NIST CYBERSECURITY FRAMEWORK ALIGNMENT ASSESSMENT

DeepShield Systems, Inc.

Assessment Date: January 11, 2024

Document Reference: NIST-CSF-2024-001

1. EXECUTIVE SUMMARY

This document presents DeepShield Systems, Inc.'s ("DeepShield" or the "Company") formal assessment of alignment with the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"). This assessment was conducted by the Company's Information Security and Legal departments in coordination with external cybersecurity consultants from SecureStack Advisory Group.

2. FRAMEWORK IMPLEMENTATION TIERS

DeepShield Systems has achieved the following implementation tiers across the core NIST CSF functions:

1. **Identify (ID)**: Tier 4 - Adaptive
- Comprehensive asset management system covering all OT/ICS environments
- Documented business environment and governance structure
- Risk assessment methodology aligned with ISO 27001 standards
- Formal risk management strategy with quarterly reviews

2. **Protect (PR)**: Tier 4 - Adaptive
- Identity management and access control using zero-trust architecture
- Multi-factor authentication implemented across all systems
- Regular security awareness training for all personnel
- Data security protocols exceeding industry standards

3. **Detect (DE)**: Tier 4 - Adaptive
- Continuous monitoring of all industrial control systems
- Advanced anomaly detection using proprietary AI algorithms
- Security continuous monitoring capabilities

- Detection processes validated through regular penetration testing

4. **Respond (RS)**: Tier 3 - Repeatable
- Documented incident response procedures
- Communications protocols established with relevant stakeholders
- Analysis procedures for incident assessment
- Mitigation strategies and continuous improvement processes

5. **Recover (RC)**: Tier 3 - Repeatable
- Recovery planning procedures documented and tested
- Regular backup and restoration testing
- Reputation management procedures established
- Lessons learned integration process

3. DETAILED CONTROL ASSESSMENT

1. **Critical Infrastructure Controls**
- Implementation of NERC CIP standards where applicable
- Integration with ISA/IEC 62443 framework requirements
- Maritime-specific controls aligned with IMO guidelines
- Subsea infrastructure protection protocols

2. **Technology Stack Assessment**
- Proprietary deep-layer security architecture evaluation
- AI-driven threat detection system validation
- SCADA network protection mechanisms
- OT network segmentation verification

4. GAP ANALYSIS AND REMEDIATION

1. **Identified Gaps**
- Incident response automation requires enhancement
- Recovery time objectives need optimization
- Supply chain risk management requires strengthening

- Third-party vendor assessment program needs expansion

2. **Remediation Timeline**

- Q1 2024: Implement enhanced incident response automation
- Q2 2024: Optimize recovery procedures and testing
- Q3 2024: Enhance supply chain risk management program
- Q4 2024: Deploy comprehensive vendor assessment platform

5. COMPLIANCE ATTESTATION

The undersigned hereby certifies that this assessment accurately reflects DeepShield Systems' current NIST CSF implementation status as of the assessment date.

6. LEGAL DISCLAIMERS

1. This assessment is provided for internal evaluation purposes only and does not constitute a guarantee of security effectiveness or regulatory compliance.

2. The information contained herein is confidential and proprietary to DeepShield Systems, Inc. and may not be disclosed without written authorization.

3. This assessment represents a point-in-time evaluation and should be reviewed and updated periodically to maintain accuracy.

7. SIGNATURES

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024

By:

Name: Sarah Blackwood

Title: Chief Technology Officer

Date: January 11, 2024

VERIFIED BY:

By:

Name: Michael Thompson

Title: Lead Assessor, SecureStack Advisory Group

Date: January 11, 2024

8. APPENDICES

1. Assessment Methodology

2. Control Testing Results

3. Supporting Documentation Index

4. Risk Assessment Matrix

5. Compliance Evidence Repository

[End of Document]