TOTAL ENERGIES TERMINAL PROTECTION ASSESSMENT

CONFIDENTIAL AND PROPRIETARY

DeepShield Systems, Inc.

Date: January 11, 2024

1. EXECUTIVE SUMMARY

This Terminal Protection Assessment ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") for Total Energies' LNG Terminal facilities ("Client Facilities") pursuant to Master Services Agreement dated June 15, 2023 ("MSA"). This Assessment evaluates the cybersecurity posture of operational technology (OT) systems and industrial control systems (ICS) at Client Facilities.

2. SCOPE OF ASSESSMENT

1. **Facility Coverage**

Assessment encompasses Total Energies' primary LNG terminal operations including:

- Main processing terminal (Port of Houston)
- Secondary distribution terminal (Corpus Christi)
- Associated pipeline control systems
- Maritime loading/offloading systems

2. **Systems Evaluated**

- SCADA control networks
- Terminal automation systems
- Safety instrumented systems (SIS)
- Process control networks (PCN)
- Maritime control interfaces
- Emergency shutdown systems (ESD)

3. METHODOLOGY

1. **Assessment Protocol**

Assessment conducted using DeepShield's proprietary Deep-Layer Security Architecture(TM)

evaluation framework, incorporating:

- Network architecture review
- Control system vulnerability scanning
- Threat modeling analysis
- Security control effectiveness testing
- Operational resilience evaluation

2. **Standards Compliance**

Assessment methodology aligns with:

- IEC 62443 Industrial Network Security Standards
- NIST Cybersecurity Framework
- API 1164 Pipeline SCADA Security
- MTSA/ISPS maritime security requirements

4. FINDINGS AND RISK ASSESSMENT

1. **Critical Vulnerabilities**

- Legacy control system protocols lacking encryption
- Insufficient network segmentation between IT/OT systems
- Outdated firmware versions on critical PLCs
- Inadequate access control mechanisms for remote maintenance

2. **Operational Risks**

- Potential for unauthorized system access via unsecured protocols
- Risk of process disruption through compromised control systems
- Safety system override vulnerabilities
- Maritime loading system exposure to network-based attacks

5. RECOMMENDED REMEDIATION MEASURES

1. **Immediate Actions**

- Implementation of DeepShield's OT Network Guardian(TM) solution
- Deployment of encrypted protocol gateways
- Enhancement of network segmentation architecture

- Installation of dedicated security monitoring systems

2. **Strategic Improvements**
- Migration to secure control system protocols
- Implementation of zero-trust architecture
- Enhancement of authentication mechanisms
- Deployment of AI-driven anomaly detection

6. IMPLEMENTATION PLAN

1. **Phase I: Critical Protection** (0-90 days)
- Network security architecture enhancement
- Control system protocol security upgrade
- Implementation of basic monitoring systems

2. **Phase II: Enhanced Security** (91-180 days)
- Advanced threat detection deployment
- Security information and event management (SIEM) integration
- Automated response system implementation

7. LEGAL DISCLAIMERS

1. This Assessment is provided pursuant to the terms and conditions of the MSA between DeepShield and Total Energies.

2. This Assessment represents DeepShield's professional opinion based on information available at the time of evaluation. DeepShield makes no warranties, express or implied, regarding the completeness or accuracy of this Assessment.

3. Implementation of recommended measures does not guarantee prevention of all security incidents or system compromises.

8. CONFIDENTIALITY

This Assessment contains confidential and proprietary information of both DeepShield Systems, Inc. and Total Energies. Distribution of this document is restricted to authorized personnel only. Unauthorized disclosure is strictly prohibited.

9. EXECUTION

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024

Reviewed and Approved:

By:

Name: James Morrison

Title: VP of Engineering

Date: January 11, 2024

[DOCUMENT ENDS]