The Republic of Palau
Palau International Ship Registry
"The Reliable Flag to Prosperity"

MARINE NOTICE 12-024 –PROVISION AND INSTALLATION OF SHIP SECURITY EQUIPMENT

To: ALL SHIPOWNERS, MANAGERS, MASTERS, REGISTRATION OFFICERS AND RECOGNIZED ORGANIZATION

Subject: PROVISION AND INSTALLATION OF SHIP SECURITY EQUIPMENT

1. Purpose

1.1 To provide specific guidelines on the implementation of security measures in accordance with SOLAS, 1974, as amended, specifically:

1.1.1 Regulation V/19 concerning Carriage Requirement for Shipborne Navigational Systems and Equipment for Automatic Identification System;

1.1.2 Regulation XI-1/3 on Ship Identification Number; and,

1.1.3 Regulation XI-2/6 on the provision of Ship Security Alert System.

1.2 To enhance maritime safety and security onboard ships registered under the Palau Flag.

2. Applicability

2.1 This Marine Notice is applicable to all vessels registered that are engaged on international voyages

3. Ship Security Alert System (SSAS)

3.1 All ships covered by this Circular shall be provided with a ship security alert system in accordance with the provisions of Regulation XI-2/6 of SOLAS 1974.

3.2 The ship security alert system, when activated shall:

3.2.1 initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration and to the company operating the ship, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;

3.2.2 not send the ship security alert to any other ships;

3.2.3 not raise any alarm on-board the ship; and

3.2.4 continue the ship security alert until deactivated and/or reset.

3.3 The ship security alert system shall:

3.3.1 be capable of being activated from the navigation bridge and in at least one other location; and

3.3.2 conform to performance standards not inferior to those adopted by the IMO.

3.4 The ship security alert system activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert.

3.5 The requirement for a ship security alert system may be complied with by using the radio installation fitted for compliance with the requirements of Chapter IV on Radio communications of SOLAS 1974 as amended, provided all requirements of this Circular are complied with.

1. Definitions

1.1 "Convention" means the International Convention for the Safety of Life at Sea, 1974 as amended.

1.2 "Contracting Government" means a government signatory to SOLAS but used more specifically to mean port State (country) receiving a ship at a port facility.

1.3 "Company" means the owner of the ship or any other organization or person such as the Manager, or the Bareboat Charterer, who has assumed the responsibility for operation of the ship from the ship owner and who on assuming such responsibility has agreed to do so in writing. This definition is the same as that found in the ISM Code and is applied in like manner.

1.4 "Ship Security Assessment" (SSA) means the identification of the possible threats to key shipboard operations, existing security measures and weaknesses in the infrastructure, policies and procedures.

1.5 "Ship Security Plan" (SSP) means a plan developed to ensure the application of measures onboard the ship designed to protect persons onboard, the cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

1.6 "Ship Security Officer" (SSO) means the person on board the ship accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the SSP and for the liaison with the Company Security Officer (CSO) and the Port Facility Security Officer (PFSO).

1.7 "Company Security Officer" (CSO) means the person ashore designated by the Company to develop and revise the SSP and for liaison with the SSO, PFSO and the Administrator.

1.8 "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.

1.9 "Security Level" means the qualification of the degree of risk that a security incident will be attempted or will occur.

1.10 "Security Level 1" means the level for which minimum appropriate protective and preventive security measures shall be maintained at all times.

1.11 "Security Level 2" means the level for which appropriate additional protective and preventive measures shall be maintained for a period of time as a result of heightened risk of a security incident.

1.12 "Security Level 3" means the level of which further specific protective and preventive measures shall be maintained for a period of time when a security incident is probable or imminent (although it may not be possible to identify the specific target).

1.13 "Short Voyage" means an international voyage in the course of which a ship is not more than 200 miles from a port or place in which a ship, the passengers and crew could be placed in safety. Neither the distance between the last port of call in the country in which the voyage begins and the final port of destination nor the return voyage shall exceed 600 miles. The final port of destination is the last port of call in the scheduled voyage at which the ship commences its return voyage to the country in which the voyage began.

1.14 "Port Facility Security Officer" (PFSO) means the person at the port facility designated by the facility to be responsible for implementation of measures required by the ISPS Code.

