CISA Cybersecurity Performance Goals Report

DeepShield Systems, Inc.

Reporting Period: Q4 2023

Date: January 11, 2024

1. Executive Summary

This report documents DeepShield Systems, Inc.'s ("DeepShield") compliance with the Cybersecurity and Infrastructure Security Agency's ("CISA") Cross-Sector Cybersecurity Performance Goals ("CPGs"). The assessment evaluates DeepShield's industrial control system (ICS) security platform and operational technology (OT) protection services against CISA's baseline security measures for critical infrastructure operators.

2. Scope of Assessment

1. Systems Evaluated

- DeepShield ICS Protection Platform v4.2
- Maritime Security Module v2.1
- Subsea Infrastructure Protection Suite v3.0
- OT Network Monitoring System v4.5
- Incident Response Automation Framework v2.3

2. Facilities Assessed

- Primary Operations Center (Delaware)
- Backup Data Center (Virginia)
- Research & Development Facility (California)
- Customer Support Operations (Texas)

3. CPG Compliance Status

1. Account Security

- Multi-factor authentication (MFA) implemented across all systems
- Privileged access management (PAM) protocols established
- Regular access reviews conducted quarterly

- Password policies conform to NIST 800-63B guidelines
- Compliance Status: FULLY COMPLIANT

2. Device Security

- Endpoint detection and response (EDR) deployed
- Asset inventory management system maintained
- Automated patch management system operational
- Hardware security modules (HSM) implemented
- Compliance Status: FULLY COMPLIANT

3. Data Protection

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Regular backup verification procedures
- Secure offline backup storage maintained
- Compliance Status: FULLY COMPLIANT

4. Technical Controls Implementation

1. Network Segmentation

- Implementation of zero-trust architecture
- OT/IT network separation maintained
- DMZ configurations validated
- Network access control lists (ACLs) implemented
- Microsegmentation deployed for critical assets

2. Monitoring and Detection

- 24/7 Security Operations Center (SOC)
- AI-driven threat detection systems
- SIEM integration with threat intelligence feeds
- OT-specific anomaly detection
- Real-time alert correlation system

5. Incident Response Capabilities

1. Response Procedures

- Documented incident response plan
- Regular tabletop exercises conducted
- Integration with customer emergency procedures
- Automated containment protocols
- Incident classification framework established

2. Recovery Protocols

- Business continuity procedures tested
- Disaster recovery capabilities verified
- System restoration priorities defined
- Recovery time objectives (RTOs) met
- Regular failover testing conducted

6. Risk Assessment Findings

1. Identified Risks

- Supply chain dependency on third-party components
- Legacy system integration challenges
- Maritime communication protocol vulnerabilities
- Cross-border data transfer compliance

2. Mitigation Strategies

- Vendor security assessment program
- Legacy system isolation protocols
- Enhanced maritime encryption standards
- Data sovereignty compliance framework

7. Continuous Improvement Initiatives

1. Planned Enhancements

- AI model retraining program
- Threat hunting capability expansion
- Additional OT protocol support

- Enhanced maritime asset protection

2. Training and Awareness

- Security awareness training program
- Technical certification requirements
- Regular skill assessment
- Compliance training tracking

8. Certification and Attestation

The undersigned hereby certifies that this report accurately reflects DeepShield Systems, Inc.'s implementation of CISA Cybersecurity Performance Goals as of the date of this report.

This assessment was conducted in accordance with CISA guidelines and industry best practices. All findings represent the current state of cybersecurity controls and capabilities as implemented within DeepShield's systems and operations.

```

EXECUTED this 11th day of January, 2024

**By: _**

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

**By: _**

James Morrison

VP of Engineering

DeepShield Systems, Inc.

```

9. Legal Disclaimer

This report is confidential and proprietary to DeepShield Systems, Inc. The information contained herein is provided for compliance and due diligence purposes only. While reasonable efforts have been made to ensure accuracy, DeepShield makes no warranties or representations regarding the

completeness or accuracy of the information presented. This report shall not be reproduced or distributed without the express written consent of DeepShield Systems, Inc.