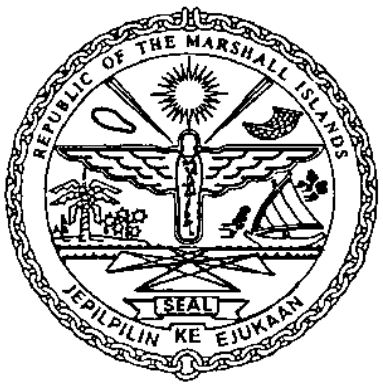
REPUBLIC OF
THE MARSHALL ISLANDS



International Ship and Port Facility Security (ISPS) Code

MARITIME ADMINISTRATOR

Feb/2022 **MN 2-011-16**

TABLE OF CONTENTS

REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-16

Rev. Feb/2022

TO: **ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS, INSPECTORS, AND RECOGNIZED SECURITY ORGANIZATIONS**

SUBJECT: **International Ship and Port Facility Security (ISPS) Code**

References:

(a) **International Ships and Port Facilities Security (ISPS) Code**, as amended

(b) **IMO Guide to Maritime Security and the ISPS Code**, 2021 Edition

(c) **SOLAS**, *International Convention for the Safety of Life at Sea (SOLAS)*, Consolidated Edition 2020

(d) **STCW including 2010 Manilla Amendments**: *STCW Convention and STCW Code: International Convention on Standards of Training, Certification and Watchkeeping for Seafarers*, 2017 Edition

(e) **IMO Circular** MSC/Circ.1097, *Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code*, dated 6 June 2003

(f) **IMO Circular** MSC.1/Circ.1154, *Guidelines on training and certification for company security officers*, dated 23 May 2005

(g) **IMO Circular** MSC.1/Circ.1190, *Guidance on the provision of information for identifying ships when transmitting ship security alerts*, dated 30 May 2006

(h) **IMO Circular** MSC.1/Circ.1193, *Guidance on voluntary self- assessment by Administrations and for ship security*, dated 30 May 2006

(i) **IMO Circular** MSC.1/Circ.1217, *Interim Guidance on voluntary self-assessment by Companies and CSOs for ship security*, dated 14 December 2006

(j) **IMO Circular** MSC.1/Circ.1283, *non-mandatory Guidelines on security aspects of the operation of ships which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code*, 22 December 2008

(k) **IMO Circular** MSC.1/Circ.1305, *Revised guidance to masters, Companies and duly authorized officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port*, dated 9 June 2009

(l) **IMO Circular** MSC-MEPC.2/Circ.9, *Guidance for the application of safety, security and environmental protection provisions to FPSOs and FSUs*, dated 25 May 2010

(m) **RMI Maritime Regulations (**MI-108**)**

(n) **RMI Requirements for Seafarer Certification**, (MI-118**)**

(o) **RMI Marine Notice** 2-011-8, *National Safety Requirements for Miscellaneous Vessels*

(p) **RMI Marine Notice** 2-011-18, *Ship Security Alert System (SSAS)*
(q) **RMI Marine Notice** 2-011-25, *Long-Range Identification and Tracking (LRIT) of Ships*
(r) **RMI Marine Notice** 2-011-35, *National Safety Requirements for Offshore Supply Vessels*
(s) **RMI Marine Notice** 2-011-39, *Piracy, Armed Robbery, and the Use of Armed Security*
(t) **RMI Marine Notice** 2-011-55, *Conducting Surveys and Issuing International Convention and National Certificates for Private Yachts*
(u) **RMI Marine Notice** 7-047-2, *Approval of Maritime Training Centers, Courses and Programs*
(v) **RMI Marine Guideline** 2-11-14, *Maritime Security off the Coast of West Africa, including the Gulf of Guinea*
(w) **RMI Marine Guideline** 2-11-16, *Maritime Cyber Risk Management*
(x) **RMI Marine Guideline** 7-41-5, *Stowaways: Prevention of Unauthorized Access and Case Resolution*

PURPOSE

This Marine Notice provides the Republic of the Marshall Islands (RMI) Maritime Administrator's (the "Administrator") requirements, policies, and interpretations for complying with the International Ship and Port Facility Security (ISPS) Code.

This Notice supersedes Rev. Mar/2020. It has been substantially revised and eliminates repetitions of the ISPS Code and is redesigned to highlight the Administrator's requirements.

