TUVALU SHIP REGISTRY

Singapore Operations Office:
10 Anson Road #25-16, International Plaza, Singapore 079903
Tel: (65) 6224 2345 Fax: (65) 6227 2345
Email: info@tvship.com Website: www.tvship.com

MARINE CIRCULAR

MC-2/2010/12/2

10/2012

FOR: Ship Owners, Ship Managers, Ship Operators, Ship Masters, Ship Officers, Classification Societies

SUBJECT: INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

DEFINITIONS:

The following abbreviations stand for:

- "CSO" – Company Security Officer
- "DoS" – Declaration of Security
- "FPU" – Floating Production Unit
- "FPSO" – Floating Production, Storage, and Offloading Unit
- "FPU" – Floating Production Unit
- "FSU" – Floating Storage Unit
- "GT" – Gross Tonnage in accordance to ITC 69
- "HSC" – High Speed Craft
- "IACS" – International Association of Classification Societies
- "IMO" – International Maritime Organization
- "ISM Code" – International Management Code for the Safe Operation of Ships and for Pollution Prevention
- "ISPS Code" – International Ship and Port Facility Security Code implemented through chapter XI-2 Special measures to enhance maritime security in SOLAS.
- "ISSC" – International Ship Security Certificates as required by the ISPS Code
- "ITC 69" – International Convention on the Tonnage Measurement of Ships, 1969
- "MARSEC" – Marine Security Level
- "MODU" – Mobile Offshore Drilling Unit
- "MOST" – Moored Oil Storage Tanker
- "MOU" – Mobile Offshore Unit
- "MSC" – Maritime Safety Committee
- "STCW" – International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended
- "PFSO" – Port Facility Security Officer
- "PFSA" – Port Facility Security Assessment
- "PFSP" – Port Facility Security Plan
- "PSC" – Port State Control
- "RO" – Recognized Organization as defined by IMO Resolution A.789(19).
- "RSO" – Recognized Security Organization as defined by the ISPS Code
- "SBM" – Single Buoy Moorings
- "SMC" – Safety Management Certificate as required by the ISM Code
- "SMS" – Safety Management System as defined by the ISM Code
- "SOLAS" – International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended
- "SSA" – Ship Security Assessment
- "SSAS" – Ship Security Alert System
- "SSO" – Ship Security Officer
- "SSP" – Ship Security Plan

The following terms shall mean:

- “Administration” – Tuvalu Ship Registry;
- “Chapter” – a chapter in the Convention;
- “Code” – please see “International Ship and Port Facility Security (ISPS) Code”;
- “Company” – 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;
- “Contracting Government” – a government signatory to SOLAS but used more specifically to mean the country (port State) receiving a ship at a port facility;
- “Convention” – the International Convention for the Safety of Life at Sea, 1974 as amended;
- “CSO” – the person ashore designated by the Company to develop and revise the SSP and for liaison with the SSO, PFSO and the Administration;
- "Gross Tonnage" – the gross tonnage of the ship as determined under the provisions of the ITC 69 and shown on the International Tonnage Certificate (based on ITC 69) of the ship;
- “HSC” – as defined in regulation X/1;
- “International Ship and Port Facility Security (ISPS) Code” or “Code” – the ISPS Code consisting of Part A and Part B as adopted;
- “MODU” – a vessel capable of engaging in drilling operations for the exploration for or exploitation of resources beneath the sea-bed such as liquid or gaseous hydrocarbons, sulphur or salt, mechanically propelled and capable of moving on its own on and off location;
- “Non-compliance” – non-fulfillment of a specified requirement or the subject matter is inappropriate for the ship;
- “Paragraph” – a paragraph of Part B of the ISPS Code;
- “Passenger Ship” – any vessel over 100 GT, carrying more than 12 passengers for hire, which makes voyages lasting more than 24 hours of which any part is on the high seas;
- “PFSO” – the person at the port facility designated by the facility to be responsible for implementation of measures required by the ISPS Code;
- “Regulation” – a regulation in the Convention;
- “Section” – a section of Part A of the ISPS Code;
- “Security Incident” – any suspicious act or circumstance threatening the security of a ship, including MODU and a HSC, or of a port facility or of any ship/port interface or any ship-to-ship activity to which the ISPS Code applies;
- “Security Level” – the qualification of the degree of risk that a security incident will be attempted or will occur;
- “Security Level 1” – the level for which minimum appropriate protective and preventive security measures shall be maintained at all times;
- “Security Level 2” – 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;