2. Compliance

2.1 In accordance with SOLAS 74 Chapter XI-2, Regulation 4, ships not in compliance with SOLAS or the ISPS Code or unable to comply with established security levels must notify the Administrator prior to conducting any ship/port interface or port entry. This means that at the moment a ship's Master or a Company Security Officer (CSO) becomes aware that a ship is not compliant or cannot maintain compliance, the Administrator is to be immediately advised, with details including corrective action, temporary alternative arrangements and current status.

3. SOLAS Chapter, XI-2, Regulation 9, "Control and Compliance Measures"

3.1 Details

3.1.1 This regulation is unique in that it addresses in a comprehensive manner port State actions that may be taken concerning a ship either in port or intending to enter the port of a Contracting Government. Port State control of ships is intended to be limited to verifying that there is a valid International Ship Security Certificate (ISSC) on

board unless there are "clear grounds" for believing the ship is not in compliance with SOLAS XI-2 or the ISPS Code. "Clear grounds" is not explicitly defined. However, paragraphs 4.29 through 4.44 of Part B of the ISPS Code provide some insight, but are not definitive.

3.2 Republic of Palau Requirements for Compliance

3.2.1 Any port State action taken upon an Republic of Palau flagged vessel by a Contracting Government or its Designated Authority is to be immediately reported by the ship's Master or the CSO to the Administrator as the Competent Authority and the RSO by whom the ship's ISSC was issued.

3.2.2 If there are "clear grounds" to believe that the ship is not in compliance with the requirements of Chapter XI-2 or Part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the SSP, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Administrator or the Master of the ship concerned.

4. SOLAS Chapter, XI-2, Regulation 12, "Equivalent Security Arrangements"

4.1 Details

4.1.1 Similar to other authorities in SOLAS, this regulation provides the mechanism for the consideration of arrangements and systems in lieu of those specifically prescribed by regulation or the Code.

4.2 Republic of Palau Requirements for Compliance

4.2.1 Equivalent Security Arrangements should only be undertaken in exceptional and unique circumstances. Owners and operators are cautioned that specific approval must be obtained from the Administrator prior to the use, installation or activation of any systems or services intended to serve as an equivalent to those prescribed by SOLAS XI-2.

5. ISPS Code

5.1 Objectives: The Objectives of the ISPS Code are:

5.1.1 to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security threats or incidents affecting ships or port facilities used in international trade;

5.1.2 to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries at the national and international level for ensuring maritime security;

5.1.3 to ensure the early and efficient collection and exchange of security-related information;

5.1.4 to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels and situations; and

5.1.5 to ensure confidence that adequate and proportionate maritime security measures are in place.

6. Requirements of the ISPS Code: Functional Requirements

6.1 gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments or authorities;

6.2 requiring the maintenance of communication protocols for ships and port facilities;

6.3 preventing unauthorized access to ships, port facilities and their restricted areas;

6.4 preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

6.5 providing means for raising the alarm in reaction to security threats or security incidents;

6.6 requiring ship and port facility security plans based upon security assessments; and

6.7 requiring training, drills and exercises to ensure familiarity with security plans and procedures.

7. Mobile and Immobile Floating Units

7.1 When engaged in periodic short voyages between a platform and the coastal State, these units are not considered to be ships engaged on international voyage. Security in territorial waters is the responsibility of the applicable coastal State, though they may take any onboard security as required by section 3.1 above into consideration.

8. Mandatory Compliance

8.1 Regulation 4 of Chapter XI-2

This regulation made the ISPS Code mandatory for ships affected as of 1 July 2004. The Code is made up of two (2) parts. Part A is the mandatory portion of the Code, and Part B is the portion that is recommendatory in nature. Part B was crafted to provide guidance and information concerning how to implement Part A. It was designed this way to take into account the need to continue to expand and develop guidance on a periodic basis without the need to go through time consuming convention amendment procedures.

11.1.2 Owners and operators should note that section 9.4 of Part A, as clarified by MSC/Circ.1097 dated 6 June 2003, requires that in order for an ISSC to be issued, the relevant guidance in Part B paragraphs 8.1 to 13.8 must be taken into account.

9. International Safety Management (ISM) Code

9.1 The Administrator considers the ISPS Code has been and will continue to be an extension of the International Safety Management (ISM) Code and an integral part of emergency preparedness and compliance with international conventions in a Company's Safety Management System.