BACKGROUND

The ISPS Code entered into force under SOLAS chapter XI-2 on 1 July 2004. Since then, it has formed the basis for a comprehensive mandatory security regime for international shipping. The Code is divided into two sections, Part A and Part B.

Mandatory Part A outlines detailed maritime and port security-related requirements to which SOLAS contracting governments, port authorities, and shipping companies must adhere to comply with the Code.

Part B of the Code provides guidelines on how to meet the requirements and obligations set out in the provisions of Part A.

APPLICABILITY

The ISPS Code applies to RMI-flagged ships as follows:

- passenger ships, including high-speed passenger craft;
- cargo ships, including high-speed craft and yachts engaged in trade, of 500 gross tonnage and upwards;
- Special Purpose Ships of 500 gross tonnage and upwards;
- self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location.

It does not apply to RMI-flagged:

- cargo ships, including commercial yachts of less than 500 gross tonnage, voluntary compliance as of 1 July 2006;
- ships not propelled by mechanical means;
- private pleasure yachts not engaged in trade;
- fishing vessels;
- non-self-propelled mobile offshore drilling units, nor to mobile offshore drilling units of any description while on location, making field moves, or in port.
- mobile and immobile floating production, storage and offloading units (FPSOs) and floating storage units (FSUs), floating production units (FPUs), moored oil storage tankers (MOSTs) and mobile offshore units (MOUs) but should have some security procedures in place; and
- single buoy moorings (SBMs) attached to an offshore facility that are covered by the facility's security regime, or if connected to a port facility, covered by the port facility security plan (PFSP).

DEFINITIONS

This Marine Notice uses the definitions of the ISPS Code and SOLAS, unless otherwise provided below.

Failure means the non-fulfilment of a specified requirement that does not compromise the ship's ability to operate at security levels 1, 2 and 3. It may also be referred to as a minor deviation.

Major Failure means the non-fulfilment of a specified requirement that compromises the ship's ability to operate at security levels 1, 2 or 3.

Observation means a statement of fact made during a verification audit and substantiated by objective evidence. It may also be a statement made by the auditor referring to the SSP which, if not corrected, may lead to a Failure in the future.

Security Incident means any suspicious act or circumstance threatening the security of a ship, including mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity to which the ISPS Code applies.

Security Drills and Exercises[1]
Drills shall test individual elements of the SSP such as those listed in the ISPS Code, Part B, §8.9. Exercises shall test the connectivity, communications and cooperation among all parties that may be involved in a security incident.

REQUIREMENTS

1.0 Compliance

1.1 ISPS Code Compliance

.1 All ships to which the ISPS Code applies must comply with Part A, as it is mandatory under SOLAS chapter XI-2.

.2 ISPS Code Part B provides guidance. Some Coastal States make mandatory security provisions of Part B. All RMI-flagged ships that enter the jurisdiction of these States are required to comply with these requirements, including any additional regional or local mandates within such coastal States. RMI-flagged ships must take into account the relevant guidance in Part B, §8.1 to §13.8, and the *IMO Guide to Maritime Security and the ISPS Code, 2021 Edition*.

1.2 SOLAS Chapter XI-2 Compliance

Ships operated by Companies that fail to maintain compliance with the ISPS Code will be considered in violation of SOLAS and may be prevented from trading.

1. MI-108, §7.41.8a.

.1 The ship's Master or Company Security Officer (CSO) must immediately advise the Administrator upon becoming aware that the ship is not compliant with the established security levels.

.2 Details must be provided through the Recognized Security Organization (RSO) that include corrective action, temporary alternative arrangements, and current status.

1.3 Safety Management System (SMS)

.1 The ISPS requirements of this Notice are not exhaustive. They must be read along with RMI Marine Notice 2-011-13, with particular attention paid to Cyber Risk Management and Emergency Preparedness.

.2 The Administrator considers the ISPS Code to be an extension of the ISM Code. A Company may incorporate additional items in its SMS based on regional or coastal State particulars, provided they are consistent with international and RMI national security requirements.

1.4 Voluntary Compliance

Vessels not subject to mandatory compliance with the ISPS Code may do so voluntarily[2]. This includes cargo ships, yachts[3] and Offshore Support Vessels[4] engaged in trade less than 500 gross tonnage. Evidence of voluntary compliance is recognized by the Administrator if it is verified and certified by an RSO.