- "Security Level 3" – 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);

- "Ship" – when used in this Code, includes unassisted mechanically propelled MODUs that are not on location and HSCs as defined in Chapter XI-2/1;

- "Short Voyage" – 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;

- "SSA" – the identification of the possible threats to key shipboard operations, existing security measures and weaknesses in the infrastructure, policies and procedures;

- "SSO" – 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 CSO and the PFSO;

- "SSP" – 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;

- "Verification" – the audit of the SSP and its implementation on a ship and associated procedures, checking the operational status of the SSAS and a representative sample of associated security and surveillance equipment and systems mentioned in the SSP.

PURPOSE:

This marine circular provides this Administration's requirements for compliance with the ISPS Code and includes policies and interpretations on the application, implementation and enforcement of the ISPS Code, including hardware requirements, for Companies and vessels seeking ISPS Code certification. However, this circular is not intended to be all-inclusive or to prohibit a Company from incorporating or requiring items in its SMS and SSP beyond those contained here.

This circular addresses certain amendments to SOLAS that are relevant to ISPS Code implementation and also provides guidance to ships not in compliance or unable to comply with the ISPS Code or SOLAS requirements. This Notice makes mandatory certain recommended practices in Part B of the ISPS Code for ships operating in the United States and Europe.

REFERENCES:

(a) Amendments to SOLAS Chapters V & XI (Conference Res. 1, adopted on 12 December 2002)
(b) ISM Code
(c) IMO Resolution MSC.104(73), ISM Code 2000 Amendments
(d) ISPS Code
(e) IMO MSC/Circ.1097, Guidance Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code
(f) IMO MSC/Circ.1072, Guidance on Provision of Ship Security Alert Systems
(g) IMO Resolution MSC.74(69) Annex 3, Recommendation on Performance Standards for Universal AIS
(h) IMO Resolutions MSC.136(76) and MSC.147(77), Performance Standards for Ship Security Alert Systems
(i) IMO Circular Letter No. 2507, Long Range Identification and Tracking of Ships (LRIT)
(j) SOLAS 74 Chapter IX, Management for the Safe Operation of Ships
(k) Tuvalu Marine Circular MC-23/2012/1, Automatic Identification Systems (AIS)
(l) Tuvalu Marine Circular MC-4/2007/12/2, Continuous Synopsis Record (CSR)

(m) Tuvalu Marine Circular MC-8/2011/1, Contact Details for Recipients of Maritime Security Related Communications
(n) Tuvalu Marine Circular MC-22/2012/1, IMO Unique Identification Number Scheme for Ship / Company / Registered Owner
(o) Tuvalu Marine Circular MC-2/2008/11/12/4, Long Range Identification and Tracking of Ships
(p) Tuvalu Marine Circular MC-3/2010/12/3, Ship Security Alert System (SSAS)

APPLICATION:

(A) The ISPS Code applies to:

a. Passenger ships, including high-speed passenger craft;

b. Cargo ships, including HSC, of 500 GT and upwards;

c. Special Purpose Ships of 500 GT, mandatory compliance as of 1 July 2008;

d. Self-propelled MODUs capable of making international voyages unassisted and unescorted when underway and not on location.

(B) The ISPS Code does not apply to:

a. Government-operated ships used for non-commercial purposes;

b. Cargo ships, including commercial yachts of less than 500 GT, voluntary compliance as of 1 July 2006 (see section on “Voluntary Compliance” below);

c. Ships not propelled by mechanical means;

d. Wooden craft of primitive origins;

e. Private pleasure yachts not engaged in trade;

f. Fishing vessels;

g. Non-self propelled MODUs, nor to MODUs of any description whilst on location, making field moves, or in port;

h. Mobile and immobile FPSOs and FSUs, FPUs, MOSTs and MOUs but should have some security procedures in place; and

i. 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 PFSP.

