DNV-GL Maritime Cybersecurity Certification Documentation

Certificate Number: MCSC-2023-0472-DS

Issued: September 15, 2023

1. Certification Overview

This document certifies that DeepShield Systems, Inc. ("DeepShield"), incorporated in Delaware, has successfully completed the DNV-GL Maritime Cybersecurity Certification Program in accordance with DNV-GL-CP-0231 standards and has demonstrated compliance with:

1. IMO Resolution MSC.428(98) on Maritime Cyber Risk Management
2. Guidelines on Cyber Security Onboard Ships v4.0
3. IEC 62443 Security for Industrial Automation and Control Systems
4. NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

2. Certified Products and Solutions

1. The following DeepShield maritime cybersecurity solutions have been evaluated and certified:

a) DeepShield Maritime Defense Platform(TM) v4.2

b) OceanGuard ICS Protection Suite(TM) v3.1

c) MarineWatch Network Monitoring System(TM) v2.8

d) Subsea Infrastructure Protection Module(TM) v1.5

2. Certification scope includes all associated software components, security protocols, and integration interfaces as detailed in Technical Appendix A (Reference: DS-TECH-2023-091).

3. Compliance Verification

1. Security Controls Assessment

- Comprehensive evaluation of security architecture
- Penetration testing of maritime-specific attack vectors
- Verification of compliance with BIMCO cybersecurity guidelines
- Assessment of integration capabilities with shipboard systems

2. Testing Environment

- Simulated maritime operational technology (OT) environment
- Virtual ship network configuration
- Integration testing with major vessel control systems
- Emergency response scenario validation

4. Certification Parameters

1. Validity Period

- Initial Certification Date: September 15, 2023
- Expiration Date: September 14, 2026
- Subject to annual surveillance audits

2. Applicable Vessel Types

- Commercial cargo vessels
- Passenger ships
- Offshore support vessels
- Special purpose ships
- Mobile offshore drilling units

5. Technical Compliance Specifications

1. The certified solutions meet or exceed the following technical requirements:

a) Network Segmentation

- Physical and logical separation of operational networks
- Dedicated maritime VLAN configurations
- Secure gateway implementations
- Protected operational technology boundaries

b) Access Control

- Role-based access control (RBAC) implementation
- Multi-factor authentication for critical systems
- Privileged access management
- Emergency access protocols

c) Threat Detection

- Real-time monitoring of maritime networks
- AI-driven anomaly detection
- SCADA-specific threat identification
- Integration with maritime security information sharing platforms

6. Certification Conditions

1. DeepShield Systems, Inc. shall:

a) Maintain continuous compliance with DNV-GL certification requirements

b) Implement security patches and updates within specified timeframes

c) Report significant security incidents to DNV-GL

d) Participate in annual surveillance audits

e) Maintain detailed documentation of all system modifications

2. This certification may be suspended or revoked if:

a) Critical security vulnerabilities are not addressed

b) Required updates are not implemented

c) Annual surveillance audits are not completed

d) Significant changes to certified systems are not reported

7. Legal Disclaimers

1. This certification represents compliance with standards at the time of assessment and does not guarantee future security performance.

2. DNV-GL assumes no liability for security incidents or breaches occurring in certified systems.

3. This certification is non-transferable and specific to the versions and configurations tested.

8. Authorization

Certified by DNV-GL Maritime Cybersecurity Certification Authority

_

Dr. Henrik Nordstrom

Principal Certification Officer

DNV-GL Maritime Cybersecurity Division

_

Maria Svenson

Technical Reviewer

DNV-GL Maritime Cybersecurity Division

Date: September 15, 2023

Location: Hamburg, Germany

9. Document Control

Document ID: MCSC-2023-0472-DS-CERT

Version: 1.0

Classification: Confidential

Distribution: Controlled Copy

[END OF CERTIFICATION DOCUMENT]