PANAMA CANAL SCADA SYSTEMS SECURITY REVIEW

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Document Reference: DSS-PC-SR-2023-001

Date: December 15, 2023

1. EXECUTIVE SUMMARY

This Security Review documents the assessment of Supervisory Control and Data Acquisition (SCADA) systems deployed across Panama Canal operations, conducted by DeepShield Systems, Inc. ("DeepShield") pursuant to Contract No. ACP-2023-155 with the Panama Canal Authority ("ACP").

2. SCOPE OF REVIEW

1. The security assessment encompassed:

a) Lock control systems at Gat n, Pedro Miguel, and Miraflores

b) Water management SCADA infrastructure

c) Vessel traffic management systems

d) Emergency response and backup control systems

e) Integration points with maritime communication networks

2. Review Period: September 15, 2023 - December 1, 2023

3. METHODOLOGY

1. Assessment Protocol

- Implementation of DeepShield's proprietary OT Security Assessment Framework v4.2
- Non-intrusive network monitoring using passive data collection
- Analysis of system architecture and security controls
- Review of existing security policies and procedures
- Threat modeling specific to maritime infrastructure

2. Testing Parameters

- Network segmentation validation

- Control system access protocols
- Authentication mechanisms
- Encryption standards
- Backup system integrity
- Emergency override capabilities

4. KEY FINDINGS

1. Critical Vulnerabilities

a) Legacy PLC systems at Gat n locks operating without current security patches

b) Insufficient network segmentation between IT and OT environments

c) Outdated authentication protocols on remote access systems

d) Unencrypted SCADA protocol communications

2. High-Risk Areas

a) Water level control systems lacking redundant security measures

b) Vessel tracking system integration points with insufficient access controls

c) Emergency override systems with inadequate authentication requirements

5. RECOMMENDATIONS

1. Immediate Actions Required

- Implementation of DeepShield's Advanced ICS Protection Suite
- Network segmentation enhancement using Next-Generation Firewalls
- PLC firmware updates and security hardening
- Implementation of encrypted SCADA protocols
- Multi-factor authentication deployment for all remote access

2. Short-Term Improvements (0-6 months)

- Installation of AI-driven anomaly detection systems
- Enhancement of backup system security
- Implementation of comprehensive access control policies
- Development of security incident response procedures

3. Long-Term Strategy (6-24 months)

- Complete modernization of control system architecture
- Implementation of zero-trust security framework
- Development of continuous monitoring capabilities
- Enhancement of disaster recovery systems

6. IMPLEMENTATION PLAN

1. Phase I: Critical Security Enhancements

- Timeline: January 2024 - March 2024
- Estimated Cost: $4.5M USD
- Primary Focus: Critical vulnerability remediation

2. Phase II: System Modernization

- Timeline: April 2024 - December 2024
- Estimated Cost: $12.8M USD
- Primary Focus: Infrastructure upgrades and security enhancement

7. LEGAL DISCLAIMERS

1. This Security Review is provided pursuant to the terms of Contract No. ACP-2023-155 and is subject to all confidentiality and non-disclosure provisions therein.

2. The findings and recommendations contained herein represent DeepShield's professional assessment based on information available during the review period. DeepShield makes no warranties or guarantees regarding the completeness or accuracy of this assessment.

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

8. CERTIFICATION

This Security Review has been prepared and verified by DeepShield's qualified security professionals in accordance with industry standards and best practices.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date: December 15, 2023

By:

James Morrison

VP of Engineering

Date: December 15, 2023

9. APPENDICES

1. Detailed Technical Findings (See Attachment A)

2. Risk Assessment Matrix (See Attachment B)

3. Implementation Timeline (See Attachment C)

4. Cost Breakdown Analysis (See Attachment D)