(C) Mobile and Immobile Floating Units

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 below into consideration.

(D) Voluntary Compliance

Vessels not subject to mandatory compliance with the ISPS Code may do so voluntarily. It is highly recommended that cargo ships, including commercial yachts, 300 or more but less than 500 GT and mobile and immobile floating units, voluntarily comply.

While still voluntary for such vessels, mandatory compliance must be anticipated in the very near future. It also must be understood that certain coastal States may impose special security requirements on these vessels.

CONTENTS:

1. Compliance

1.1. 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 Administration and RO/RSO prior to conducting any ship/port interface or port entry. This means that at the moment a ship's Master or a CSO becomes aware that a ship is not compliant or cannot maintain compliance, the Administration and RO/RSO is to be immediately advised, with details including corrective action, temporary alternative arrangements and current status.

1.2. Please refer to Tuvalu Marine Circular MC-8/2011/1 for the Administration's contact details for maritime security related communications.

2. Amendments (SOLAS)

2.1. There are a number of SOLAS amendments that impact the safety and security of a ship and are necessary elements of a SSP. Some of these measures are explained within the context of this Marine Circular. However, many are more extensive, and as a result, are the subject of the following separate Marine Circulars:

2.1.1. Tuvalu Marine Circular MC-23/2012/1, Automatic Identification Systems (AIS)

2.1.2. Tuvalu Marine Circular MC-4/2007/12/2, Continuous Synopsis Record (CSR)

2.1.3. Tuvalu Marine Circular MC-22/2012/1, IMO Unique Identification Number Scheme for Ship / Company / Registered Owner

2.1.4. Tuvalu Marine Circular MC-2/2008/11/12/4, Long Range Identification and Tracking of Ships

2.1.5. Tuvalu Marine Circular MC-3/2010/12/3, Ship Security Alert System (SSAS)

2.1.6. Tuvalu Marine Circular MC-4/2010/12/2, Updates to Issues Relating to Piracy and Armed Robbery Against Ships in Waters off the Coast of Somalia and other High Risk Areas

2.2. Control & Compliance Measures (SOLAS Chapter, XI-2, Regulation 9)

2.2.1. 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 waters of a Contracting Government. PSC of ships is intended to be limited to verifying that there is a valid ISSC on board unless there are "clear grounds" for believing the ship is not in compliance with SOLAS XI-2 or the ISPS Code.

2.2.2. "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.

2.2.3. "Clear grounds" is a series of potential factors that indicates to the PSC official that the ship's security system, which includes the crew, equipment, and procedures, is not adequate to meet the ISPS Code. It ranges from the unfamiliarity of the Master with the security provisions that are supposed to be implemented via the SSP, to evidence that the ship has loaded persons, stores or goods at a port facility that is not required to or does not comply with the ISPS Code. The potential for uneven and inequitable implementation is real and shipowners are cautioned to consider how this may impact their operations, business, and financial health and to take necessary precautions.

2.2.4. Any PSC action taken upon an Tuvalu 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

Administration and the RSO who issued the ship's ISSC. There can be no satisfactory resolution of a security issue unless the Administration or RSO is directly involved.

2.2.5. SSPs are not to be inspected by officers duly authorized by a Contracting Government to carry out control and compliance measures unless in circumstances where "clear grounds" are evident and then only to the extent specified in Part A section 9.8.1 of the ISPS Code.

2.2.6. 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, then limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Administration or the Master of the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of Part A of the Code and the related provisions of Part B are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Administration and the Contracting Government concerned.

2.3. Equivalent Security Arrangements (SOLAS Chapter, XI-2, Regulation 12)

2.3.1. 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.

2.3.2. As a matter of principle it is believed that this should only be undertaken in exceptional and unique circumstances. Close coordination with the Administration and RSO is necessary for the evaluation and approval of any such equivalencies. Owners and operators are cautioned that specific approval must be obtained from the Administration or RSO 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.

