CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) DOCUMENTATION

Document ID: CMMC-2024-DSI-001

Effective Date: January 11, 2024

Version: 2.0

Classification: CONFIDENTIAL

Entity: DeepShield Systems, Inc.

1. CERTIFICATION OVERVIEW

1. DeepShield Systems, Inc. ("Company"), a Delaware corporation with principal offices at 2500 Cyber Drive, Suite 400, Boston, MA 02110, hereby documents its compliance with the Cybersecurity Maturity Model Certification (CMMC) Level 3 requirements as established by the U.S. Department of Defense (DoD).

2. This documentation serves as evidence of the Company's implementation of specified security practices and processes in accordance with CMMC Assessment Guide v2.0 and National Institute of Standards and Technology (NIST) Special Publication 800-171.

2. SCOPE OF CERTIFICATION

1. The certification encompasses all Company facilities, systems, and processes involved in:

a) Development and deployment of the DeepShield ICS Security Platform

b) Maritime and subsea infrastructure protection systems

c) OT network monitoring and response capabilities

d) AI-driven threat detection systems

e) SCADA security implementations

2. Certification Coverage Period: January 1, 2024 - December 31, 2026

3. COMPLIANCE FRAMEWORK

1. The Company maintains compliance with the following CMMC domains:

1.1. Access Control (AC)

1.2. Asset Management (AM)

1.3. Audit and Accountability (AU)

1.4. Awareness and Training (AT)

1.5. Configuration Management (CM)

1.6. Identification and Authentication (IA)

1.7. Incident Response (IR)

1.8. Maintenance (MA)

1.9. Media Protection (MP)

1.10. Personnel Security (PS)

1.11. Physical Protection (PE)

1.12. Recovery (RE)

1.13. Risk Management (RM)

1.14. Security Assessment (CA)

1.15. Situational Awareness (SA)

1.16. System and Communications Protection (SC)

1.17. System and Information Integrity (SI)

4. IMPLEMENTATION DETAILS

1. Security Operations Center (SOC)

- 24/7 monitoring facility located at Boston headquarters
- Redundant backup facility in Austin, TX
- Staffing: 12 certified security analysts
- Implementation of SIEM platform version 4.2.1

2. Access Control Implementation

- Zero Trust Architecture framework
- Multi-factor authentication for all system access
- Privileged Access Management (PAM) system
- Regular access reviews and attestation

3. Data Protection Measures

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Hardware Security Modules (HSM) for key management
- Secure enclaves for sensitive processing

5. ASSESSMENT AND CERTIFICATION

1. Third-Party Assessment

- Assessor: CyberCert Solutions, LLC
- Assessment Date: December 1-15, 2023
- Assessment Number: CMMC-2023-456789
- Certification Level Achieved: Level 3

2. Gap Analysis and Remediation

- All identified gaps addressed per Remediation Plan DSI-2023-12
- Verification testing completed December 20, 2023
- Final certification awarded January 5, 2024

6. MAINTENANCE AND MONITORING

1. Continuous Monitoring Program

- Weekly security metrics review
- Monthly compliance dashboard updates
- Quarterly internal audits
- Annual third-party assessment

2. Documentation Management

- All CMMC documentation maintained in GRC platform
- Version control through Document Management System
- Annual review and update cycle
- Change management procedures per SOP-2023-089

7. CERTIFICATION AUTHORITY

This documentation is certified as accurate and complete by:

/s/ Dr. Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

/s/ James Morrison

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024

8. LEGAL DISCLAIMER

This documentation contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, reproduction, or distribution is strictly prohibited. The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing. DeepShield Systems, Inc. and its affiliates shall not be liable for any damages suffered as a result of using, modifying, contributing, copying, or distributing this information.