TAIWAN MARITIME SECURITY IMPLEMENTATION PROTOCOL

Document No.: DSS-TW-2023-114

Effective Date: January 15, 2024

Version: 2.0

1. INTRODUCTION

1 This Taiwan Maritime Security Implementation Protocol (the "Protocol") is established by DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2100 Innovation Drive, Suite 400, Wilmington, Delaware 19801 ("DeepShield" or the "Company").

2 This Protocol governs the implementation of DeepShield's maritime cybersecurity solutions within Taiwan's territorial waters and exclusive economic zone in compliance with applicable regulations.

2. DEFINITIONS

1 "Critical Maritime Infrastructure" means ports, terminals, vessel traffic services, and associated operational technology systems within Taiwan's jurisdiction.

2 "DeepShield Maritime Platform" means the Company's proprietary OT security solution specifically configured for maritime applications, including all associated software, hardware, and monitoring systems.

3 "Local Operating Entity" means any Taiwanese entity authorized by DeepShield to implement or operate the DeepShield Maritime Platform.

3. REGULATORY COMPLIANCE

1 Implementation Standards

a) All deployments shall comply with Taiwan's Maritime and Port Bureau (MPB) cybersecurity requirements

b) Adherence to International Ship and Port Facility Security (ISPS) Code standards

c) Compliance with Taiwan's Critical Infrastructure Protection Act (CIPA)

2 Data Localization Requirements

a) Primary data centers must be located within Taiwan

b) Backup systems may be maintained internationally subject to MPB approval

c) All data transfers must comply with Taiwan Personal Data Protection Act

4. IMPLEMENTATION PROCEDURES

1 Pre-Implementation Assessment

a) Site-specific risk assessment

b) Network architecture review

c) Legacy system compatibility analysis

d) Regulatory compliance verification

2 Deployment Protocol

a) Phase I: Infrastructure preparation

b) Phase II: System installation

c) Phase III: Integration testing

d) Phase IV: Operational validation

3 Documentation Requirements

a) Technical implementation plans

b) Security assessment reports

c) Compliance certification documents

d) Training materials in Traditional Chinese

5. OPERATIONAL REQUIREMENTS

1 Security Standards

a) Multi-factor authentication for all access points

b) End-to-end encryption meeting Taiwan national standards

c) Real-time threat monitoring and response

d) Regular security audits by MPB-certified entities

2 Maintenance Procedures

a) Quarterly system updates

b) Monthly security patches

c) Annual comprehensive review

d) Emergency response protocols

6. LOCAL PARTNERSHIP REQUIREMENTS

1 DeepShield shall maintain at least one Local Operating Entity meeting the following criteria:

a) Minimum 51% Taiwanese ownership

b) MPB certification for maritime systems

c) Demonstrated cybersecurity expertise

d) Local support capabilities

2 Technology Transfer Restrictions

a) Core intellectual property remains with DeepShield

b) Local customization rights as approved

c) Source code escrow arrangements

7. LIABILITY AND INDEMNIFICATION

1 DeepShield shall maintain professional liability insurance with coverage of not less than US$10,000,000 per occurrence.

2 The Company shall indemnify Local Operating Entities against claims arising from system failures, subject to compliance with implementation procedures.

8. TERM AND TERMINATION

1 This Protocol shall remain in effect for five (5) years from the Effective Date.

2 Early termination requires 180 days' written notice and MPB approval.

9. GOVERNING LAW AND JURISDICTION

1 This Protocol shall be governed by the laws of Taiwan.

2 Any disputes shall be resolved through arbitration in Taipei under Chinese Arbitration Association rules.

10. EXECUTION

IN WITNESS WHEREOF, this Protocol is executed by DeepShield's authorized representative:

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 15, 2024

Witness:

By:

Name: Robert Kessler

Title: Chief Financial Officer

Date: January 15, 2024

[CORPORATE SEAL]