3. Objectives and Functional Requirements

3.1. The objectives of the ISPS Code are:

3.1.1. 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;

3.1.2. 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;

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

3.1.4. 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

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

3.2. Functional Requirements

In order to achieve its objectives, the ISPS Code embodies a number of functional requirements. These include, but are not limited to:

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

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

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

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

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

3.2.6. requiring ship and port facility security plans based upon security assessments; and

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

4. SOLAS Chapter, XI-2, Regulation 4

4.1. 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.

4.2. 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.

5. International Safety Management (ISM) Code

5.1. This Administration considers the ISPS Code to be an extension of the ISM Code and an integral part of emergency preparedness and compliance with international conventions in a Company's SMS.

5.2. Failure of a Tuvalu flagged vessel to comply with the ISPS Code will be considered a major non-conformity as defined in the ISM Code, resulting in the immediate withdrawal of the vessel's SMC and ISSC, which will effectively prevent the ship from trading.

5.3. 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 Administration that they are satisfied with the vessel's compliance with the ISPS Code.

6. Recognized Security Organizations (RSO)

6.1. The ISPS Code created a new type of organization for the purpose of providing verification and certification with respect to the Code. These new organizations are termed RSOs, and specific experience and qualification requirements must be met prior to approval by administrations. This Administration has authorized all its existing ROs as RSOs to take on the specific security related duties under Chapter XI-2. A list of the authorized ROs can be found at www.tvship.com, which is updated as necessary.

6.2. The ISPS Code expressly prohibits those instances where an RSO provides consulting services and risk assessments in security plan development for ISPS Code Certifications, the RSO shall not review and approve the plans or verify and issue any required certificates. In short, RSOs cannot approve or certify their own work product.

6.3. An RSO may provide ISPS Code verification services to vessels for which the parent RO also provides ship statutory certification services and/or ISM Code certification. Services shall be provided in accordance with IACS Procedural Rule (PR) 24.

6.4. 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.

6.5. Companies may choose from any of the 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. Once chosen, however, this Administration expects the CSO to maintain continuity in the process by having the RSO perform the entire review, approval, verification and certification of the vessel's SSP. Any deviation from this will require prior approval from this Administration.

6.6. This Administration highly recommends in keeping with the previous section 6.3 that the chosen RSO be part of the RO currently certifying the ship under the ISM Code so that the audits and certification of both may be harmonized.

7. Declaration of Security (DoS)

7.1. A 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 this Administration, a Contracting Government, PFSO, CSO or SSO deems it necessary.

7.2. Use of a DoS at MARSEC 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.

7.3. At MARSEC Level 1, the Master or SSO, or their designated representative, of any passenger ship or manned vessel carrying Certain Dangerous Cargoes, in bulk, must complete and sign a DoS with the SSO or FSO, or their designated representative, of any vessel or facility with which it interfaces.

7.4. At MARSEC Levels 1 and 2, SSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, a single Declaration of Security for multiple visits, provided that:

7.4.1. The DoS is valid for the specific MARSEC Level;

7.4.2. The effective period at MARSEC Level 1 does not exceed 90 days; and

7.4.3. The effective period at MARSEC Level 2 does not exceed 30 days.

7.5. All DoSs 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.

7.6. Ships arriving with a higher MARSEC Level than the port that the vessel is calling upon must notify the PFSO who should undertake an assessment of the situation and, in consultation with the CSO or SSO, should agree on appropriate security measures with the ship. Vessels that are operating at a higher Security Level shall request a DoS with the facility, and the facility should complete a DoS with the vessel. The conditions under which a vessel may request a DoS from the facility must be included in the SSP.

7.7. Should the PFSO refuse to complete a DoS and demand that the ship operate at the lower Security Level of its facility, all measures considered necessary should be maintained at the higher Security Level while still allowing cargo operations (see section 8 below), the proposed DoS executed by the SSO and retained for the record and the incident properly logged.

7.8. Generally, port facilities set the MARSEC Level based upon the Level set by the Contracting Government (Port State). A facility may request that a vessel complete a DoS with the facility as

appropriate for that facility's Security Plan or direction of the PFSO. If the facility owner or operator requires a DoS, the vessel must comply.

