PORT OF SINGAPORE SECURITY AUDIT FINDINGS 2023

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Audit Reference: PSA-2023-DS-847

1. EXECUTIVE SUMMARY

This security audit report documents the findings and recommendations from the comprehensive cybersecurity assessment conducted by DeepShield Systems, Inc. ("DeepShield") at the Port of Singapore Authority ("PSA") facilities between March 15, 2023, and June 30, 2023, pursuant to Contract No. PSA-CYB-2023-156.

2. SCOPE OF AUDIT

1. **Physical Infrastructure Assessment**

- Terminal Operations Control Centers (Terminals 1-4)
- Automated Guided Vehicle (AGV) Systems
- Crane Control Systems
- Gate Access Control Systems
- CCTV and Surveillance Infrastructure

2. **Digital Systems Assessment**

- SCADA Networks
- Terminal Operating System (TOS)
- Vessel Traffic Management System (VTMS)
- Container Tracking Systems
- Access Control and Authentication Systems

3. METHODOLOGY

1. The audit was conducted using DeepShield's proprietary Deep-Layer Security Architecture(TM) assessment framework, incorporating:

- Network penetration testing
- OT system vulnerability scanning

- Control system integrity verification
- Protocol analysis
- Threat modeling
- Risk assessment matrices

2. Testing Protocols

- Non-intrusive monitoring
- Simulated attack scenarios
- System response analysis
- Recovery time objectives (RTO) validation
- Incident response evaluation

4. KEY FINDINGS

1. **Critical Vulnerabilities**

- Three (3) Level 1 vulnerabilities in SCADA network segmentation
- One (1) Level 1 vulnerability in crane control system authentication
- Two (2) Level 2 vulnerabilities in AGV communication protocols

2. **High-Risk Areas**

- Legacy systems integration points
- Remote access protocols
- Firmware update mechanisms
- Third-party vendor access controls

3. **Medium-Risk Findings**

- Backup system redundancy
- Incident response documentation
- Change management procedures
- Access control audit trails

5. DETAILED VULNERABILITY ANALYSIS

1. **SCADA Network Segmentation (Critical)**

- Finding: Insufficient isolation between operational and administrative networks
- Impact: Potential unauthorized access to critical control systems
- Risk Level: Critical (CVSS Score: 9.8)
- Remediation Timeline: Immediate (30 days)

2. **Crane Control System Authentication (Critical)**

- Finding: Weak authentication protocols in legacy control systems
- Impact: Possible unauthorized system access and manipulation
- Risk Level: Critical (CVSS Score: 9.5)
- Remediation Timeline: Immediate (30 days)

3. **AGV Communication Protocols (High)**

- Finding: Unencrypted communication channels
- Impact: Potential interference with automated vehicle operations
- Risk Level: High (CVSS Score: 8.4)
- Remediation Timeline: 60 days

6. REMEDIATION RECOMMENDATIONS

1. **Immediate Actions (0-30 days)**

- Implement network segmentation using DeepShield's OT-specific firewall rules
- Deploy multi-factor authentication for all control system access
- Upgrade encryption protocols for AGV communications
- Install DeepShield's Deep-Layer Security Architecture(TM) monitoring system

2. **Short-Term Actions (31-90 days)**

- Develop comprehensive incident response procedures
- Implement automated patch management system
- Enhance system logging and monitoring capabilities
- Conduct staff security awareness training

3. **Long-Term Actions (91-180 days)**

- Develop system modernization roadmap
- Implement continuous monitoring solutions

- Establish security metrics and KPIs
- Create vendor security management program

7. COMPLIANCE AND REGULATORY CONSIDERATIONS

1. This audit was conducted in accordance with:

- Maritime and Port Authority of Singapore (MPA) Cybersecurity Code of Practice
- ISO 27001:2013 Information Security Management Standards
- IEC 62443 Industrial Network and System Security Standards
- NIST Cybersecurity Framework

8. IMPLEMENTATION PLAN

1. **Phase 1: Critical Remediation**

- Timeline: Immediate - 30 days
- Resource Requirements: 3 DeepShield security engineers
- Estimated Cost: $450,000 USD

2. **Phase 2: System Hardening**

- Timeline: 31-90 days
- Resource Requirements: 2 DeepShield security engineers
- Estimated Cost: $325,000 USD

3. **Phase 3: Long-term Security Enhancement**

- Timeline: 91-180 days
- Resource Requirements: 1 DeepShield security engineer
- Estimated Cost: $275,000 USD

9. DISCLAIMERS AND LIMITATIONS

1. This report represents findings as of June 30, 2023, and does not account for subsequent system changes or newly discovered vulnerabilities.

2. DeepShield Systems, Inc. makes no warranties, express or implied, regarding the completeness of this security assessment or the effectiveness of recommended remediation measures.

3. This document contains confidential and proprietary information and shall not be disclosed to third parties without written authorization from both DeepShield Systems, Inc. and the Port of Singapore Authority.

10. CERTIFICATION AND SIGNATURES

This security audit report is hereby certified as complete and accurate to the best of our knowledge as of the date of issuance.

Dated: June 30, 2023

```

–
Dr. Elena Rodriguez
Chief Security Architect
DeepShield Systems, Inc.

–
James Morrison
VP of Engineering
DeepShield Systems, Inc.

–
Sarah Blackwood
Chief Technology Officer
DeepShield Systems, Inc.
```

APPENDICES

A. Detailed Technical Findings

B. Test Cases and Methodologies

C. Risk Assessment Matrices

D. Compliance Mapping

E. Remediation Procedures

F. Network Architecture Diagrams

[End of Document]