

ABS CYBERSECURITY NOTATION DOCUMENTATION

DeepShield Systems, Inc.

Document Reference: DSS-ABS-2024-001

Effective Date: January 15, 2024

1. PURPOSE AND SCOPE

1. This document establishes the requirements and procedures for maintaining the American Bureau of Shipping (ABS) Cybersecurity Notation for DeepShield Systems, Inc.'s ("DeepShield") maritime and offshore cybersecurity solutions, specifically relating to the DeepShield Maritime Defense Platform(TM) v4.2 and associated subsystems.

2. The notation requirements herein apply to all DeepShield cybersecurity implementations designated for maritime vessels, offshore facilities, and subsea infrastructure operating under ABS classification.

2. DEFINITIONS

1. "ABS CS1" means the first-level ABS Cybersecurity Notation indicating compliance with ABS Guide for Cybersecurity Implementation for Marine and Offshore Operations.

2. "Critical Systems" refers to operational technology (OT) systems essential for vessel/facility operations, safety systems, and environmental protection systems.

3. "Security Architecture" means DeepShield's proprietary deep-layer security framework as documented in Technical Specification DSS-TS-2023-142.

3. COMPLIANCE REQUIREMENTS

1. System Architecture Documentation

- a) Maintain current documentation of system architecture diagrams
- b) Update network topology maps quarterly
- c) Document all integration points with vessel/facility systems
- d) Maintain current inventory of protected assets

2. Risk Assessment Protocols

- a) Conduct quarterly risk assessments of protected systems
- b) Document threat modeling for new attack vectors
- c) Maintain vulnerability management program
- d) Update risk matrices following system modifications

3. Security Controls Implementation

- a) Implement ABS-approved access control mechanisms
- b) Maintain network segmentation per ABS CS1 requirements
- c) Deploy approved encryption protocols for all data transmission
- d) Implement continuous monitoring and logging capabilities

4. TESTING AND VERIFICATION

1. Testing Requirements

- a) Annual penetration testing by ABS-certified assessors
- b) Quarterly security control effectiveness testing
- c) Monthly automated vulnerability scanning
- d) Continuous monitoring system verification

2. Documentation Requirements

- a) Maintain test results for 36 months
- b) Document all remediation actions
- c) Track security incidents and resolution measures
- d) Maintain compliance audit trail

5. INCIDENT RESPONSE AND RECOVERY

1. Incident Response Procedures

- a) Maintain ABS-compliant incident response plan
- b) Document incident classification criteria
- c) Establish notification protocols
- d) Define escalation procedures

2. Recovery Requirements

- a) Maintain system recovery procedures
- b) Document backup and restoration processes
- c) Establish business continuity protocols
- d) Define system resilience measures

6. MAINTENANCE AND UPDATES

1. System Maintenance

- a) Schedule regular maintenance windows
- b) Document all system changes
- c) Maintain patch management program
- d) Track configuration changes

2. Documentation Updates

- a) Review documentation quarterly
- b) Update procedures as required
- c) Maintain version control
- d) Archive superseded documents

7. REPORTING AND NOTIFICATIONS

1. Regular Reporting

- a) Submit quarterly compliance reports to ABS
- b) Provide monthly security metrics
- c) Document system performance indicators
- d) Report on security incidents

2. Notification Requirements

- a) Report significant security events within 24 hours
- b) Notify ABS of system modifications
- c) Submit annual compliance certification
- d) Report changes in critical personnel

8. CERTIFICATION AND AUDIT

1. The DeepShield Maritime Defense Platform(TM) shall maintain continuous compliance with ABS CS1 requirements through:

- a) Annual third-party audits
- b) Quarterly internal assessments
- c) Monthly compliance reviews
- d) Continuous monitoring reports

9. DISCLAIMER AND LIMITATIONS

- 1. This documentation is confidential and proprietary to DeepShield Systems, Inc.
- 2. Nothing in this document shall be construed to modify or supersede any requirements established by ABS or applicable regulatory authorities.

EXECUTION

IN WITNESS WHEREOF, this documentation has been executed by the duly authorized representative of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024

Witness:

Name: James Morrison

Title: VP of Engineering

Date: January 15, 2024