7.9. When the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

7.10. A sample of DoS can be downloaded from the Appendix of this Circular at www.tvship.com

8. Non-compliant Ports and Port Facilities

8.1. In this regard, masters are encouraged to establish security measures when calling at non-compliant ports and port facilities. The following steps may be taken:

8.1.1. Implement measures per the SSP equivalent to Security Level 2;

8.1.2. Ensure that each access point to the ship is guarded and that the guards have total visibility of the exterior (both landside and waterside) of the vessel. Guards may be:

- provided by the ship's crew, however, additional crewmembers should be placed on the ship if necessary to ensure that limits on maximum hours of work are not exceeded and/or minimum hours of rest are met, or
- provided by outside security forces approved by the ship's master and Company Security Officer.

8.1.3. Attempt to execute a Declaration of Security; and

8.1.4. Log all security actions in the ship's log.

9. Responsibilities of the Company

9.1. 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.

9.2. 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.

9.3. 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:

9.3.1. 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;

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

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

9.4. The Company shall ensure that the CSO, the Master and the SSO are given the necessary support to fulfill their duties and responsibilities in accordance with Chapter XI-2, Part A and the relevant provisions of Part B of the ISPS Code.

10. Ship Security Assessment

10.1. 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.

10.2. The ISPS Code does not permit the SSA to be performed by the same RSO chosen by the Company to perform the Plan review, approval, verification and certification.

10.3. 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.

10.4. At completion of the SSA, and approval by the Company, the CSO shall prepare a report consisting of how the assessment was conducted, a description of vulnerabilities found during the assessment and a description of countermeasures and management practices employed to address vulnerabilities.

10.5. 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.

11. Ship Security Plan

11.1. 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.

11.2. 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.

11.3. 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.

11.4. The RSO shall review the SSP to ensure that each element required by Part A, the relevant provisions of Part B of the Code and best management practices are satisfactorily addressed as well as all the vulnerabilities referenced in the SSA. This Administration recommends that the plan review process takes place in the Company, if possible, with the direct interaction of the CSO and RSO to preclude the need to transport or ship this sensitive material by means out of their control.

11.5. Identification of the locations where the SSAS activation points are provided, and the procedures, instructions and guidance on the use of the SSAS, including the testing, activation, deactivation and resetting, and to limit false alerts, may, in order to avoid compromising in any way the objective of the system, be kept elsewhere in a separate document known only to the Master, the SSO and other senior management level officers on board.

12. Best Management Practices (BMPs)

12.1. 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 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.

12.2. Thus, while every BMP does not have to be included in an SSP, this Administration 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 this Administration and the MSC. From the Administration's perspective, the important point is that the shipowner/operator has a well-thought-out plan in place and documented in the SSP.

12.3. Insofar as verification is concerned, we realize that flexibility in planning is needed due to constantly changing circumstances. Therefore, SSPs are not required to be re-submitted for review and approval. It is acceptable to attach an Annex to the SSP that includes the actual plan implemented by the ship owner/operator to protect against terrorism, piracy and armed robbery, provided that there is a general statement in the SSP. This general statement should state as an example that:

12.3.1. Due to the changing circumstances, the operator is following certain procedures, including guidance given in the BMPs;

12.3.2. These procedures and information are contained in an accompanying Annex/file to the SSP; and

12.3.3. This file will be updated as necessary.

It is not acceptable to simply attach the BMPs as an Annex. There must be an actual plan in place. Verification of a plan being in place should be considered during the owner/operators scheduled ISM/ISPS Code Audits.

13. Records

13.1. Records of activities detailed in Part A, Section 10.1 of the Code shall be addressed in the SSP and kept onboard for a minimum period as specified below. The records shall be kept in the working language of the ship. If the working language of the ship is not English, French or Spanish, then a translation into one (1) of these languages shall be included.

13.2. Due to the security sensitive nature of these records, they shall be protected from unauthorized disclosure.

13.3. Such records shall be maintained on board for a period of three (3) years after the events and thereafter may be removed to the Company for safekeeping and review by the RSO during periodical and renewal audits.

13.4. Records required to be kept by SOLAS Chapter XI-2, Regulation 9.2.1, including DoSs, for at least the last 10 calls at port facilities shall be maintained on board.

