INDIAN PORTS ASSOCIATION SECURITY REVIEW

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Date: January 11, 2024

Reference: DSS-IPA-2024-001

1. EXECUTIVE SUMMARY

This Security Review Report ("Report") documents the comprehensive assessment of cybersecurity infrastructure and operational technology (OT) protection systems implemented across Indian Ports Association ("IPA") facilities by DeepShield Systems, Inc. ("DeepShield") pursuant to Contract No. IPA-CYBER-2023-142 dated September 15, 2023.

2. SCOPE OF REVIEW

1. The security review encompassed the following major ports under IPA jurisdiction:

a) Mumbai Port Trust

b) Jawaharlal Nehru Port Trust

c) Kandla Port Trust

d) Visakhapatnam Port Trust

e) Chennai Port Trust

2. Assessment Parameters:

- Maritime Operations Control Systems (MOCS)
- Vessel Traffic Management Systems (VTMS)
- Terminal Operating Systems (TOS)
- Industrial Control Systems (ICS)
- SCADA Networks
- Physical Access Control Systems
- Emergency Response Systems

3. METHODOLOGY

1. The security review was conducted using DeepShield's proprietary Deep-Layer Security

Architecture Assessment Framework(TM) (DSAAF), incorporating:

- Network architecture analysis
- Threat modeling
- Vulnerability assessment
- Penetration testing
- Control system security evaluation
- Incident response capability assessment

2. Testing Protocol:

All assessments were conducted in accordance with:

- ISO/IEC 27001:2013 standards
- NIST Cybersecurity Framework
- IEC 62443 Industrial Network Security Standards
- IALA Guidelines for Maritime Security

4. KEY FINDINGS

1. Critical Infrastructure Protection:

- Implementation of segmented network architecture
- Deployment of industrial firewalls
- Integration of OT-specific intrusion detection systems
- Real-time monitoring capabilities
- Backup and recovery systems

2. Identified Vulnerabilities:

- Legacy SCADA systems requiring updates
- Insufficient network segmentation at Chennai Port
- Outdated firmware in critical ICS components
- Non-standardized security protocols across facilities
- Limited OT-specific incident response procedures

5. RECOMMENDATIONS

1. Immediate Actions:

a) Implementation of DeepShield's Maritime-Shield(TM) platform

b) Upgrade of legacy SCADA systems

c) Enhancement of network segmentation

d) Standardization of security protocols

e) Development of OT-specific incident response procedures

2. Long-term Strategic Initiatives:

a) Establishment of Security Operations Center (SOC)

b) Implementation of AI-driven threat detection

c) Regular security audits and assessments

d) Staff training and capacity building

e) Continuous monitoring and improvement program

6. IMPLEMENTATION TIMELINE

1. Phase I (Q1 2024):

- Initial deployment of Maritime-Shield(TM)
- Critical system upgrades
- Network architecture enhancement

2. Phase II (Q2-Q3 2024):

- SOC establishment
- Staff training
- Protocol standardization

3. Phase III (Q4 2024):

- Advanced feature implementation
- Integration testing
- Final security validation

7. COMPLIANCE AND REGULATORY CONSIDERATIONS

1. This security review and subsequent recommendations comply with:

- Indian Ports Act, 1908

- Information Technology Act, 2000
- Major Port Authorities Act, 2021
- International Ship and Port Facility Security (ISPS) Code
- Maritime Transportation Security Act (MTSA)

8. CONFIDENTIALITY AND DISCLAIMERS

1. This Report contains confidential and proprietary information of DeepShield Systems, Inc. and the Indian Ports Association. Unauthorized disclosure, copying, or distribution is strictly prohibited.

2. The findings and recommendations contained herein are based on conditions observed during the review period and information provided by IPA. DeepShield makes no warranties, express or implied, regarding the completeness or accuracy of this Report.

9. EXECUTION

IN WITNESS WHEREOF, this Security Review Report has been executed by the authorized representatives of DeepShield Systems, Inc. on the date first above written.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

By:

Name: James Morrison

Title: VP of Engineering

Date: January 11, 2024

[CORPORATE SEAL]