THAMES WATER TREATMENT PLANT SECURITY ASSESSMENT

CONFIDENTIAL AND PRIVILEGED

DeepShield Systems, Inc.

Assessment Date: January 11, 2024

Document Reference: DSS-SEC-2024-011

1. EXECUTIVE SUMMARY

This Security Assessment Report ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") for the Thames Water Treatment Plant facility located at [REDACTED], United Kingdom. The Assessment evaluates critical infrastructure vulnerabilities and cybersecurity risks within the operational technology (OT) environment pursuant to Contract No. TWU-2023-456 dated September 15, 2023.

2. SCOPE OF ASSESSMENT

1. The Assessment encompasses:

a) Industrial Control System (ICS) architecture review

b) SCADA network vulnerability analysis

c) Physical security controls evaluation

d) OT/IT convergence risk assessment

e) Critical process monitoring systems

f) Chemical management systems

g) Remote access infrastructure

h) Emergency response systems

2. Assessment Methodology

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

- Network topology mapping
- Threat modeling
- Vulnerability scanning (passive)
- Control system configuration review

- Security policy analysis
- Incident response capability evaluation

3. KEY FINDINGS

1. Critical Vulnerabilities

a) Legacy PLC systems operating without current firmware updates

b) Insufficient network segmentation between IT and OT environments

c) Outdated authentication protocols on remote access systems

d) Unencrypted SCADA communications on specific control loops

2. High-Risk Areas

- Chemical dosing control systems
- Filter backwash automation
- Remote pump station monitoring
- SCADA historian databases

3. Compliance Status

Assessment of compliance with:

- IEC 62443 Series
- NIST Cybersecurity Framework
- UK National Cyber Security Centre Guidelines
- Water-ISAC Security Recommendations

4. RECOMMENDED REMEDIATION MEASURES

1. Immediate Actions (0-30 days):

a) Implementation of network segmentation controls

b) Update of critical PLC firmware

c) Enhancement of access control systems

d) Deployment of encrypted SCADA protocols

2. Short-Term Measures (31-90 days):

a) Installation of DeepShield's OT Network Monitoring Solution

b) Implementation of anomaly detection systems

c) Security awareness training for operational staff

d) Enhancement of backup and recovery procedures

3. Long-Term Initiatives (91-180 days):

a) Complete system architecture redesign

b) Implementation of zero-trust security model

c) Establishment of Security Operations Center (SOC)

d) Development of comprehensive incident response plan

5. RISK ASSESSMENT MATRIX

1. Risk Categories:

- Critical (Immediate action required)
- High (Action required within 30 days)
- Medium (Action required within 90 days)
- Low (Monitor and review quarterly)

2. Impact Assessment:

- Safety and Environmental Impact
- Operational Continuity
- Regulatory Compliance
- Public Health Impact

6. LIMITATIONS AND DISCLAIMERS

1. This Assessment represents conditions observed during the assessment period and cannot guarantee future security status.

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

3. Implementation of recommendations does not guarantee prevention of all security incidents or compliance with all applicable regulations.

7. CONFIDENTIALITY

This document contains confidential and proprietary information of DeepShield Systems, Inc. and Thames Water Utilities. Distribution is restricted to authorized personnel only. Unauthorized disclosure may result in legal action.

8. CERTIFICATION

This Assessment has been prepared in accordance with DeepShield's professional standards and methodologies by qualified security professionals.

EXECUTED this 11th day of January, 2024.

DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

By:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

[CORPORATE SEAL]