CROSS-BORDER DATA TRANSFER AGREEMENT

THIS CROSS-BORDER DATA TRANSFER AGREEMENT (the "Agreement") is made effective as of February 1, 2024 (the "Effective Date")

BY AND BETWEEN:

DEEPSHIELD SYSTEMS, INC., a Delaware corporation with its principal place of business at 2100 Innovation Drive, Suite 400, Wilmington, Delaware 19801 ("Data Exporter")

AND

Its affiliates, subsidiaries, and authorized third-party processors as listed in Schedule A (each a "Data Importer")

RECITALS

WHEREAS, Data Exporter provides industrial control system (ICS) security solutions and operational technology (OT) protection services to clients globally;

WHEREAS, in the course of its operations, Data Exporter must transfer certain protected data across international borders to Data Importers for processing and analysis;

WHEREAS, the parties wish to ensure all cross-border data transfers comply with applicable data protection laws including but not limited to GDPR, CCPA, and other relevant regulations;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the parties agree as follows:

1. DEFINITIONS

1 "Applicable Data Protection Laws" means all laws, regulations, and binding requirements relating to the processing of Personal Data and privacy in any relevant jurisdiction.

2 "Industrial Control System Data" means operational data collected from industrial automation systems, SCADA networks, and manufacturing operations.

3 "Personal Data" means any information relating to an identified or identifiable natural person as defined under Applicable Data Protection Laws.

4 "Processing" means any operation performed on Protected Data, whether automated or not.

5 "Protected Data" means Personal Data and Industrial Control System Data subject to this Agreement.

2. SCOPE AND PURPOSE

1 This Agreement governs all transfers of Protected Data from Data Exporter to Data Importers for the following purposes:

(a) Threat detection and security monitoring

(b) Anomaly detection and pattern analysis

(c) Incident response and forensic investigation

(d) System optimization and performance analysis

(e) Regulatory compliance and reporting

2 Geographic Scope: This Agreement covers data transfers to and from the following territories: United States, European Union, United Kingdom, Canada, Australia, and Japan.

3. DATA PROTECTION SAFEGUARDS

1 Technical Measures. Data Importers shall implement appropriate technical safeguards including:

(a) End-to-end encryption (minimum AES-256)

(b) Access controls and multi-factor authentication

(c) Network segmentation and firewalls

(d) Regular security assessments and penetration testing

(e) Secure backup and disaster recovery systems

2 Organizational Measures. Data Importers shall maintain:

(a) Written information security policies

(b) Regular staff training on data protection

(c) Incident response procedures

(d) Data minimization protocols

(e) Access management and review processes

4. TRANSFER MECHANISMS

1 Standard Contractual Clauses. Where required by law, transfers shall be governed by the Standard Contractual Clauses adopted by relevant data protection authorities.

2 Binding Corporate Rules. Where applicable, transfers may be conducted under approved Binding Corporate Rules.

3 Adequacy Decisions. Transfers to countries with adequacy decisions shall comply with relevant requirements.

5. DATA IMPORTER OBLIGATIONS

1 Processing Limitations. Data Importers shall:

(a) Process Protected Data only as instructed by Data Exporter

(b) Limit access to authorized personnel

(c) Maintain confidentiality obligations

(d) Implement purpose limitation controls

(e) Delete or return data upon request

2 Subprocessing. Data Importers shall:

(a) Obtain prior written authorization for subprocessors

(b) Flow down all obligations in this Agreement

(c) Remain liable for subprocessor compliance

6. AUDIT AND COMPLIANCE

1 Data Exporter may audit Data Importers' compliance annually with 30 days notice.

2 Data Importers shall maintain records demonstrating compliance with this Agreement.

3 Data Importers shall promptly address any compliance gaps identified.

7. SECURITY INCIDENTS

1 Data Importers shall notify Data Exporter within 24 hours of discovering any security incident affecting Protected Data.

2 Notification shall include:

(a) Nature and extent of the incident

(b) Categories of data affected

(c) Mitigation measures taken

(d) Potential risks and impacts

(e) Remediation timeline

8. TERM AND TERMINATION

1 This Agreement shall remain in effect while Protected Data transfers continue.

2 Upon termination, Data Importers shall:

(a) Cease processing Protected Data

(b) Return or securely delete all copies

(c) Certify deletion in writing

9. MISCELLANEOUS

1 Governing Law. This Agreement shall be governed by Delaware law.

2 Amendments. This Agreement may only be modified in writing signed by both parties.

3 Severability. If any provision is invalid, the remainder shall continue in effect.

4 Entire Agreement. This Agreement constitutes the complete agreement regarding data transfers.

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

DEEPSHIELD SYSTEMS, INC.

By:

Name: Robert Kessler

Title: Chief Financial Officer

Date:

[SIGNATURE BLOCKS FOR DATA IMPORTERS TO FOLLOW]

SCHEDULE A

[List of Data Importers and contact details]