MONTREAL PORT AUTHORITY INFRASTRUCTURE SECURITY REVIEW

CONFIDENTIAL AND PRIVILEGED

Security Assessment Report - Q4 2023

1. EXECUTIVE SUMMARY

This Infrastructure Security Review (the "Review") has been prepared by DeepShield Systems, Inc., a Delaware corporation ("DeepShield" or the "Company") for the Montreal Port Authority ("MPA") pursuant to Contract No. MPA-2023-456 dated September 15, 2023 (the "Service Agreement").

2. SCOPE OF REVIEW

1. The Review encompasses the following critical infrastructure components:

(a) Terminal automation systems

(b) Vessel traffic management systems

(c) Cargo handling control systems

(d) Access control infrastructure

(e) Emergency response systems

(f) SCADA networks supporting maritime operations

2. Assessment Period: October 1, 2023 - December 31, 2023

3. METHODOLOGY AND STANDARDS

1. The Review was conducted in accordance with:

(a) Transport Canada Marine Security Regulations (SOR/2004-144)

(b) NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

(c) IEC 62443 Industrial Network and System Security Standards

(d) ISO/IEC 27001:2013 Information Security Management Systems

2. Assessment Protocols

The Company deployed its proprietary DeepShield Maritime Infrastructure Protection Suite(TM) v4.2, incorporating:

- Network topology mapping
- Vulnerability scanning
- Threat modeling
- Penetration testing
- Control system security assessment

4. KEY FINDINGS

1. Critical Vulnerabilities

(a) Legacy SCADA protocols lacking encryption

(b) Outdated firmware in terminal automation controllers

(c) Insufficient network segmentation between IT/OT systems

2. High-Risk Areas

(a) Remote access mechanisms for third-party vendors

(b) Wireless network security for mobile terminal equipment

(c) Authentication protocols for operational technology systems

3. Compliance Status

(a) 87% alignment with Transport Canada requirements

(b) 73% conformance with NIST CSF controls

(c) Notable gaps in IEC 62443 compliance

5. REMEDIATION RECOMMENDATIONS

1. Immediate Actions (0-30 days)

(a) Implementation of encrypted protocols for all SCADA communications

(b) Firmware updates for vulnerable terminal controllers

(c) Enhanced access control mechanisms for critical systems

2. Short-Term Initiatives (31-90 days)

(a) Network segmentation implementation

(b) Security information and event management (SIEM) deployment

(c) OT system hardening

3. Long-Term Strategy (91-180 days)

(a) Zero-trust architecture implementation

(b) Advanced threat detection capabilities

(c) Automated incident response procedures

6. IMPLEMENTATION PLAN

1. Phase I: Emergency Remediation

- Timeline: January 15 - February 15, 2024
- Estimated Cost: $475,000 USD
- Resource Requirements: 3 senior security engineers

2. Phase II: Infrastructure Hardening

- Timeline: February 16 - May 15, 2024
- Estimated Cost: $890,000 USD
- Resource Requirements: 5 security engineers, 2 system architects

7. DISCLAIMERS AND LIMITATIONS

1. This Review represents a point-in-time assessment based on information available to DeepShield during the assessment period.

2. The Company makes no warranties, express or implied, regarding the completeness or accuracy of third-party information utilized in this Review.

3. Implementation of recommendations does not guarantee prevention of all security incidents or compliance with future regulatory requirements.

8. CONFIDENTIALITY

This document contains confidential and proprietary information of DeepShield Systems, Inc. and the Montreal Port Authority. Unauthorized disclosure, reproduction, or distribution is strictly prohibited.

9. EXECUTION

PREPARED AND SUBMITTED BY:

DeepShield Systems, Inc.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 10, 2024

REVIEWED BY:

By:

Name: James Morrison

Title: VP of Engineering

Date: January 10, 2024

Document Reference: DSS-MPA-SEC-2023-Q4-001

Version: 1.0

Classification: CONFIDENTIAL