# CRITICAL INFRASTRUCTURE PROTECTION PLAN 2024

**DeepShield Systems, Inc.**

*Effective Date: January 1, 2024*

## 1. INTRODUCTION AND PURPOSE

1. This Critical Infrastructure Protection Plan ("Plan") establishes the comprehensive framework for protecting critical infrastructure assets, operational technology environments, and industrial control systems under the management or protection of DeepShield Systems, Inc. ("DeepShield" or the "Company").

2. This Plan is designed to comply with relevant regulatory requirements including but not limited to NERC CIP Standards, NIST Framework for Critical Infrastructure Cybersecurity, and Maritime Transportation Security Act (MTSA) requirements.

## 2. SCOPE AND APPLICABILITY

1. This Plan applies to all critical infrastructure protection activities conducted by DeepShield, including:

a) Industrial Control System (ICS) security operations

b) SCADA network protection services

c) Maritime and subsea infrastructure security

d) Manufacturing operations security

e) Operational Technology (OT) environment protection

2. All DeepShield employees, contractors, and authorized third parties must comply with this Plan when accessing or managing protected infrastructure components.

## 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, public health or safety, or any combination thereof.

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

3. "Deep-Layer Security Architecture" means DeepShield's proprietary security framework incorporating AI-driven threat detection, real-time monitoring, and adaptive defense mechanisms.

## 4. PROTECTION STRATEGIES AND PROTOCOLS

1. Risk Assessment and Classification

a) Quarterly vulnerability assessments of protected infrastructure

b) Asset classification based on criticality matrix

c) Threat modeling specific to industrial environments

d) Impact analysis for potential security breaches

2. Technical Security Controls

a) Implementation of Deep-Layer Security Architecture

b) Network segmentation and access control

c) Encrypted communications protocols

d) Real-time threat monitoring and response

e) Automated incident detection and containment

3. Physical Security Measures

a) Multi-factor authentication for facility access

b) Video surveillance of critical areas

c) Environmental monitoring systems

d) Backup power systems

e) Redundant communication channels

## 5. INCIDENT RESPONSE AND RECOVERY

1. Incident Classification

a) Level 1 - Minor disruption

b) Level 2 - Significant system impact

c) Level 3 - Critical infrastructure compromise

d) Level 4 - Catastrophic failure

2. Response Procedures

a) Initial incident assessment

b) Containment strategies

c) Evidence preservation

d) System restoration

e) Post-incident analysis

3. Business Continuity

a) Backup system activation

b) Alternative processing facilities

c) Emergency communication procedures

d) Stakeholder notification protocols

## 6. COMPLIANCE AND AUDIT

1. Regular compliance assessments against:

a) NERC CIP Standards

b) ISO 27001 requirements

c) Industry-specific regulations

d) Client contractual obligations

2. Audit Schedule

a) Monthly internal security audits

b) Quarterly compliance reviews

c) Annual third-party assessments

d) Continuous monitoring reports

## 7. TRAINING AND AWARENESS

1. Required Training Programs

a) Initial security awareness training

b) Annual refresher courses

c) Role-specific technical training

d) Incident response drills

2. Documentation Requirements

a) Training completion records

b) Certification maintenance

c) Drill participation logs

d) Competency assessments

## 8. PLAN MAINTENANCE AND UPDATES

1. This Plan shall be reviewed and updated:

a) Annually at minimum

b) Following major security incidents

c) Upon significant technology changes

d) As required by regulatory updates

2. All updates must be approved by:

a) Chief Security Architect

b) VP of Engineering

c) Chief Technology Officer

d) Chief Executive Officer

## 9. AUTHORIZATION

This Critical Infrastructure Protection Plan is hereby authorized and approved:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 1, 2024