13.5. Records may be kept in any format but must be protected from unauthorized access or disclosure and loss. The records shall be in a form to be readily available to PSC officials if so requested. By this it is meant that those parts of the records describing corrective or preventive actions determined necessary as the result of a drill or exercise that involve revisions to the required details of the SSP which address Sections 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of Part A of the Code, which is considered confidential, cannot be subject to inspection and shall not be disclosed without a prior request from the Contracting Government of the State

where the vessel is being inspected and the authorization to do so from this Administration, both of which shall be made in writing

14. Company Security Officer (CSO)

14.1. The CSO is the person designated by the Company and recognized by the Administration to perform the duties and responsibilities of the CSO as detailed in Part A, Section 11 and the relevant provisions of Part B, Sections 8, 9 and 13 of the Code. The CSO shall have the knowledge of, and receive training in, some or all of the elements of Part B, Section 13.1 of the Code.

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

14.3. The Company shall provide this Administration with the full name of the CSO and information to enable direct and immediate contact at all times between the Administration and the CSO with regard to matters related to the ISPS Code. The Company shall use “Form CSO, Declaration of CSO (ISPS Code)”, which can be downloaded from our website at www.tvship.com.

14.4. Taking into account the professional background and security related training of the Company selected CSO, this Administration reserves the right to deny affirmation of the CSO based on any one or combination of elements that the Administration feels the CSO to be deficient.

14.5. A Company may designate more than one (1) CSO. The company must structure their plans accordingly. It may be advisable to have a CSO for different geographical areas or groups of ships within a fleet, as an example. However, in doing so, it must be clearly declared and understood who is responsible for which ships in the fleet.

14.6. 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 this Administration in this regard.

14.7. 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.

14.8. The CSO shall ensure that each vessel for which he or she is responsible is appointed a trained and qualified SSO.

15. Ship Security Officer (SSO)

15.1. 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.

15.2. The SSO shall be a management level officer. It is highly recommended that this be the Master who shall have completed an approved training course regarding the requirements and recommendations of the ISPS Code. If it is not the Master, it must be understood that the Master still holds overall responsibility for the security of the ship which cannot be relinquished.

15.3. 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.

16. Training and Certification

16.1. 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 of the Code.

16.2. 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 of the Code.

16.3. This Administration has not deemed it necessary to add to the competencies already identified in the ISPS Code. However, it has identified a need to assure that training is adequate before authorizing the issuance of an ISSC. Companies must ensure that training courses for CSOs provide the equivalent of at least 20 hours training by a training facility recognized and endorsed by a RSO.

16.4. The CSO must assure that persons to be appointed as SSO have received formal course training provided by a recognized training facility endorsed by a RSO. In addition, the CSO must assure that documented familiarization training is provided to appointed SSOs as outlined in Part B, 13.2 of the Code.

16.5. Self-instruction and distance learning programs such as computer-based training (CBT) are “provisionally” acceptable for training, but only when combined with a comprehensive Company training program supervised by the CSO. CBT and other training programs designed to just meet the bare minimum of ISPS Code Part A, 13.2, of the Code do not meet the requirements addressed in Part B, 13.2, which call for SSO training in “the layout of the ship” (13.2.1) and “the ship security plan and related procedures” (13.2.2).

16.6. Companies may elect to establish their own training programs; however, prior to implementation, such programs shall be presented to the RSO for review and endorsement. A CSO conducting such courses must meet the requirements of section 16.3 above and have some experience with training to be endorsed.

17. Drills and Exercises

17.1. Objectives

17.1.1. 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.

17.1.2. Drills shall test individual elements of the SSP such as those security threats listed in Part B, Section 8.9 of the Code. When practicable, the Company and ship should participate in the drills being conducted by a port facility where they may be located.

17.1.3. 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.

17.1.4. Training courses, although considered advisable, shall not be considered as satisfying the requirements to conduct drills or exercises.

17.2. Frequency

17.2.1. 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.

17.2.2. Exercises shall be carried out at least once each calendar year with no more than 18 months between the exercises.

