NERC-CIP Standards Implementation Framework

Version 3.2

Effective Date: January 15, 2024

Document ID: DSS-NERC-CIP-FW-3.2

1. Purpose and Scope

1. This Framework document ("Framework") establishes DeepShield Systems, Inc.'s ("DeepShield") comprehensive approach to implementing North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC-CIP") Standards within its Industrial Control System (ICS) security solutions and related services.

2. This Framework applies to all DeepShield products, services, and internal operations that interface with or support Bulk Electric System (BES) Cyber Systems or their associated Electronic Security Perimeters (ESPs).

2. Definitions

1. "BES Cyber Assets" means Cyber Assets that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, affect the reliable operation of the Bulk Electric System.

2. "Critical Infrastructure Protection Standards" or "CIP Standards" refers to NERC-CIP Standards CIP-002 through CIP-014, as amended and in effect.

3. "Deep-Layer Security Architecture" means DeepShield's proprietary security framework incorporating AI-driven threat detection and response capabilities.

3. NERC-CIP Compliance Integration

1. System Architecture Alignment

a) DeepShield's Deep-Layer Security Architecture shall maintain strict alignment with NERC-CIP requirements through modular security controls.

b) All system components shall support categorization of BES Cyber Systems per CIP-002-5.1a.

c) Implementation of security management controls shall comply with CIP-003-8.

2. Access Control and Identity Management

a) Role-based access control (RBAC) implementation per CIP-004-6

b) Multi-factor authentication integration

c) Automated access revocation procedures

d) Personnel risk assessment procedures

3. Electronic Security Perimeter Protection

a) ESP identification and protection mechanisms per CIP-005-7

b) Interactive Remote Access management

c) Encryption requirements for data in transit

d) Network segmentation validation

4. Security Controls Implementation

1. Physical Security

a) Facility security plans aligned with CIP-006-6

b) Physical access control systems

c) Visitor management procedures

d) Logging and monitoring requirements

2. Systems Security Management

a) Security patch management per CIP-007-6

b) Malicious code prevention

c) Security event monitoring

d) System access control

e) Password requirements and management

3. Incident Response and Recovery

a) Incident response procedures per CIP-008-6

b) Recovery plan requirements per CIP-009-6

c) Testing and documentation requirements

d) Post-incident analysis procedures

5. Configuration Change Management

1. All changes to DeepShield systems affecting BES Cyber Systems shall follow:

a) Configuration change management procedures per CIP-010-4

b) Vulnerability assessment requirements

c) Development and testing environment controls

d) Baseline configuration management

6. Information Protection

1. DeepShield shall implement and maintain:

a) Information protection procedures per CIP-011-3

b) Data classification schemes

c) Information handling procedures

d) Media sanitization requirements

7. Supply Chain Risk Management

1. Supply chain security controls shall include:

a) Vendor risk assessment procedures per CIP-013-2

b) Software integrity verification

c) Vendor remote access management

d) Procurement controls

8. Compliance Monitoring and Assessment

1. DeepShield shall maintain:

a) Continuous compliance monitoring procedures

b) Regular self-assessment protocols

c) Documentation of compliance evidence

d) Audit preparation procedures

9. Framework Maintenance

1. This Framework shall be:

a) Reviewed annually

b) Updated upon material changes to NERC-CIP Standards

c) Approved by DeepShield's Chief Security Architect

d) Version controlled and documented

10. Legal Disclaimer

This Framework is proprietary to DeepShield Systems, Inc. and contains confidential information. Unauthorized disclosure, reproduction, or distribution is prohibited. While DeepShield strives to maintain compliance with NERC-CIP Standards, this Framework does not guarantee compliance and should not be construed as legal advice.

Approval and Version Control

Document Owner: Dr. Elena Rodriguez, Chief Security Architect

Approved By: Dr. Marcus Chen, CEO

Version: 3.2

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

[SIGNATURE PAGE FOLLOWS]