SECURITY COMPLIANCE AUDIT CHECKLIST

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document Reference: DSS-SEC-2024-001

1. PURPOSE AND SCOPE

1. This Security Compliance Audit Checklist ("Checklist") establishes the comprehensive framework for evaluating and documenting DeepShield Systems, Inc.'s ("Company") compliance with applicable security standards, regulations, and internal policies governing its industrial cybersecurity operations and critical infrastructure protection services.

2. This Checklist applies to all Company facilities, systems, personnel, and operations involved in the development, deployment, and maintenance of industrial control system (ICS) security solutions.

2. REGULATORY COMPLIANCE VERIFICATION

1. **Federal Regulations**

- [ ] NIST Cybersecurity Framework compliance
- [ ] CFIUS requirements for critical technology companies
- [ ] Department of Homeland Security CISA guidelines
- [ ] Federal Energy Regulatory Commission (FERC) standards
- [ ] Maritime Transportation Security Act requirements

2. **Industry Standards**

- [ ] ISO/IEC 27001:2013 Information Security Management
- [ ] ISA/IEC 62443 Industrial Automation and Control Systems
- [ ] NERC CIP Standards for critical infrastructure
- [ ] API 1164 Pipeline SCADA Security
- [ ] DNV-RP-G108 Cyber Security requirements

3. OPERATIONAL SECURITY CONTROLS

1. **Access Control and Authentication**

- [ ] Multi-factor authentication implementation

- [ ] Privileged access management systems
- [ ] Role-based access control (RBAC) matrix
- [ ] Physical access control systems
- [ ] Biometric authentication protocols

2. **Network Security**
- [ ] Network segmentation verification
- [ ] Firewall rule set review
- [ ] IDS/IPS deployment validation
- [ ] DMZ configuration audit
- [ ] VPN infrastructure assessment

3. **Data Protection**
- [ ] Encryption standards compliance
- [ ] Data classification protocols
- [ ] Backup systems verification
- [ ] Data retention policy compliance
- [ ] Secure data destruction procedures

4. INDUSTRIAL CONTROL SYSTEM SECURITY

1. **OT Environment Protection**
- [ ] Air-gap verification procedures
- [ ] SCADA system security controls
- [ ] PLC/RTU security configurations
- [ ] Industrial protocol security
- [ ] Safety system isolation

2. **Maritime Infrastructure Security**
- [ ] Subsea control system protection
- [ ] Vessel cybersecurity measures
- [ ] Port facility security controls
- [ ] Maritime SCADA systems

- [ ] Navigation system security

5. INCIDENT RESPONSE AND RECOVERY

1. **Incident Management**

- [ ] Incident response plan review
- [ ] Emergency communication procedures
- [ ] Escalation protocols
- [ ] Forensic investigation capabilities
- [ ] Incident documentation systems

2. **Business Continuity**

- [ ] Disaster recovery procedures
- [ ] Backup site readiness
- [ ] Critical system redundancy
- [ ] Recovery time objectives
- [ ] Business impact analysis

6. SECURITY TESTING AND VALIDATION

1. **Penetration Testing**

- [ ] External penetration testing
- [ ] Internal network assessment
- [ ] Web application security testing
- [ ] Social engineering evaluations
- [ ] Physical security testing

2. **Vulnerability Management**

- [ ] Vulnerability scanning procedures
- [ ] Patch management systems
- [ ] Configuration management
- [ ] Security baseline compliance
- [ ] Risk assessment protocols

7. PERSONNEL AND TRAINING

1. **Security Awareness**

- [ ] Employee security training program
- [ ] Contractor security requirements
- [ ] Security policy acknowledgment
- [ ] Social engineering awareness
- [ ] Incident reporting procedures

2. **Background Screening**

- [ ] Pre-employment screening
- [ ] Periodic background checks
- [ ] Security clearance verification
- [ ] Vendor personnel screening
- [ ] Access privilege review

8. COMPLIANCE DOCUMENTATION

1. **Required Documentation**

- [ ] Security policies and procedures
- [ ] System architecture diagrams
- [ ] Network topology maps
- [ ] Asset inventory records
- [ ] Change management logs

2. **Audit Records**

- [ ] Previous audit findings
- [ ] Remediation tracking
- [ ] Compliance certificates
- [ ] Testing results
- [ ] Incident reports

9. THIRD-PARTY RISK MANAGEMENT

1. **Vendor Assessment**

- [ ] Vendor security questionnaires
- [ ] Service level agreements
- [ ] Security requirements in contracts
- [ ] Third-party access controls
- [ ] Vendor compliance monitoring

2. **Supply Chain Security**

- [ ] Component verification procedures
- [ ] Supplier security requirements
- [ ] Software supply chain controls
- [ ] Hardware security validation
- [ ] Third-party code review

10. CERTIFICATION AND REPORTING

1. **Compliance Reporting**

- [ ] Quarterly security metrics
- [ ] Annual compliance reports
- [ ] Board security briefings
- [ ] Regulatory submissions
- [ ] Client security assessments

2. **Certification Maintenance**

- [ ] ISO certification status
- [ ] Industry certifications
- [ ] Personnel certifications
- [ ] Laboratory accreditations
- [ ] Quality management system

ATTESTATION

The undersigned certifies that this Security Compliance Audit Checklist has been reviewed and approved for use in evaluating DeepShield Systems, Inc.'s security compliance status.

Date: _

Signature: _

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

DeepShield Systems, Inc.

Signature: _

Name: James Morrison

Title: VP of Engineering

DeepShield Systems, Inc.

CONFIDENTIALITY NOTICE

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized reproduction or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.