HOUSTON SHIP CHANNEL PROTECTION ASSESSMENT

CONFIDENTIAL AND PROPRIETARY

Prepared by DeepShield Systems, Inc.

Date: January 11, 2024

Document Reference: HSC-PA-2024-001

1. EXECUTIVE SUMMARY

This Protection Assessment evaluates the cybersecurity and operational technology (OT) vulnerabilities of maritime infrastructure along the Houston Ship Channel, pursuant to the requirements set forth in Maritime Security Directive 104-6 and the Port Security Enhancement Act of 2022. This assessment has been prepared by DeepShield Systems, Inc. ("DeepShield") based on comprehensive technical analysis and site evaluations conducted between September 15, 2023 and December 31, 2023.

2. SCOPE OF ASSESSMENT

1. Geographic Coverage

- Main Houston Ship Channel (25-mile segment)
- Bayport Terminal Complex
- Barbours Cut Container Terminal
- Buffalo Bayou turning basin
- Associated petrochemical facilities within 1000 yards of channel boundaries

2. Systems Evaluated

- SCADA control systems
- Terminal automation systems
- Vessel traffic management systems
- Industrial control systems (ICS)
- Physical access control infrastructure
- Emergency shutdown systems
- Communications infrastructure

3. METHODOLOGY

1. Assessment Protocol

The evaluation was conducted using DeepShield's proprietary Deep-Layer Security Architecture(TM) assessment methodology, incorporating:

- Network architecture analysis
- Control system vulnerability scanning
- Threat modeling and risk quantification
- Attack surface mapping
- Operational resilience evaluation
- Recovery capability assessment

2. Compliance Framework

This assessment adheres to:

- NIST Cybersecurity Framework v1.1
- Maritime Transportation Security Act requirements
- API 1164 Pipeline SCADA Security standards
- ISA/IEC 62443 series standards
- Coast Guard Navigation and Vessel Inspection Circular 01-20

4. FINDINGS AND RISK ASSESSMENT

1. Critical Vulnerabilities

- Legacy control system protocols lacking encryption
- Insufficient network segmentation between IT/OT systems
- Outdated firmware in critical infrastructure components
- Inadequate authentication mechanisms for remote access
- Unpatched known vulnerabilities in SCADA systems

2. Risk Quantification

Risk levels are categorized as follows:

- High Risk: 7 identified issues
- Medium Risk: 12 identified issues
- Low Risk: 15 identified issues

5. RECOMMENDED MITIGATION MEASURES

1. Immediate Actions (0-90 days)

a) Implementation of DeepShield's Maritime Protection Module(TM)

b) Network segmentation enhancement

c) Control system protocol encryption

d) Multi-factor authentication deployment

e) Critical firmware updates

2. Medium-Term Actions (90-180 days)

a) SCADA system hardening

b) Security information and event management (SIEM) implementation

c) OT network monitoring enhancement

d) Incident response plan development

e) Staff security awareness training

3. Long-Term Actions (180-360 days)

a) Complete system architecture redesign

b) Redundant control system implementation

c) Advanced threat detection deployment

d) Recovery capability enhancement

e) Continuous monitoring program establishment

6. IMPLEMENTATION TIMELINE AND COSTS

1. Phase I (Immediate Actions)

- Timeline: February 1, 2024 - April 30, 2024
- Estimated Cost: $4,750,000

2. Phase II (Medium-Term Actions)

- Timeline: May 1, 2024 - October 31, 2024
- Estimated Cost: $6,250,000

3. Phase III (Long-Term Actions)

- Timeline: November 1, 2024 - January 31, 2025
- Estimated Cost: $8,500,000

7. LEGAL DISCLAIMERS AND LIMITATIONS

This assessment represents DeepShield Systems, Inc.'s professional opinion based on information available at the time of evaluation. The assessment is provided "as-is" without warranty of any kind, either expressed or implied. DeepShield assumes no responsibility for any losses or damages resulting from the use of this information.

Implementation of recommended measures does not guarantee complete protection against all potential threats or vulnerabilities. This document is confidential and intended solely for the use of authorized recipients.

8. CERTIFICATION

This Protection Assessment has been prepared and reviewed by qualified cybersecurity professionals at DeepShield Systems, Inc. in accordance with industry standards and applicable regulations.

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Reviewed and Approved by:

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 11, 2024

[END OF DOCUMENT]