SERVICE LEVEL AGREEMENT

Pipeline Security Services Agreement

Between DeepShield Systems, Inc. and Kinder Morgan, Inc.

Effective Date: January 15, 2024

This Service Level Agreement ("Agreement") is entered into by and between DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2200 Technology Drive, Houston, TX 77002 ("Provider"), and Kinder Morgan, Inc., a Delaware corporation ("Client").

1. DEFINITIONS

1 "Critical Infrastructure" means Client's pipeline control systems, SCADA networks, and associated operational technology infrastructure.

2 "Security Services" means Provider's comprehensive industrial cybersecurity monitoring, threat detection, and incident response services.

3 "Service Level Metrics" means the quantitative and qualitative measurements defined in Section 3.

4 "System Availability" means the percentage of time the Security Services are operational and accessible.

2. SCOPE OF SERVICES

1 Provider shall deliver the following Security Services:

a) 24/7 real-time monitoring of Client's Critical Infrastructure

b) AI-driven threat detection and analysis

c) Automated incident response and mitigation

d) Monthly security assessment reports

e) Quarterly penetration testing

f) Emergency response within specified timeframes

2 Geographic Coverage: All Client pipeline assets within North America, including:

- Trans Mountain Pipeline System
- Natural Gas Pipeline Company of America

- Tennessee Gas Pipeline

3. SERVICE LEVEL METRICS

1 System Availability

- Minimum 99.99% uptime
- Maximum 4.38 hours of planned downtime per year
- Scheduled maintenance limited to 2:00 AM - 4:00 AM EST

2 Incident Response Times

- Critical Incidents: 15 minutes
- High Priority: 1 hour
- Medium Priority: 4 hours
- Low Priority: 24 hours

3 Threat Detection

- False Positive Rate: <0.1%
- Mean Time to Detect (MTTD): <5 minutes
- Mean Time to Respond (MTTR): <30 minutes

4. REPORTING AND COMMUNICATIONS

1 Provider shall deliver:

- Real-time threat alerts
- Daily security status reports
- Weekly performance metrics
- Monthly executive summaries
- Quarterly compliance reports

2 Communication Protocols

- Dedicated secure communication channel
- Encrypted messaging system
- 24/7 emergency hotline
- Designated technical liaison

5. COMPLIANCE AND STANDARDS

1 Provider shall maintain compliance with:

- NIST Cybersecurity Framework
- API 1164 Pipeline SCADA Security
- TSA Pipeline Security Guidelines
- ISO 27001:2013
- NERC CIP Standards

6. PERFORMANCE CREDITS

1 System Availability Credits:

- <99.99%: 10% of monthly fee
- <99.9%: 25% of monthly fee
- <99%: 50% of monthly fee

2 Incident Response Credits:

- Critical Incident >15 min: $10,000 per incident
- High Priority >1 hour: $5,000 per incident

7. TERM AND TERMINATION

1 Initial Term: Three (3) years from Effective Date

2 Renewal: Automatic one-year renewals unless terminated

3 Termination Rights:

- For cause with 30 days' notice
- For convenience with 90 days' notice

8. CONFIDENTIALITY

1 All security-related information, including but not limited to threat data, incident reports, and system vulnerabilities, shall be treated as Confidential Information.

9. LIMITATION OF LIABILITY

1 Provider's aggregate liability shall not exceed the total fees paid in the twelve (12) months preceding the claim.

2 Neither party shall be liable for indirect, special, or consequential damages.

10. EXECUTION

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date:

KINDER MORGAN, INC.

By:

Name:

Title:

Date: