VANCOUVER HARBOR SECURITY SYSTEMS CONTRACT

THIS SECURITY SYSTEMS CONTRACT (the "Agreement") is made and entered into as of February 15, 2024 (the "Effective Date"), by and between:

DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2500 Harbor Drive, Suite 400, Seattle, WA 98101 ("Contractor")

and

Vancouver Fraser Port Authority, a Canadian federal crown corporation operating as the Vancouver Fraser Port Authority, with its principal place of business at 100 The Pointe, 999 Canada Place, Vancouver, BC V6C 3T4 ("Port Authority")

RECITALS

WHEREAS, the Port Authority operates and maintains critical maritime infrastructure requiring advanced cybersecurity protection for its operational technology (OT) systems and industrial control systems (ICS);

WHEREAS, Contractor specializes in providing industrial cybersecurity solutions and has developed proprietary technology for protecting maritime and port infrastructure;

WHEREAS, the Port Authority desires to engage Contractor to implement and maintain a comprehensive security system for the Vancouver Harbor facilities, and Contractor desires to provide such services;

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

1. DEFINITIONS

1 "Critical Systems" means the Port Authority's operational technology systems, including but not limited to SCADA networks, terminal operating systems, vessel traffic management systems, and related industrial control systems.

2 "DeepShield Platform" means Contractor's proprietary industrial cybersecurity platform and all associated software, hardware, and documentation.

3 "Services" means the security system implementation, maintenance, and monitoring services described in Exhibit A.

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

2. SCOPE OF SERVICES

1 Implementation Services. Contractor shall:

(a) Install and configure the DeepShield Platform across all designated Critical Systems

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

(c) Implement automated incident response protocols

(d) Configure maritime-specific security modules

(e) Integrate with existing Port Authority security infrastructure

2 Ongoing Services. Contractor shall provide:

(a) 24/7 security monitoring and threat detection

(b) Regular system updates and maintenance

(c) Incident response and remediation support

(d) Monthly security assessment reports

(e) Quarterly system optimization reviews

3. TERM AND TERMINATION

1 Term. This Agreement shall commence on the Effective Date and continue for an initial term of three (3) years, unless earlier terminated as provided herein.

2 Renewal. This Agreement may be renewed for additional one-year terms upon mutual written agreement of the parties.

3 Termination for Cause. Either party may terminate this Agreement upon thirty (30) days written notice in the event of a material breach by the other party that remains uncured during such notice period.

4. COMPENSATION

1 Implementation Fees. Port Authority shall pay Contractor a one-time implementation fee of CAD

2,750,000, payable as follows:

(a) 40% upon contract execution

(b) 30% upon system deployment

(c) 30% upon final acceptance

2 Annual Service Fees. Port Authority shall pay annual service fees of CAD 850,000, payable in quarterly installments.

5. SECURITY REQUIREMENTS

1 Compliance. Contractor shall comply with:

(a) Transport Canada Marine Security Regulations

(b) International Ship and Port Facility Security Code

(c) Port Authority's Security Policies and Procedures

(d) Applicable cybersecurity standards and regulations

2 Security Incidents. Contractor shall:

(a) Notify Port Authority within 30 minutes of detecting any Security Incident

(b) Provide immediate incident response support

(c) Submit detailed incident reports within 24 hours

(d) Implement necessary remediation measures

6. CONFIDENTIALITY

1 Each party shall maintain the confidentiality of all proprietary information, technical data, trade secrets, and know-how disclosed by the other party.

2 Contractor shall not disclose details of Port Authority's security infrastructure or vulnerabilities to any third party without prior written consent.

7. WARRANTIES AND LIMITATIONS

1 Contractor warrants that:

(a) Services will be performed in a professional manner

(b) DeepShield Platform will perform substantially as documented

(c) Contractor has necessary rights and licenses

2 EXCEPT AS EXPRESSLY STATED HEREIN, CONTRACTOR MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED.

8. INDEMNIFICATION

1 Contractor shall indemnify Port Authority against third-party claims arising from:

(a) Contractor's negligence or willful misconduct

(b) Infringement of intellectual property rights

(c) Breach of confidentiality obligations

9. INSURANCE

1 Contractor shall maintain:

(a) Commercial General Liability Insurance: CAD 5,000,000

(b) Professional Liability Insurance: CAD 10,000,000

(c) Cyber Liability Insurance: CAD 15,000,000

10. GENERAL PROVISIONS

1 Governing Law. This Agreement shall be governed by the laws of British Columbia.

2 Dispute Resolution. Disputes shall be resolved through mandatory mediation followed by binding arbitration in Vancouver, BC.

3 Force Majeure. Neither party shall be liable for delays caused by events beyond reasonable control.

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: February 15, 2024

VANCOUVER FRASER PORT AUTHORITY

By: _

Name: [Port Authority Signatory]

Title: [Title]

Date: February 15, 2024