1.5 Mobile and Immobile Floating Units and FPSOs/FSUs

When mobile and immobile Floating Units are engaged in periodic short voyages between a platform and the coastal State, these units are not considered to be ships engaged on an international voyage. Security in territorial waters is the responsibility of the applicable coastal State, though they may take any ISPS Code objectives into consideration. For guidance on applying the ISPS Code to the interaction between FPSOs/FSUs see MSC-MEPC.2/Circ.9.

2.0 Responsibilities and Authority

2.1 Company Obligations

.1 The Company must appoint a CSO for each of its ships. A ship may have only one CSO. However, 'Alternate' or 'Deputy' CSOs may be appointed for different geographical areas or groups of ships within a fleet to reduce the potential for single point failure. Where this is the case, the ship security plan

2. The concept of voluntary compliance is that this is optional. Voluntary compliance may be established using IMO guidance. See MSC.1/Circ.1193, MSC.1/Circ.1217, or MSC.1/Circ.1283
3. See MN 2-011-55, §1.2 and §1.3.
4. See also MN 2-011-8, §7 and MN 2-011-35, §8.

(SSP) must clearly identify who is responsible for which ships in the fleet.

.2 The CSO must be an internal employee of the Company and must assume all duties and responsibilities required by the ISPS Code (Part A, §11.2) Entrusting this function to a third party is not acceptable to the Administrator.

.3 To enable direct and immediate contact between the Administrator and the CSO, the Company must provide the Administrator with the CSO particulars:

a. using the MI-101 series, *Application for Registration,* when registering the vessel; or

b. use form MI-297B, *Combined Declaration Form,* whenever changing the CSO.

.4 These forms must be submitted to an Administrator Regional Office for processing.

2.2 Company Security Officer

.1 The CSO must ensure that a Ship Security Assessment (SSA) is drawn up by persons with the appropriate skills[5] to evaluate terrorism, piracy, and armed robbery risks, and that a trained and qualified Ship Security Officer (SSO) has been appointed to each ship.

.2 Companies must ensure that CSOs are trained as required by ISPS Code Part A, Section 13.1 and demonstrate the competencies listed in the Annex of IMO MSC.1/Circ.1154. The Administrator recognizes all CSO training courses that are based on IMO Model Course 3.20.

.3 The CSO must arrange internal[6] security audits onboard each ship in accordance with ISPS Code Part A, §11.2.5 and §19.4.2.4.2 as part of their duties.

2.3 Ship Security Officer

To be designated as an SSO by the Company, the individual must hold the applicable STCW and RMI certifications. See §5.0 of this Notice.

2.4 Master's Responsibility and Authority

.1 The Master has overriding authority and responsibility to make decisions with respect to the safety and security of the ship. This must not be relinquished to anyone, per MI-108, §7.41.16. The Master may request assistance of the Company, any Contracting Government, or any recognized authority.

5. See §5 of this Notice.
6. Once every 12 months, see also IACS Procedural Requirements 24.

.2 Every vessel Master must make an official log book entry for stowaway and contraband searches, which must be conducted prior to the vessel's departure from each port in accordance with MI-108, §7.41.2f (14).

3.0 Security Level and Declaration of Security

3.1 Setting of the Security Level

.1 A ship must operate at the security level established by the port facility, which is typically based on the level set by the Port State.

.2 If a security level has not been set by the Port State, there still may be a need for enhanced security measures due to reported threats in the area. Refer to the Administrator's Maritime Security webpage for current security level guidance.

.3 Security measures equivalent to a higher security level may be implemented if a ship deems it necessary to operate at a higher security level than the port.

3.2 Declaration of Security

.1 A Declaration of Security (DoS) must state the security activities for which the facility and ship are responsible during ship-to-ship or ship-to-facility interfaces. They must be kept for at least the last 10 calls at port facilities, as part of the vessel's record keeping. A DoS must be completed as follows:

Maritime Security Levels	DoS Use
Security Level 1	Discretionary with the Master and the SSO
Security Levels 2 and 3 (High-risk ports)	Mandatory for ships and facilities
Ports not compliant with the ISPS Code	Mandatory for ships to keep a detailed log of security measures implemented while at port.
Any time upon request	When deemed necessary by the Administrator, a Contracting Government, CSO, or SSO

.2 The Administrator allows the use of a single DoS to cover frequent calls at the same port facility provided that:

a. the DoS is valid for the same security level;

b. the effective period at security level 1 does not exceed 90 days; and

c. the effective period at security level 2 does not exceed 30 days.

.3 A new DoS must be signed and implemented whenever the security level increases.

.4 Where ships need to complete a DoS, contact information of the authority responsible for ship and port facility security is provided in the Global Integrated Shipping Information System[7], Maritime Security module.

4.0 Ship Security Plan

4.1 A Ship Security Plan (SSP) must be developed, implemented, and maintained onboard each vessel to which the ISPS Code applies. The SSP must address:

.1 unlawful acts threatening the safety of the ship and the security of its passengers and crew based on a security risk assessment.

.2 countermeasures to protect against terrorism, piracy, and armed robbery when operating in high-risk areas. See MN 2-011-39.

.3 the Master's overriding authority to make decisions relating to ship safety and security.

4.2 The SSP must be reviewed and approved by the Administrator or an RMI-authorized RSO. Subsequent amendments to the SSP that are related to the requirements of ISPS Code Part A, §9.4.1 to §9.4.18, must also be reviewed and approved. The implementation of the SSP, including amendments, must be verified by the Administrator or RSO during an onboard attendance.

4.3 The SSO must review the SSA and the SSP in conjunction with an on-scene security survey at intervals not exceeding 12 months. The SSP must be amended if inadequacies are identified during this annual review. Additional ship security risks may also be identified during trainings, exercises, drills, or following a security incident.

7. Registration is free.

5.0 Training and Certification

Security-Related Training	Training Requirement[8]	Certification Requirement
All persons employed or engaged on a ship which is required to comply with the ISPS Code, other than passengers, must receive **security-related familiarization** training before being assigned to shipboard duties.	MI-108 §7.41.12 a; MI-118 §5.23.1.1; and STCW Code Section A-VI/6, and B-VI/6	None
Security awareness training for seafarers as part of the ship's complement without designated security duties prior to being assigned shipboard duties.	MI-118, §5.23.1.2	MI-118, §5.22 and §5.23.2; STCW Convention Regulation VI/5, VI/6; and STCW Code Section A-VI/5, A-VI/6
Designated security duties training for shipboard personnel with duties and responsibilities under the SSP	MI-118, §5.23.1.3	
SSO	MI-118, §5.22.2	
CSO	ISPS Code Part A, §13.1	IMO Model Course 3.20; and MSC.1/Circ.1154
Appropriate shore-based personnel having specific security duties and responsibilities		None

8. See MN 7-047-2 on the use of RMI approved or recognized Maritime Training Institutions, Programs, and Courses.

6.0 Security Drills and Exercises

6.1 Annual Program

The Master must ensure security drills are carried out as per MI-108, §7.41.8.

6.2 Company Security Exercises

.1 As provided by ISPS Code A, §13.5, a Company's shore-based management and CSOs responsible for a ship's security incident response must participate in exercises.

.2 The Company may invite the Administrator, PFSO, coastal state authorities and other stakeholder to participate in a security exercise.

.3 A security exercise may be held with others such as search and rescue or emergency response scenarios.

.4 Exercises must involve at least one ship of a Company's fleet but are not required to involve each ship within a fleet. The ship(s) may be RMI or non-RMI flagged.

a. Operators of large fleets with various trading patterns and port activities must include representative ships in exercises. Operators may want to consider including additional vessels when conducting an exercise to allow more officers to gain direct experience and training.

b. The Administrator will accept a real security incident involving one of the Company's vessels (including non-RMI flagged) as meeting the exercise requirement as long as the security incident is reported to the Administrator per § 7.0 of this Notice.

c. The results and lessons learned during each exercise or incident must be distributed to the RMI-flagged vessels in the Company's fleet.

6.3 Frequencies

The drills and exercises must be conducted as follows:

Security Drill or Exercise	Frequency
Ship security drills (ISPS Code Part B, §13.6; and MI-108 §7.41.8b.)	In cases where more than 25% of the ship's personnel have changed, at any one time, with personnel that have not previously participated in any drill on that ship within the last three months, then a drill must be conducted within **1 week** of the change.
	Drills must be conducted at least once **every 3 months**.
Company security exercises (ISPS Code Part B, §13.7; and MI-108 §7.41.8c.)	Exercises shall be carried out at least **once each calendar year** with no more than **18 months** between the exercises.

