FINNISH MARITIME INFRASTRUCTURE ASSESSMENT

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Date: January 11, 2024

1. EXECUTIVE SUMMARY

This Maritime Infrastructure Assessment ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") to evaluate cybersecurity vulnerabilities and industrial control system (ICS) protection requirements for maritime facilities and port infrastructure in Finland ("Target Infrastructure"), pursuant to Contract No. FIN-2023-144 dated November 15, 2023.

2. SCOPE OF ASSESSMENT

1. Geographic Coverage

- Port of Helsinki
- Port of Turku
- Port of Kotka
- Vuosaari Harbor Complex
- Associated maritime control systems within Finnish territorial waters

2. Systems Under Review

- Vessel Traffic Service (VTS) systems
- Port Management Information Systems (PMIS)
- Terminal Operating Systems (TOS)
- Automated cargo handling systems
- Navigation and positioning infrastructure
- Industrial control systems (ICS) for port operations
- SCADA networks supporting maritime operations

3. METHODOLOGY AND STANDARDS

1. Assessment Protocol

The evaluation was conducted in accordance with:

- ISO 27001:2013 Information Security Management Standards
- IEC 62443 Industrial Network and System Security
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- ENISA Guidelines for Maritime Cybersecurity

2. Testing Procedures

- Network architecture review
- Vulnerability scanning and penetration testing
- Control system isolation verification
- Security policy assessment
- Incident response capability evaluation
- Recovery procedure validation

4. KEY FINDINGS

1. Critical Vulnerabilities

- Legacy SCADA systems operating without modern security protocols
- Insufficient network segmentation between IT and OT environments
- Outdated firmware in critical navigation systems
- Inadequate access controls for remote maintenance interfaces

2. Risk Assessment Matrix

Vulnerability Category	Risk Level	Priority
Network Security	High	Immediate
Access Control	Medium	60 Days
System Updates	High	30 Days
Incident Response	Medium	90 Days

5. RECOMMENDATIONS

1. Immediate Actions (0-30 Days)

- Implementation of DeepShield's Maritime Security Module
- Network segmentation enhancement

- Critical firmware updates
- Access control system upgrade

2. Short-Term Actions (31-90 Days)

- Installation of advanced intrusion detection systems
- Employee security awareness training
- Incident response plan updates
- Security policy revision

3. Long-Term Actions (91-180 Days)

- Full system architecture modernization
- Redundancy implementation
- Security operations center establishment
- Continuous monitoring program development

6. IMPLEMENTATION PLAN

1. Phase I: Emergency Remediation

- Duration: 30 days
- Resource Requirements: 4 senior security engineers
- Estimated Cost: 450,000

2. Phase II: System Hardening

- Duration: 60 days
- Resource Requirements: 6 security specialists
- Estimated Cost: 750,000

3. Phase III: Long-Term Security Enhancement

- Duration: 90 days
- Resource Requirements: 8 technical staff
- Estimated Cost: 1,200,000

7. LEGAL DISCLAIMERS

1. This Assessment is provided for informational purposes only and does not constitute legal advice.

2. DeepShield makes no warranties, express or implied, regarding the completeness, accuracy, or reliability of the information contained herein.

3. This document contains confidential and proprietary information of DeepShield Systems, Inc. and shall not be disclosed without written authorization.

8. CERTIFICATION

The undersigned hereby certifies that this Assessment has been prepared in accordance with industry standards and professional practices.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024

By:

Name: James Morrison

Title: VP of Engineering

Date: January 11, 2024

9. APPENDICES

1. Technical Specifications
2. Testing Protocols
3. Vulnerability Reports
4. Implementation Timeline
5. Cost Breakdown

[End of Document]