BP North Sea Platform Security Assessment

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Assessment Date: December 15, 2023

1. EXECUTIVE SUMMARY

This security assessment report ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") for BP p.l.c. ("Client") regarding the cybersecurity and operational technology (OT) infrastructure of the Client's North Sea offshore platforms, specifically platforms Alpha, Bravo, and Charlie located in blocks 15/21a and 15/21b of the UK Continental Shelf ("Target Assets").

2. SCOPE OF ASSESSMENT

1. This Assessment evaluates the following systems and infrastructure:

a) Industrial Control Systems (ICS)

b) Supervisory Control and Data Acquisition (SCADA) networks

c) Platform automation systems

d) Emergency shutdown systems

e) Process control networks

f) Maritime communication systems

g) Subsea control infrastructure

2. Assessment methodology included:

a) Network architecture review

b) Vulnerability scanning

c) Penetration testing

d) Control system audit

e) Security policy review

f) Incident response capability assessment

3. KEY FINDINGS

1. Critical Vulnerabilities

- Legacy SCADA protocols without encryption
- Outdated firmware in subsea control units
- Insufficient network segmentation between IT/OT systems
- Unpatched control system vulnerabilities (CVE-2023-27163)

2. High-Risk Areas

- Remote access protocols
- Wireless network security
- Third-party vendor access controls
- Backup and recovery systems

3. Compliance Status

- IEC 62443 compliance: Partial
- NIST Cybersecurity Framework alignment: 67%
- UK NIS Regulations compliance: Substantial

4. RECOMMENDATIONS

1. Immediate Actions (0-3 months)

a) Implement encrypted SCADA protocols

b) Update subsea control unit firmware

c) Deploy network segmentation solutions

d) Patch identified vulnerabilities

2. Short-Term Actions (3-6 months)

a) Enhanced access control implementation

b) Security monitoring system deployment

c) Incident response plan updates

d) Staff security training program

3. Long-Term Actions (6-12 months)

a) Full IEC 62443 compliance program

b) OT network modernization

c) Automated threat detection deployment

d) Security operations center establishment

5. IMPLEMENTATION PLAN

1. Phase I - Critical Remediation

- Timeline: January 15, 2024 - March 31, 2024
- Estimated Cost: $2.7M USD
- Resource Requirements: 3 FTE security engineers

2. Phase II - Security Enhancement

- Timeline: April 1, 2024 - September 30, 2024
- Estimated Cost: $4.1M USD
- Resource Requirements: 5 FTE security engineers

6. RISK ASSESSMENT MATRIX

1. Current Risk Levels

- Critical: 3 findings
- High: 7 findings
- Medium: 12 findings
- Low: 8 findings

2. Post-Implementation Risk Levels

- Critical: 0 findings
- High: 2 findings
- Medium: 8 findings
- Low: 20 findings

7. DISCLAIMERS AND LIMITATIONS

1. This Assessment represents findings as of December 15, 2023, and does not account for subsequent changes in infrastructure, threats, or vulnerabilities.

2. DeepShield makes no warranties, express or implied, regarding the completeness of this Assessment or the effectiveness of recommended security measures.

3. This Assessment is based on information provided by Client and testing permitted within agreed-upon parameters.

8. CONFIDENTIALITY

This document contains confidential and proprietary information of both DeepShield Systems, Inc. and BP p.l.c. Unauthorized disclosure, reproduction, or distribution is strictly prohibited.

9. EXECUTION

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: December 15, 2023

By:

Name: James Morrison

Title: VP of Engineering

Date: December 15, 2023

10. APPENDICES

Appendix A: Detailed Vulnerability Findings

Appendix B: Testing Methodology

Appendix C: Compliance Requirements

Appendix D: Technical Specifications

Appendix E: Risk Assessment Details

[End of Document]