SECURITY AUDIT COMPLIANCE CERTIFICATE

CERTIFICATE DATE: January 11, 2024

COMPANY: DeepShield Systems, Inc.

PERIOD COVERED: January 1, 2023 - December 31, 2023

CERTIFICATE NUMBER: SAC-2024-001

1. CERTIFICATION STATEMENT

The undersigned, in their capacity as Chief Security Architect of DeepShield Systems, Inc., a Delaware corporation (the "Company"), hereby certifies that:

2. AUDIT SCOPE AND STANDARDS

1. The Company has undergone comprehensive security audits and assessments in accordance with:

(a) ISO/IEC 27001:2013 Information Security Management Systems

(b) NIST Cybersecurity Framework v1.1

(c) IEC 62443 Industrial Network and System Security

(d) Maritime Cybersecurity Framework (BIMCO Guidelines)

(e) Critical Infrastructure Protection (CIP) Standards

2. The audit scope encompassed:

(a) All production environments hosting the DeepShield Industrial Control System (ICS) Security Platform

(b) Operational Technology (OT) monitoring infrastructure

(c) Threat detection and response systems

(d) Maritime and subsea infrastructure protection modules

(e) Development and testing environments

(f) Corporate information systems and networks

3. COMPLIANCE VERIFICATION

1. Based on the results of internal and external security audits conducted during the Period Covered, the Company hereby confirms:

(a) Full compliance with all applicable security standards listed in Section 2.1

(b) Implementation of required technical controls

(c) Maintenance of documented security policies and procedures

(d) Regular security training for all personnel

(e) Incident response and business continuity planning

(f) Supply chain security management

2. The following independent third-party assessments have been completed:

(a) Annual SOC 2 Type II Audit by Ernst & Young LLP

(b) Penetration Testing by NCC Group

(c) Industrial Control Systems Security Assessment by Dragos, Inc.

(d) Maritime Systems Security Verification by DNV GL

4. SECURITY CONTROLS AND MEASURES

1. Network Security

- Segmented architecture with defined security zones
- Next-generation firewalls with IPS/IDS capabilities
- Encrypted communications using TLS 1.3
- Regular vulnerability scanning and remediation
- Network access control and monitoring

2. System Security

- Hardened system configurations
- Regular security patches and updates
- Privileged access management
- Multi-factor authentication
- Endpoint protection and EDR solutions

3. Data Security

- Data classification and handling procedures
- Encryption at rest and in transit
- Secure backup and recovery systems

- Data loss prevention controls
- Privacy controls for GDPR compliance

4. Operational Security

- 24/7 Security Operations Center
- Incident response procedures
- Change management controls
- Asset management system
- Security monitoring and logging

5. MATERIAL FINDINGS AND REMEDIATION

1. During the Period Covered, the following material findings were identified and remediated:

(a) Finding: Legacy protocol support in maritime module requiring additional encryption

- Remediation: Implemented additional encryption layer
- Completion Date: March 15, 2023
- Verified By: Maritime Systems Security Team

(b) Finding: Access control granularity improvement needed for OT systems

- Remediation: Enhanced role-based access control system
- Completion Date: June 30, 2023
- Verified By: Internal Security Team

2. No critical or high-risk findings remain open as of the Certificate Date.

6. ONGOING COMPLIANCE MONITORING

1. The Company maintains continuous compliance monitoring through:

- Automated security testing and validation
- Regular internal audits
- Compliance dashboard monitoring
- Quarterly security reviews
- Annual third-party assessments

2. Security metrics and KPIs are tracked and reported monthly to the Board of Directors.

7. REPRESENTATIONS AND WARRANTIES

The undersigned hereby represents and warrants that:

1. All statements contained in this Certificate are true and accurate as of the Certificate Date.

2. The Company maintains all necessary licenses, certifications, and authorizations required for its security operations.

3. All security incidents during the Period Covered have been properly documented, investigated, and resolved according to established procedures.

8. LIMITATIONS AND DISCLAIMERS

1. This Certificate relates solely to the security controls and compliance status as of the Certificate Date.

2. No representation is made regarding future security posture or compliance status.

3. This Certificate shall not be construed as a guarantee against security breaches or incidents.

9. CONFIDENTIALITY

This Certificate contains confidential and proprietary information of the Company and shall be treated as Confidential Information under applicable non-disclosure agreements.

10. EXECUTION

IN WITNESS WHEREOF, the undersigned has executed this Security Audit Compliance Certificate as of the Certificate Date.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

WITNESS:

By:

Name: James Morrison

Title: VP of Engineering

11. ATTACHMENTS

Appendix A: Summary of Security Audit Results

Appendix B: Compliance Testing Evidence

Appendix C: Third-Party Assessment Reports

Appendix D: Remediation Documentation

[END OF CERTIFICATE]