9.2 If a vessel Flagged under the Republic of Palau fails to comply with the ISPS Code has been and will continue to be considered a major non-conformity as defined in the ISM Code, resulting in the immediate withdrawal of the vessel's Safety Management Certificate (SMC) and ISSC, which will effectively prevent the ship from trading.

9.3 Reinstatement of certification shall not occur until the vessel's RSO and, if the situation warrants, the Contracting Government or its Designated Authority of the coastal State under whose jurisdiction the vessel is located are able to advise the Administrator that they are satisfied with the vessel's compliance with the ISPS Code.

10. Recognized Organizations

10.1 The Administrator, utilizing the MSC guidelines that it helped to formulate and the authority provided in the ISPS Code, has carefully chosen, certain Recognized Organizations (ROs) to be authorized Recognized Security Organizations (RSOs) and has delegated to them by written agreement specific security related duties under Chapter XI-2.

10.2 The RSOs shall also review and approve all amendments to the approved SSP. Those amendments, which significantly alter or change the security management system on board, shall be subject to a re-verification audit by the RSO.

10.3 Companies may choose from any of the Palau Flag Administration's authorized RSOs to conduct SSP review and approval, verification audits, and to issue the ISSC and SSP amendment approval, provided that the selected RSO has not provided consultative services with regard to preparation of the SSA.

11. Declaration of Security

11.1 A Declaration of Security (DoS) provides a means for ensuring that critical security concerns are properly addressed prior to and during a vessel-to-facility or vessel-to-vessel interface. The DoS addresses security by delineating responsibilities for security arrangements and procedures between a vessel and a facility. DoSs shall be completed at anytime the Administrator, a Contracting Government, PFSO, CSO or SSO deems it necessary.

11.2 Use of a DoS at Republic of Palau Security Level 1 is discretionary with the Master and the SSO. At Maritime Security Levels 2 and 3, all vessels and facilities shall complete the Declaration of Security.

11.3 All Declarations of Security shall state the security activities for which the facility and vessel are responsible during vessel-to-vessel or vessel-to-facility interfaces. DoSs must be kept as part of the vessel's record keeping.

12. Obligations of the Company

12.1 Every Company shall develop, implement, and maintain a functional SSP aboard its ships that is compliant with SOLAS Chapter XI-2 and the ISPS Code.

12.2 In accordance with SOLAS Chapter, XI-2, Regulation 8, the Company shall ensure that the SSP contains a clear statement emphasizing the Master's authority and that the Master has overriding authority and responsibility to make decisions with respect to the safety and security of the ship which shall not be relinquished to anyone and to request assistance of the Company or of any Contracting Government or any recognized authority as may be necessary. There is to be no question but that the Master of the vessel has the ultimate responsibility for both safety and security aboard ship. This has been made very clear in the Code in both Parts A and B.

12.3 The Company shall ensure that the Master has available on board, at all times, the following information required by SOLAS Chapter XI-2, Regulation 5, to provide to coastal State authorities:

12.3.1 The person or entity responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;

12.3.2 The person or entity responsible for deciding the employment of that ship; and

12.3.3 In cases where the ship is employed under the terms of charter party(ies), who the parties to such charter party(ies) are.

13. Ship Security Assessment

13.1 The CSO is responsible for satisfactory development of the SSA whether prepared by the company itself or a contracted organization. The SSA serves as a tool for development of a realistic SSP. It takes into account the unique operating environment of each individual ship, the ship's compliment and duties, structural configuration and security enhancements.

13.2 Accordingly, the CSO shall ensure that the SSA addresses at least those elements for an SSA as detailed in Part B, Section 8, of the Code, the conditions of operation of the vessel and internationally recognized best management practices to avoid, deter or delay acts of terrorism, piracy and armed robbery. Due to the potentially sensitive operational and security information contained therein, the SSA shall be protected from unauthorized disclosure.

13.3 The SSA shall be sent, together with the SSP, to the RSO by a predetermined method to prevent unauthorized disclosure. The RSO shall review the SSA to ensure that each element required by the Code is satisfactorily addressed and is used as a reference for the SSP.

