# SUEZ CANAL AUTHORITY PROTECTION SYSTEMS AGREEMENT

THIS PROTECTION SYSTEMS AGREEMENT (the "Agreement") is made and entered into as of March 15, 2024 (the "Effective Date"), by and between:

DEEPSHIELD SYSTEMS, INC., a Delaware corporation with its principal place of business at 2200 Innovation Way, San Jose, California 95134 ("DeepShield" or "Provider")

and

THE SUEZ CANAL AUTHORITY, an autonomous public authority of the Arab Republic of Egypt with its principal office at Circular Road, Ismailia, Egypt ("SCA" or "Authority")

## RECITALS

WHEREAS, the Authority operates and maintains the Suez Canal, a critical maritime infrastructure connecting the Mediterranean Sea and the Red Sea;

WHEREAS, Provider specializes in advanced industrial control system security solutions and critical infrastructure protection systems;

WHEREAS, the Authority desires to engage Provider to implement and maintain comprehensive cybersecurity protection systems for its operational technology infrastructure; and

WHEREAS, Provider desires to provide such services subject to the terms and conditions set forth herein.

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

## 1. DEFINITIONS

1 "Critical Infrastructure" means the operational technology systems, SCADA networks, and industrial control systems used in the operation and management of the Suez Canal.

2 "DeepShield Platform" means Provider's proprietary industrial cybersecurity platform and associated software, including all updates and modifications thereof.

3 "Protected Systems" means the Authority's Critical Infrastructure components covered under this Agreement, as specified in Exhibit A.

4 "Security Incident" means any actual or suspected unauthorized access, breach, or cyber attack affecting the Protected Systems.

## 2. SCOPE OF SERVICES

1 Implementation Services. Provider shall:

(a) Deploy the DeepShield Platform across all Protected Systems

(b) Configure maritime-specific security modules

(c) Establish real-time monitoring and threat detection capabilities

(d) Implement automated incident response protocols

(e) Integrate with existing Authority security infrastructure

2 Ongoing Services. Provider shall:

(a) Provide 24/7 monitoring and threat detection

(b) Conduct regular security assessments

(c) Deliver monthly security reports

(d) Maintain and update the DeepShield Platform

(e) Provide incident response support

## 3. SERVICE LEVELS AND PERFORMANCE STANDARDS

1 System Availability. Provider shall maintain 99.99% system availability for core security functions.

2 Incident Response Times:

(a) Critical Incidents: 15 minutes

(b) High Priority: 1 hour

(c) Medium Priority: 4 hours

(d) Low Priority: 24 hours

3 Performance Credits. Provider shall issue service credits for failure to meet performance standards according to Schedule B.

## 4. FEES AND PAYMENT

1 Implementation Fee: USD 2,500,000, payable as follows:

(a) 40% upon contract execution

(b) 30% upon system deployment

(c) 30% upon acceptance testing

2 Annual Maintenance Fee: USD 1,200,000, payable quarterly in advance

3 Additional Services: As specified in Schedule C

## 5. TERM AND TERMINATION

1 Initial Term: Five (5) years from the Effective Date

2 Renewal: Automatic two-year renewals unless terminated with 180 days' notice

3 Termination Rights:

(a) For cause with 30 days' cure period

(b) For convenience with 180 days' notice and early termination fee

## 6. SECURITY AND CONFIDENTIALITY

1 Data Security Standards. Provider shall maintain ISO 27001 certification and comply with IEC 62443 standards.

2 Confidential Information. All technical specifications, security protocols, and infrastructure details shall be treated as strictly confidential.

3 Security Clearances. Provider personnel shall obtain necessary security clearances from Egyptian authorities.

## 7. COMPLIANCE AND REGULATIONS

1 Regulatory Compliance. Provider shall comply with:

(a) Egyptian cybersecurity regulations

(b) Maritime security standards

(c) International maritime conventions

(d) Critical infrastructure protection requirements

2 Export Controls. Provider shall maintain compliance with U.S. export control regulations.

## 8. LIABILITY AND INDEMNIFICATION

1 Limitation of Liability. Provider's aggregate liability shall not exceed annual fees paid.

2 Indemnification. Provider shall indemnify Authority for third-party claims arising from security breaches caused by Provider's gross negligence.

3 Insurance. Provider shall maintain cyber liability insurance of USD 10,000,000.

## 9. GENERAL PROVISIONS

1 Governing Law: Laws of England and Wales

2 Dispute Resolution: ICC Arbitration in London

3 Force Majeure: Standard provisions excluding cyber attacks

4 Assignment: Requires prior written consent

5 Amendments: Must be in writing and signed by both parties

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: _**

SUEZ CANAL AUTHORITY

**By: _**

**Name: _**

**Title: _**

**Date: _**

[Exhibits and Schedules to follow]