SECURITY SYSTEM CERTIFICATION DOCUMENT

EFFECTIVE DATE: January 11, 2024

DOCUMENT NUMBER: SEC-CERT-2024-011

ISSUING ENTITY: DeepShield Systems, Inc.

CLASSIFICATION: Confidential

1. CERTIFICATION OVERVIEW

1. This Security System Certification Document ("Certification") is issued by DeepShield Systems, Inc., a Delaware corporation ("DeepShield" or the "Company"), to certify the security capabilities, compliance status, and operational effectiveness of its Industrial Control System (ICS) security solutions and Critical Infrastructure Protection platform (the "System").

2. This Certification encompasses all components of DeepShield's proprietary deep-layer security architecture, including but not limited to:

a) Network monitoring systems

b) Threat detection modules

c) Incident response frameworks

d) Maritime protection solutions

e) SCADA security implementations

2. SYSTEM SPECIFICATIONS

1. The System implements the following security architecture components:

1.1. **Core Security Framework**

- Multi-layered defense architecture (Patent No. US 11,234,567)
- Real-time threat detection using AI-driven analytics
- Adaptive response mechanisms for OT environments
- Proprietary DeepShield Security Protocol (DSP) v4.2

1.2. **Monitoring Capabilities**

- Continuous network traffic analysis
- Behavioral anomaly detection

- Asset inventory management
- Protocol-specific deep packet inspection

3. COMPLIANCE CERTIFICATIONS

1. The System has been independently verified to meet or exceed the following standards:

a) IEC 62443 Security Levels 1-4

b) NIST Cybersecurity Framework v1.1

c) ISO/IEC 27001:2022

d) Maritime Cybersecurity Framework (MCF) Level 3

e) Critical Infrastructure Protection Standards (NERC CIP) v6

2. Third-party validation has been performed by:

- CyberTrust International (Certification #CTI-2023-456)
- Industrial Security Alliance (ISA) Certification Board
- Maritime Security Verification Council

4. SECURITY TESTING AND VALIDATION

1. The System undergoes continuous security testing, including:

1.1. **Periodic Assessments**

- Quarterly penetration testing
- Monthly vulnerability scanning
- Bi-annual red team exercises
- Continuous automated security testing

1.2. **Performance Metrics**

- Mean Time to Detect (MTTD): < 2 minutes
- Mean Time to Respond (MTTR): < 5 minutes
- False Positive Rate: < 0.01%
- System Availability: 99.999%

5. OPERATIONAL SAFEGUARDS

1. DeepShield maintains the following operational security measures:

a) 24/7 Security Operations Center (SOC)

b) Incident Response Team with 15-minute SLA

c) Redundant monitoring systems

d) Geographically distributed backup facilities

e) Annual disaster recovery testing

2. All system components are subject to:

- Weekly security updates
- Monthly configuration reviews
- Quarterly compliance audits
- Annual certification renewal

6. WARRANTY AND LIMITATIONS

1. DeepShield warrants that the System meets all specifications detailed in this Certification as of the Effective Date.

2. This Certification is valid for one (1) year from the Effective Date and must be renewed annually.

3. DISCLAIMER: While DeepShield employs industry-leading security measures, no security system can guarantee complete protection against all potential threats or vulnerabilities.

7. CERTIFICATION AUTHORITY

This Security System Certification Document is issued under the authority of DeepShield Systems, Inc.'s Executive Management and Security Review Board.

8. EXECUTION

IN WITNESS WHEREOF, the undersigned, being duly authorized representatives of DeepShield Systems, Inc., have executed this Security System Certification Document as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

By:

Name: James Morrison

Title: VP of Engineering

WITNESSED BY:

By:

Name: Robert Kessler

Title: Chief Financial Officer

[CORPORATE SEAL]