KOREAN SHIPYARD SECURITY ASSESSMENT REPORT

CONFIDENTIAL AND PRIVILEGED

Prepared for: DeepShield Systems, Inc.

Date: January 11, 2024

Reference: DSS-KOR-SA-2024-001

1. EXECUTIVE SUMMARY

This security assessment report evaluates the cybersecurity posture and operational technology (OT) infrastructure at three major Korean shipyards implementing DeepShield Systems' maritime protection solutions. The assessment was conducted between November 15, 2023, and December 20, 2023, by DeepShield's Advanced Security Assessment Team.

2. SCOPE OF ASSESSMENT

1. Target Facilities

- Facility A: Geoje Maritime Complex
- Facility B: Ulsan Heavy Industries Yard
- Facility C: Busan Naval Construction Center

2. Assessment Parameters

- Industrial Control System (ICS) architecture
- SCADA network infrastructure
- Maritime operational technology systems
- Critical infrastructure protection measures
- Integration points with existing security frameworks
- Compliance with KMSA (Korean Maritime Safety Administration) requirements

3. METHODOLOGY

1. Assessment Framework

- DeepShield Maritime Security Protocol v4.2
- IEC 62443 Industrial Network Security Standards
- NIST Framework for Maritime Cybersecurity

- Korean Shipyard Security Standards (KSSS 2023)

2. Testing Procedures

- Network architecture review
- Control system penetration testing
- OT system vulnerability assessment
- Security control validation
- Incident response capability evaluation
- Recovery procedure verification

4. KEY FINDINGS

1. Critical Infrastructure Protection

- All facilities maintain ISO 27001:2013 certification
- Implementation of air-gapped networks for critical systems
- Redundant control mechanisms for essential operations
- Multi-layer authentication protocols in place

2. Vulnerabilities Identified

- Legacy SCADA systems at Facility B requiring updates
- Insufficient network segmentation at Facility A
- Outdated firmware in critical PLCs at Facility C
- Non-standardized access control protocols

3. Risk Assessment Matrix

Risk Category	Severity	Probability	Impact Score
Network Security	High	Medium	8.5
Access Control	Medium	High	7.8
System Integration	Medium	Low	5.4
Incident Response	Low	Medium	4.2

5. COMPLIANCE ANALYSIS

1. Regulatory Compliance

- KMSA Maritime Security Directive 2023-04
- International Ship and Port Facility Security (ISPS) Code
- Korean Industrial Security Standards
- ISO/IEC 27001:2013 Requirements

2. Gap Analysis

- Documentation requirements
- Training protocols
- Incident reporting procedures
- Emergency response capabilities

6. RECOMMENDATIONS

1. Immediate Actions Required

- Upgrade SCADA systems at Facility B within 60 days
- Implement network segmentation at Facility A
- Update PLC firmware at Facility C
- Standardize access control protocols across all facilities

2. Medium-Term Improvements

- Enhanced monitoring capabilities
- Staff training program development
- Documentation standardization
- Integration of AI-driven threat detection

3. Long-Term Strategic Initiatives

- Infrastructure modernization roadmap
- Comprehensive security framework implementation
- Cross-facility standardization
- Advanced threat prevention capabilities

7. IMPLEMENTATION TIMELINE

1. Phase I (0-90 days)

- Critical system upgrades
- Immediate vulnerability remediation
- Essential staff training
- Documentation updates

2. Phase II (91-180 days)

- Security framework enhancement
- Advanced monitoring implementation
- Process standardization
- Integration testing

3. Phase III (181-365 days)

- Long-term improvements
- System optimization
- Advanced capability deployment
- Continuous improvement program

8. BUDGET IMPLICATIONS

1. Estimated Costs

- Immediate remediation: USD 1.2M
- Medium-term improvements: USD 2.8M
- Long-term initiatives: USD 4.5M
- Total investment required: USD 8.5M

9. CERTIFICATION

This security assessment was conducted in accordance with DeepShield Systems' Standard Operating Procedures and international security standards. The findings and recommendations contained herein represent our professional opinion based on the information available at the time of the assessment.

10. DISCLAIMERS AND LIMITATIONS

This report is confidential and intended solely for the use of DeepShield Systems, Inc. and its

authorized representatives. The assessment results are based on conditions observed during the assessment period and information provided by facility personnel. Future security incidents may occur due to changing conditions or circumstances beyond the scope of this assessment.

11. AUTHORIZATION

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Reviewed by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Approved by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: January 11, 2024

[END OF REPORT]