Security Controls Implementation Evidence

DeepShield Systems, Inc.

Document Reference: SEC-CTRL-2023-12

Last Updated: December 15, 2023

1. Purpose and Scope

This document provides evidence of security control implementations across DeepShield Systems, Inc.'s ("Company") industrial cybersecurity platform and operational infrastructure. This documentation serves as verification of compliance with industry standards and regulatory requirements applicable to critical infrastructure protection solutions.

2. Control Framework Alignment

1. The Company maintains alignment with the following control frameworks:

- NIST Cybersecurity Framework (CSF) v1.1
- IEC 62443 Industrial Automation and Control Systems Security
- ISO/IEC 27001:2013 Information Security Management
- Maritime cybersecurity requirements (BIMCO Guidelines)

2. Implementation verification is maintained through:

- Quarterly internal audits
- Annual third-party assessments
- Continuous monitoring and logging
- Regular penetration testing

3. Technical Control Implementation

1. Network Segmentation

- Implementation of air-gapped development environments
- Strict separation between IT and OT networks
- Microsegmentation of critical system components
- Dedicated secure zones for maritime control systems

2. Access Control Mechanisms

- Multi-factor authentication (MFA) for all privileged access
- Role-based access control (RBAC) with principle of least privilege
- Biometric verification for physical access to secure areas
- Automated access review and certification processes

3. Encryption and Key Management

- AES-256 encryption for data at rest
- TLS 1.3 for all data in transit
- Hardware security modules (HSMs) for key storage
- Automated key rotation every 90 days

4. Operational Controls

1. Change Management

- Documented change control procedures
- Pre-implementation security impact analysis
- Automated configuration management
- Version control for all security-relevant code

2. Incident Response

- 24/7 Security Operations Center (SOC)
- Automated threat detection and response
- Incident classification matrix
- Documented escalation procedures

3. Business Continuity

- Redundant data centers (US East, US West, EU)
- Real-time data replication
- Monthly failover testing
- Recovery time objective (RTO) of 4 hours

5. Evidence Collection and Retention

1. System Logs

- Centralized log management system
- Minimum 12-month retention period
- Tamper-evident logging mechanisms
- Automated log analysis and alerting

2. Audit Records

- Quarterly control effectiveness reviews
- Annual penetration test reports
- Monthly vulnerability assessment results
- Third-party audit findings and remediation tracking

6. Compliance Monitoring

1. Continuous Compliance Monitoring

- Automated compliance scanning
- Real-time policy violation alerts
- Compliance dashboard monitoring
- Regular compliance gap assessments

2. Regulatory Reporting

- Monthly compliance status reports
- Quarterly board updates
- Annual regulatory submissions
- Incident notification procedures

7. Certification and Attestation

The undersigned hereby certifies that the security controls described herein are accurately implemented and maintained as of the date of this document.

8. Legal Disclaimers

1. This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, reproduction, or distribution is strictly prohibited.

2. While the Company maintains reasonable security measures, no security controls can guarantee

absolute protection against all threats.

3. This document does not constitute a warranty or guarantee of security effectiveness.

9. Execution

IN WITNESS WHEREOF, this Security Controls Implementation Evidence document has been executed by the duly authorized representatives of the Company.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: December 15, 2023

By:

Name: Sarah Blackwood

Title: Chief Technology Officer

Date: December 15, 2023

10. Document Control

Version: 3.2

Last Review Date: December 15, 2023

Next Review Date: March 15, 2024

Document Owner: Security Architecture Team

Classification: Confidential