7.0 Security Incident Reporting

Security incidents must be reported in accordance with: MN 2-011-39 and MG 2-11-14 (Form MI-109-2); MG 2-11-16 (Form MI-109-5); or MG 7-41-5 (Form MI-109-3).

8.0 Security Equipment and Systems

Security equipment specified in the SSP must always remain operational.

8.1 Major Failure

.1 Any Major Failure must be reported immediately to:

a. the Administrator or RSO, or both;

b. the Port Facility Security Officer (PFSO); and

c. the competent authorities of any relevant coastal State(s).

.2 An ISSC shall not be issued or endorsed if a Major Failure exists. Immediate action is required to restore compliance and the Major Failure must be downgraded before departure. An additional verification audit must be carried out within an agreed period to verify effective implementation of corrective actions.

8.2 Failure

.1 Any Failure must be reported without delay to:

a. the Administrator; or

b. the RSO

.2 The report must include:

a. details of equivalent alternative security measures the ship is applying until the failure or suspension is rectified; and

b. an action plan specifying the timing of any repair or replacement

.3 If a Failure is identified, the ISSC may be endorsed, provided compliance has been restored prior to departure or a schedule has been agreed between the Company and the auditor for the completion of corrective action to restore compliance and to prevent recurrence. Additional audits may be carried out as necessary.

8.3 Equipment testing

System	Testing requirements
Ship Security Alert System (SSAS)	Following initial installation of the SSAS, per RMI MN 2-011-18, §3.1
	Upon the transfer of flag to RMI, per MSC.1/Circ.1190 Annex, §6
Long-Range Identification and Tracking (LRIT)	The conditions that would trigger LRIT Conformance Testing (SOLAS chapter V, regulation 19-1) are detailed in MN 2-011-25. The responsibility for maintaining LRIT equipment falls under the control of the CSO.

9.0 Documentation

9.1 The SSP must remain strictly confidential. Port State Control Officers are not permitted to access the plan. Only RMI qualified maritime security auditors or trained RSO auditors that certify the ship are granted access to the plan.

9.2 Security records must be maintained on board for three years.

10.0 Recognized Security Organizations

10.1 The Administrator or an RMI-authorized RSO[9] may be selected by the Company for security services including:

.1 SSP review and approval;

.2 verification; and

.3 ISSC issuance.

10.2 The selected RSO may not provide consultative services per ISPS Code Part A, §9.2.1.

11.0 Verifications

11.1 Initial, renewal, and intermediate verifications must be conducted as required by ISPS Code Part A, §19.

11.2 The entity that has provided ISPS Code certification must be consulted if changes are made to security systems, equipment, or the approved SSP.

11.3 A ship detained on maritime security grounds must undergo an additional verification before being allowed to sail.

9. See MG 2-11-15.

12.0 International Ship Security Certificate

12.1 Only the Administrator or an RMI-authorized RSO may issue the ISSC.

12.2 An ISSC may not be reissued in case of:

.1 Major Failures; or

.2 Failures or Minor Deviations

12.3 Failures or minor deviations from the SSP must be resolved before the ISSC issuance, even if they do not compromise the ship's ability to operate at any security level (see MSC/Circ.1097). Unresolved deviations will invalidate the ISSC.

13.0 Port Facility

13.1 The SSO will be the primary contact with the Port Facility for coordinating security related activities.

13.2 The PFSO will normally advise of any change in the port facility's security level and provide relevant security information and instructions.

13.3 Ships operating at ports and port facilities considered non-compliant with the ISPS Code must establish protective security measures by:

.1 implementing measures per the ship's security plan equivalent to security level 2 or higher;

.2 ensuring all access points to the ship are guarded;

.3 attempting to execute a Declaration of Security; and

.4 logging all implemented security measures for potential review by authorities at future port calls

13.4 If a PFSC refuses to complete a DoS or demands the ship operate at a lower security level than the port facility, then the ship must maintain the higher security measures while still allowing for continued cargo operations. The DoS proposed by the SSO must be retained and the incident properly logged.