14. Ship Security Plan

14.1 The CSO is responsible for satisfactory development of the SSP whether prepared by the Company itself or a contracted organization. The SSP is developed from the information compiled in the SSA. It ensures application of measures onboard the ship designed to protect persons onboard, the cargo, cargo transport units, ship's stores or the ship from all manner of risks of security violations. Because of the potentially sensitive operational information contained therein, the SSP shall be protected from unauthorized disclosure.

14.2 The CSO shall ensure that the SSP addresses in detail those elements for an SSP as detailed in Part B, Section 9, of the Code, especially those vulnerabilities found during the assessment with a description of countermeasures and best management practices that address those vulnerabilities.

14.3 At completion of a new or substantially revised SSP, and approval by the Company, the CSO shall send the SSP, together with the SSA, for approval by the RSO by a predetermined method to prevent unauthorized disclosure.

15. Best Management Practices (BMP)

15.1 When addressing ways to avoid, deter or delay acts of terrorism, piracy and armed robbery, BMPs have been decided, organized and promulgated by members of the United Nations Contact Industry Working Group. They have also been sanctioned by the IMO Maritime Safety Committee (MSC) and provided in MSC.1/Circ.623. They are also reflected in the "Advice to Masters" section within www.MSCHOA.eu, and a PDF copy of the document is available for unrestricted download on the "Piracy Alert" section of www.icc-ccs.org . The BMPs are not mandatory requirements, but are guidelines to be considered by a ship owner/operator in producing or revising an SSP.

15.2 Thus, while every BMP does not have to be included in an SSP, the Administrator does expect a shipowner/operator to give full consideration to all of the BMPs and utilize those that make sense (based on security risk assessment) for the ship's operations. It should also be noted that these BMPs are not an exclusive list, but are those identified thus far and supported by the Administrator and the MSC. From the Administrator's perspective, the important point is that the shipowner/operator has a well-thought-out plan in place and documented in the SSP.

16. Company Security Officer (CSO)

16.1 The Company shall appoint a CSO for each ship in its fleet.

16.2 The Company shall provide the Administrator with the full name of the CSO and information to enable direct and immediate contact at all times between the Administrator and the CSO with regard to matters related to the ISPS Code.

16.3 A Company may not use a contract third party as CSO. By definition, the Company has stated in writing its obligations with respect to any vessel. The CSO is considered to be a part of that Company and is required to protect the integrity of its SSPs. Entrusting this function to a third party is not considered acceptable to the Administrator in this regard.

16.4 The CSO shall ensure that an approved SSP is placed onboard the named ship and that the SSO and crew are familiar with its contents. The CSO shall ensure that each vessel for which he or she is responsible is appointed a trained and qualified SSO.

17. Ship Security Officer (SSO)

17.1 The SSO is the person designated by the CSO to perform the duties and responsibilities detailed in Part A, Section 12 and Part B, Sections 8, 9 and 13. The SSO shall have the knowledge of, and receive formal training in the elements of Part B, Section 13.1, and specific Company training in the elements of Part B, Section 13.2, of the Code.

17.2 The SSO shall be a management level officer. There may be need for more than one (1) SSO to be assigned per ship by the CSO, the number required being determined by the CSO through the SSA process giving due consideration to the requirements of minimum safe manning, the nature of ship operations and compliance with rest hour requirements established by the STCW Convention, 1978, as amended.

18. Training and Certification

18.1 Company and shipboard personnel having specific security duties must have sufficient knowledge, ability and resources to perform their assigned duties per Part B, Section 13.1, 13.2, and 13.3.

18.2 All other shipboard personnel must have sufficient knowledge of and be familiar with relevant provisions of the SSP including the elements described in Part B, Section 13.4.

19. Drills and Exercises

19.1 The objective of security drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and to identify and address security-related deficiencies encountered during such drills and exercises.

19.2 Exercises may be varied including participation of CSOs, PFSOs, relevant authorities of Contracting Governments as well as SSOs. These exercises should test communications, coordination, resource availability, and response.

19.3 The SSP shall address drill and training frequency. Drills shall be conducted at least every three (3) months. In cases where more than 25% of the ship's personnel have changed, at any one time, with personnel previously not participating in any drill on that ship within the last three (3) months, a drill shall be conducted within one (1) week of the change. Exercises shall be carried out at least once each calendar year with no more than 18 months between the exercises.

