SYDNEY PORTS CORPORATION SECURITY REVIEW

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Review Date: December 15, 2023

1. EXECUTIVE SUMMARY

This Security Review document ("Review") has been prepared by DeepShield Systems, Inc. ("DeepShield") pursuant to Contract No. SPC-2023-185 with Sydney Ports Corporation ("SPC") dated September 1, 2023, for the assessment and implementation of maritime cybersecurity infrastructure.

2. SCOPE OF REVIEW

1. The Review encompasses the following operational areas:

a) Port Management Systems (PMS)

b) Vessel Traffic Services (VTS)

c) Terminal Operating Systems (TOS)

d) Industrial Control Systems (ICS)

e) SCADA Networks

f) Maritime IoT Infrastructure

2. Assessment Period: October 1, 2023 - December 1, 2023

3. METHODOLOGY

1. Security Assessment Protocol

- Implementation of DeepShield's proprietary Maritime Infrastructure Security Assessment Framework (MISAF)
- Continuous monitoring over 60-day period
- Deep-layer architecture analysis
- Network topology mapping
- Threat vector identification
- Vulnerability scanning using DS-Scan(TM) v4.2

2. Testing Parameters

- Real-time threat simulation
- Penetration testing of critical systems
- API security validation
- Authentication protocols review
- Access control assessment
- Emergency response validation

4. FINDINGS

1. Critical Vulnerabilities

- Three (3) Level 1 vulnerabilities identified in legacy SCADA systems
- One (1) Zero-day vulnerability in VTS communication protocols
- Two (2) High-risk access control deficiencies in Terminal Operating Systems

2. System Architecture

- Current security architecture requires significant modernization
- Existing firewall configurations inadequate for emerging threats
- Limited segregation between operational and administrative networks
- Outdated ICS protocols in use across 40% of systems

3. Compliance Status

- Non-compliant with ISPS Code Section 2.4 requirements
- Partial compliance with IEC 62443 standards
- Gap identified in MTSA security requirements

5. RECOMMENDATIONS

1. Immediate Actions Required

- Implementation of DeepShield's OT Security Suite v3.5
- Network segmentation enhancement
- SCADA system upgrade to current security standards
- Installation of AI-driven threat detection systems
- Emergency response protocol modernization

2. Medium-Term Implementation

- Deployment of DeepShield's Maritime-Shield(TM) platform
- Integration of automated incident response systems
- Enhancement of access control mechanisms
- Implementation of zero-trust architecture
- Security awareness training program development

6. IMPLEMENTATION TIMELINE

1. Phase I (Immediate) - January 2024

- Critical vulnerability remediation
- Emergency response system upgrade
- Initial security architecture enhancement

2. Phase II (Q2 2024)

- Full platform deployment
- Staff training and certification
- System integration and testing

3. Phase III (Q3-Q4 2024)

- Advanced feature implementation
- Performance optimization
- Compliance verification

7. COST ANALYSIS

1. Initial Implementation: USD 2,850,000

2. Annual Maintenance: USD 425,000

3. Training and Support: USD 175,000

8. LEGAL DISCLAIMERS

This Review contains confidential and proprietary information of DeepShield Systems, Inc. and is protected under applicable intellectual property laws. The information contained herein is provided "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

9. CERTIFICATION

This Security Review has been prepared and certified by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: December 15, 2023

Robert Kessler

Chief Financial Officer

DeepShield Systems, Inc.

Date: December 15, 2023

10. APPENDICES

A. Technical Specifications

B. Compliance Documentation

C. Testing Protocols

D. Risk Assessment Matrices

E. Implementation Schedules

[END OF DOCUMENT]