SECURITY COMPLIANCE AUDIT SCHEDULE

FISCAL YEAR 2024

DeepShield Systems, Inc.

1. PURPOSE AND SCOPE

1 This Security Compliance Audit Schedule ("Schedule") establishes the mandatory security compliance audit framework for DeepShield Systems, Inc. ("Company") for Fiscal Year 2024, pursuant to the Company's Master Security and Compliance Program.

2 This Schedule covers all operational divisions, subsidiaries, and controlled affiliates of the Company, including but not limited to:

(a) Core ICS security operations

(b) Maritime security division

(c) Critical infrastructure protection unit

(d) Research & development facilities

(e) Cloud operations infrastructure

2. AUDIT CATEGORIES AND FREQUENCY

1 **Tier 1 - Critical Systems Audits**

- Frequency: Quarterly
- Scope: Industrial Control System (ICS) security architecture
- Coverage: Deep-layer security protocols, SCADA integration points
- Duration: 5-7 business days per audit
- Q1: March 4-10, 2024
- Q2: June 3-9, 2024
- Q3: September 2-8, 2024
- Q4: December 2-8, 2024

2 **Tier 2 - Operational Technology Audits**

- Frequency: Semi-annual
- Scope: OT network infrastructure, maritime systems

- Coverage: Subsea protection systems, automated response mechanisms
- Duration: 10 business days per audit
- H1: April 15-26, 2024
- H2: October 14-25, 2024

3 **Tier 3 - Compliance Framework Audits**

- Frequency: Annual
- Scope: Regulatory compliance, certification maintenance
- Coverage: ISO 27001, IEC 62443, NIST frameworks
- Duration: 15 business days
- Annual: July 8-26, 2024

3. AUDIT REQUIREMENTS

1 **Documentation Requirements**

The Company shall maintain and make available:

(a) System architecture diagrams

(b) Security control inventories

(c) Incident response procedures

(d) Change management logs

(e) Access control matrices

(f) Threat modeling documentation

(g) Risk assessment reports

(h) Penetration testing results

2 **Personnel Availability**

The following personnel must be available during scheduled audits:

- Chief Security Architect
- VP of Engineering
- Security Operations Manager
- Compliance Officer
- Technical Lead(s) for affected systems

3 **Testing Environment**

Dedicated test environments must be maintained for:

(a) ICS security validation

(b) Maritime systems testing

(c) SCADA integration verification

(d) Threat detection simulation

4. AUDIT METHODOLOGY

1 **Pre-Audit Phase**

- Documentation review: 5 business days
- Scope confirmation: 3 business days
- Resource allocation: 2 business days
- Environment preparation: 5 business days

2 **Active Audit Phase**

- Control testing: Per schedule in Section 2
- Vulnerability assessment
- Configuration review
- Process validation
- Compliance verification

3 **Post-Audit Phase**

- Findings documentation: 5 business days
- Management review: 3 business days
- Remediation planning: 5 business days
- Final report issuance: 10 business days

5. COMPLIANCE STANDARDS

1 All audits shall assess compliance with:

- ISO/IEC 27001:2022
- IEC 62443 series
- NIST SP 800-82 Rev. 2

- Maritime cybersecurity guidelines (BIMCO)
- Company security policies and procedures

2 **Minimum Testing Requirements**

(a) Penetration testing of critical systems

(b) Configuration compliance verification

(c) Access control validation

(d) Incident response capability assessment

(e) Business continuity validation

6. REPORTING AND REMEDIATION

1 **Audit Reports**

Each audit shall produce:

(a) Executive summary

(b) Detailed findings report

(c) Risk assessment matrix

(d) Compliance status dashboard

(e) Remediation recommendations

2 **Remediation Timelines**

- Critical findings: 24 hours
- High-risk findings: 5 business days
- Medium-risk findings: 15 business days
- Low-risk findings: 30 business days

3 **Follow-up Validation**

- Critical/High: Mandatory retest
- Medium: Documentation review
- Low: Next scheduled audit

7. CONFIDENTIALITY

1 All audit activities, findings, and reports are classified as Confidential Information under the Company's Information Classification Policy.

2 Distribution of audit materials is restricted to:

(a) Board of Directors

(b) Executive Management

(c) Security Leadership Team

(d) Compliance Team

(e) External auditors (as required)

8. AMENDMENTS AND UPDATES

1 This Schedule may be amended by written approval of:

- Chief Security Architect
- VP of Engineering
- Compliance Officer

2 Material changes require Board notification within 5 business days.

9. AUTHORIZATION

This Security Compliance Audit Schedule is hereby adopted and approved:

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024

By:

Name: James Morrison

Title: VP of Engineering

Date: January 15, 2024

By:

Name: Robert Kessler

Title: Chief Financial Officer

Date: January 15, 2024