NERC CIP Standards Implementation Guide

Version 4.2

DeepShield Systems, Inc.

Effective Date: January 15, 2024

1. Purpose and Scope

1. This Implementation Guide ("Guide") establishes the procedures and requirements for DeepShield Systems, Inc.'s ("DeepShield") compliance with North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC CIP") Standards in relation to its Industrial Control System (ICS) security solutions and services.

2. This Guide applies to all DeepShield products, services, and 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 Cyber Assets" refers to BES Cyber Assets that execute or enable one or more reliability tasks.

3. "Electronic Security Perimeter" means the logical border surrounding a network where Critical Cyber Assets reside.

3. NERC CIP Standards Compliance Framework

1. Security Management Controls (CIP-003)

- Implementation of comprehensive security policies
- Assignment of senior management responsibility
- Exceptions management procedures
- Information protection protocols

2. Personnel & Training (CIP-004)

- Personnel risk assessment program
- Security awareness training requirements
- Access management and revocation procedures
- Quarterly access reviews

3. Electronic Security Perimeters (CIP-005)

- ESP identification and documentation
- Access point protection
- Remote access management
- Encryption requirements for external connectivity

4. Product Implementation Requirements

1. DeepShield's Industrial Cybersecurity Platform shall:

- Maintain continuous monitoring of all ESP access points
- Implement multi-factor authentication for all interactive remote access
- Log all access attempts and security events
- Provide automated alerts for potential security violations

2. Maritime and Subsea Infrastructure Modules shall:

- Comply with CIP-007 System Security Management requirements
- Implement port and services hardening
- Maintain security patch management capabilities
- Provide malicious code prevention mechanisms

5. Compliance Monitoring and Testing

1. Periodic Assessments

- Quarterly internal compliance reviews
- Annual third-party compliance audits
- Vulnerability assessments every 6 months
- Penetration testing on an annual basis

2. Documentation Requirements

- Maintenance of all required compliance evidence
- Version control of all security configurations
- Change management documentation
- Incident response records

6. Incident Response and Recovery

1. Security Incident Response Plan

- Identification of reportable cyber security incidents
- Required notification procedures
- Incident handling procedures
- Post-incident analysis requirements

2. Recovery Plans

- System restoration procedures
- Backup and restore requirements
- Testing of recovery plans
- Documentation of recovery activities

7. Compliance Verification

1. DeepShield shall maintain:

- Current documentation of all applicable NERC CIP requirements
- Evidence of compliance with each applicable requirement
- Records of all testing and assessments
- Training records for all applicable personnel

2. Annual Review Process

- Review of all policies and procedures
- Update of implementation documentation
- Validation of technical controls
- Assessment of compliance gaps

8. Disclaimer and Limitations

1. This Guide is intended for internal use only and does not constitute legal advice.

2. Compliance with this Guide does not guarantee compliance with all NERC CIP requirements.

3. DeepShield reserves the right to modify this Guide as necessary to maintain alignment with NERC CIP Standards updates.

9. Document Control

Document Owner: Chief Security Architect

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

Version: 4.2

Approval

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024