CRITICAL INFRASTRUCTURE PROTECTION PLAN

FISCAL YEAR 2023

DeepShield Systems, Inc.

Document No. CIP-2023-001

Effective Date: January 1, 2023

1. INTRODUCTION

1 This Critical Infrastructure Protection Plan ("Plan") is established by DeepShield Systems, Inc. ("Company") to define and implement comprehensive security measures for the protection of critical infrastructure assets and operational technology environments under the Company's purview.

2 This Plan is developed in accordance with NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1, ISA/IEC 62443 standards, and applicable federal regulations governing critical infrastructure protection.

2. SCOPE AND APPLICABILITY

1 This Plan applies to all Company operations, including:

a) Industrial Control System (ICS) security solutions

b) SCADA network protection systems

c) Maritime and subsea infrastructure security platforms

d) Manufacturing operations security protocols

e) AI-driven threat detection systems

2 Geographic Coverage: All Company facilities and client installations within North America, with specific provisions for offshore and maritime deployments.

3. DEFINITIONS

1 "Critical Infrastructure" means systems and assets, whether physical or virtual, so vital that their incapacity or destruction would have a debilitating impact on security, economic security, or public health or safety.

2 "OT Environment" means the hardware and software systems that monitor or control physical devices, processes, and events in industrial and critical infrastructure environments.

3 "Security Incident" means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

4. PROTECTION MEASURES

1 Network Security

a) Implementation of DeepShield's proprietary deep-layer security architecture

b) Continuous monitoring of OT network traffic

c) Real-time threat detection and response

d) Segmentation of critical systems from enterprise networks

e) Encrypted communications for all remote access

2 Physical Security

a) Multi-factor authentication for facility access

b) 24/7 surveillance of critical infrastructure sites

c) Biometric access controls for high-security areas

d) Environmental monitoring systems

e) Redundant power systems with UPS backup

3 Cybersecurity Controls

a) AI-powered anomaly detection

b) Automated incident response protocols

c) Regular vulnerability assessments

d) Patch management procedures

e) Supply chain security verification

5. INCIDENT RESPONSE

1 Response Team Structure

- Primary Incident Commander: Chief Security Architect
- Technical Lead: VP of Engineering
- Communications Lead: Chief Technology Officer
- Legal/Compliance: General Counsel

2 Response Procedures

a) Initial incident assessment within 15 minutes

b) Stakeholder notification within 1 hour

c) Containment measures implemented within 2 hours

d) Recovery procedures initiated within 4 hours

e) Post-incident analysis within 24 hours

6. COMPLIANCE AND REPORTING

1 Regulatory Compliance

- NERC CIP Standards
- Maritime Transportation Security Act requirements
- Department of Homeland Security guidelines
- State-specific critical infrastructure regulations

2 Reporting Requirements

a) Monthly security metrics to executive leadership

b) Quarterly compliance reports to Board of Directors

c) Annual security assessment to regulatory authorities

d) Immediate notification of critical incidents to relevant agencies

7. TRAINING AND AWARENESS

1 Required Training Programs

- New hire security orientation
- Annual security awareness training
- Quarterly incident response drills
- Role-specific technical training

2 Documentation Requirements

- Training completion records
- Drill participation logs
- Certification maintenance records

8. PLAN MAINTENANCE

1 Review Schedule

- Annual comprehensive review
- Quarterly updates as needed
- Post-incident revision assessment

2 Version Control

- Document control number: CIP-2023-001
- Last revision date: December 15, 2022
- Next scheduled review: December 1, 2023

9. AUTHORIZATION

This Critical Infrastructure Protection Plan is hereby approved and adopted:

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Marcus Chen

Chief Executive Officer

Date: December 15, 2022

By:

Dr. Elena Rodriguez

Chief Security Architect

Date: December 15, 2022

10. CONFIDENTIALITY NOTICE

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, reproduction, or distribution is strictly prohibited and may result in civil and criminal penalties.