation meets SMA requirements through:

- Physical separation of OT/IT networks
- VLAN implementation per MCC 2021 3.4
- Dedicated maritime operations network
- Secure gateway interfaces

3. SECURITY CONTROLS EVALUATION

3.1 Access Control Systems

- Multi-factor authentication implemented across all critical access points
- Role-based access control (RBAC) properly configured
- Privileged access management protocols in place
- Regular access review cycles documented

3.2 Threat Detection Capabilities

- AI-driven anomaly detection system exceeds MCC 2021 requirements
- Real-time monitoring of maritime control systems
- Integration with national maritime threat intelligence feeds
- Automated incident response protocols validated

3.3 Data Protection Measures

- Encryption standards comply with MCC 2021 4.2
- Secure key management procedures implemented
- Data retention policies properly enforced
- Backup systems tested and verified

4. COMPLIANCE ASSESSMENT

4.1 Regulatory Compliance

DeepShield Systems demonstrates compliance with:

- Maritime Cybersecurity Code 2021
- International Ship and Port Facility Security (ISPS) Code
- ISO 27001:2013 requirements
- Maritime and Port Authority of Singapore (MPA) guidelines

4.2 Required Improvements

The following enhancements are required within 90 days:

Implementation of additional logging mechanisms for privileged user actions

Enhancement of backup verification procedures

Update of incident response documentation

Strengthening of third-party access controls

5. PENETRATION TESTING RESULTS

5.1 Testing Methodology

- Black box testing of external interfaces
- Grey box testing of internal systems
- Social engineering resistance assessment
- Physical security controls evaluation

5.2 Findings Summary

- No critical vulnerabilities identified
- Three (3) medium-risk findings documented
- Seven (7) low-risk findings noted
- All findings detailed in Appendix A

6. INCIDENT RESPONSE CAPABILITIES

6.1 Response Protocols

- Incident classification system validated
- Response team structure appropriate
- Communication protocols tested
- Recovery procedures documented

6.2 Business Continuity

- Failover systems tested successfully
- Recovery time objectives (RTO) met
- Disaster recovery procedures validated
- Emergency communication systems verified

7. RECOMMENDATIONS

7.1 Short-term Actions (0-90 days)

Implement enhanced privileged access monitoring

Update incident response documentation

Strengthen backup verification procedures

Enhance third-party access controls

7.2 Long-term Improvements (90-180 days)

Expand AI-driven threat detection capabilities

Enhance integration with national security frameworks

Implement additional redundancy measures

Strengthen supply chain security controls

8. CERTIFICATION STATEMENT

Based on the comprehensive audit conducted, DeepShield Systems, Inc.'s maritime security solutions substantially comply with Singapore Maritime Authority requirements, subject to the implementation of improvements noted in Section 4.2.

9. AUDIT TEAM

Lead Auditor: Capt. Lawrence Tan

Technical Assessor: Dr. Sarah Wong

Security Specialist: Mr. David Kumar

Maritime Systems Expert: Ms. Jennifer Lim

10. DISCLAIMERS AND LIMITATIONS

This report is provided pursuant to Singapore Maritime Authority regulations and is subject to the following limitations:

The audit represents system status as of the audit date

Findings are based on systems and configurations presented

Future security threats may impact current security posture

Report is confidential and for authorized use only

APPENDICES

Appendix A: Detailed Vulnerability Findings

Appendix B: Test Cases and Results

Appendix C: System Architecture Diagrams

Appendix D: Compliance Matrices

APPROVED BY:

[Signature]

Capt. Lawrence Tan

Lead Auditor, Singapore Maritime Authority

Registration: SMA-LA-2023-0891

Date: December 15, 2023

[Official SMA Seal]