20. SSP Onboard Verification Audits for Issuance of the ISSC

20.1 Each ship to which the ISPS Code applies shall be subject to an initial verification audit before the ship is put in service or before an ISSC is issued for the first time; a renewal verification at intervals specified by the Administrator, but not more than five (5) years; and at least one (1) intermediate verification.

20.2 Verification audits for issuing, endorsing or renewing the ISSC shall be performed by RSOs on behalf of the Administrator.

20.3 If the auditor identifies, through objective evidence, non-compliance with the approved SSP, this shall be communicated to the Company, the Administrator and the organization that approved the SSP. In such cases an ISSC shall not be issued until it can be shown that the security system, and any associated security and surveillance equipment of the ship, is in all respects, satisfactory and that the ship complies with the applicable requirements of Chapter XI-2 and ISPS Code Part A and B, as applicable.

20.4 Intermediate verification audits shall take place between the second and third anniversary dates of an ISSC issued for five (5) years. Should the Company chose to harmonize the ISSC cycle with the ship's SMC cycle, the Initial ISSC may be issued for a shorter period. If that period is three (3) years or less, the Intermediate verification audit shall not be required.

20.5 Renewal verification audits shall take place at intervals not to exceed five (5) years and should be carried out within the three (3) month window prior to the expiry date of the certificate. If the Renewal verification audit is carried out more than three (3) months prior to the expiry date, the new certificate shall be issued from the completion date of the Renewal verification audit.

20.6 Additional ship verification audits may be carried out at any time by the RSO on behalf of the Administrator. A ship detained on maritime security grounds shall be required to undergo an additional audit by the RSO before being allowed to sail, as is currently the case for detentions stemming from non-compliance with the ISM Code because it is still an ISM Code issue. However, the nature and extent of the non-compliance will determine extent that re-verification of the SSP would be necessary.

21. International Ship Security Certificate (ISSC)

21.1 The International Ship Security Certificate (ISSC) shall be issued by the RSO after the ship has successfully completed an Initial or Renewal verification audit in compliance with the applicable requirements of Chapter XI-2 and ISPS Code Parts A and relevant provisions of Part B. The original ISSC must remain onboard the vessel.

21.2 Certificates shall not be issued in cases where minor deviations from the approved plan or the requirements of SOLAS Chapter XI-2 and Parts A and relevant provisions of Part B of the Code exist, even if these deviations do not compromise the ship's ability to operate at security levels 1, 2 and 3.

21.3 The ISSC shall normally be valid for a period of five (5) years or a period specified by the Administrator from the date of the Initial Verification Audit and be subject to an Intermediate Audit between the second and third anniversary date.

22. Failures of Security Equipment/Systems or Suspension of Security Measures

22.1 Any failure of security equipment or systems, or suspension of a security measure that does not compromise the ship's ability to operate at security levels 1, 2 or 3 shall be reported without delay to the Administrator or the ship's RSO with details of equivalent alternative security measures the ship is applying until the failure or suspension is rectified together with an action plan specifying the timing of any repair or replacement.

22.2 The Administrator or the ship's RSO, on instructions from the Administrator, shall withdraw or suspend the ISSC if the alternative security measures are not, in fact, in place, or if an approved action plan has not been complied with.

23. Interim ISSC Certificate

23.1 An Interim ISSC shall be issued by the RSO on behalf of the Administrator for a period of not longer than six (6) months for the purposes of

23.1.1 a ship without a Certificate, on delivery or prior to its entry or re-entry into service;

23.1.2 the transfer of a ship from the flag of a Contracting Government to the Republic of Palau

23.1.3 a Company assuming the responsibility for the operation of a ship not previously operated by that Company.

23.2 A ship that has obtained an Interim ISSC shall undergo an Initial Audit within the period of its validity after implementing the system onboard for not less than two (2) months.

23.3 A subsequent consecutive Interim ISSC shall not be issued to a ship if, in the judgment of the Administrator or the RSO, the purpose of requesting such Certificate by the ship or Company is to avoid compliance with the ISPS Code beyond the period of the initial issue of an Interim Certificate.

24. Contact

24.1 In order to obtain further information, contact information is provided below:

The Palau International Ship Registry
Department: Maritime Safety and Environment Protection
PIC: Mrs. Marisabel Arauz Park
Email: technical@palaushipregistry.com
Tel: 281-876-9533
Fax: 281-876-9534