17.2.3. Records indicating type of drill or exercise, SSP element(s) covered, and attendance shall be maintained by the SSO for a period of three (3) years. They may be kept in any

format but must be protected from unauthorized access or disclosure. The records shall be in a form to be readily available to PSC officials if so requested.

17.2.4. Although exercises are to be carried out at least once each calendar year with no more than 18 months between the exercises, fleets of more than six (6) vessels may be scheduled to exercise in small groups with the eventual direct participation of every vessel over a period of three (3) years. The results and lessons learned during each exercise shall be distributed throughout the fleet and available aboard each vessel as objective evidence of direct or indirect participation in the exercises.

17.2.5. The Administration will recognize Company's participation in exercises with another Contracting Government.

18. SSP Onboard Verification Audits for Issuance of the ISSC

18.1. 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 below, but not more than five (5) years; and at least one (1) intermediate verification.

18.2. Verification audits for issuing, endorsing or renewing the ISSC shall be performed by RSOs on behalf of this Administration.

18.3. If upon initial verification, the auditing RSO has not performed the SSP review and approval, the CSO shall have a pre-verification review of the SSA and SSP documentation performed by the auditing RSO before the verification audit is conducted.

18.4. Initial verification shall include finding objective evidence demonstrating:

18.4.1. that the security management system has been in operation for at least two (2) months from the date the SSP is logged as received onboard from the CSO;

18.4.2. that all technical equipment specified in the SSP is fully operational;

18.4.3. that the recording activities detailed in Parts A/10.1.1, 10.1.6 and 10.1.10 of the Code have been carried out; and

18.4.4. that the specific requirements of paragraphs 8.1 to 13.8 of Part B of the Code have been taken into account before an ISSC may be issued by the RSO.

18.5. If the auditor identifies, through objective evidence, non-compliance with the approved SSP, this shall be communicated to the Company, the Administration 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.

18.6. 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.

18.7. 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.

18.8. This Administration highly recommends that Initial, Intermediate or Renewal verification audits be carried out in conjunction with the ISM Code SMS audits of the ship.

18.9. Additional ship verification audits may be carried out at any time by the RSO on behalf of the Administration. 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 to what extent a re-verification of the SSP would be necessary.

19. International Ship Security Certificate (ISSC)

19.1. Issuance

19.1.1. The 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.

19.1.2. An ISSC shall only be issued when:

19.1.2.1. the ship has an approved SSP;

19.1.2.2. all technical equipment specified in the SSP is fully operational; and

19.1.2.3. there is sufficient objective evidence found to the satisfaction of the Administration's RSO through the verification audit that the ship is operating in accordance with the provisions of the approved SSP.

19.1.3. 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.

19.2. Validity

19.2.1. The ISSC shall normally be valid for a period of five (5) years or a period specified by the Administration from the date of the Initial Verification Audit and be subject to an Intermediate Audit between the second and third anniversary date. However, the period of validity may be shorter than five (5) years if so requested by the CSO.

19.2.2. Upon initial issue, the expiry date may be harmonized with the ship's SMC so that renewal and auditing may occur together.

20. Interim ISSC Certificate

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

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

20.1.2. the transfer of a ship from the flag of a Contracting Government to Tuvalu;

20.1.3. the transfer of a ship to Tuvalu from a State which is not a Contracting Government; or

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

20.2. Before an Interim Certificate may be issued, the RSO must find that:

20.2.1. an SSA has been completed;

20.2.2. a copy of the SSP is provided on board, has been submitted for review and approval, and is being implemented;

20.2.3. the ship is provided with a compliant SSAS;

20.2.4. the CSO has ensured the review of the SSP for compliance, submitted for approval, and is being implemented;

20.2.5. the CSO has established the necessary arrangements, including that for drills, exercises and internal audits, through which the CSO is satisfied that the ship will successfully complete the required verification in accordance with Part A, Section 19.1.1.1, of the Code within six (6) months;

20.2.6. the CSO has made arrangements for carrying out the required verifications under Part A, Section 19.1.1.1 of the Code;

20.2.7. the Master, the SSO and other ship's personnel with specific security duties are familiar with their duties and responsibilities, with the relevant SSP provisions, and are provided information in their working language and understand it; and

20.2.8. the SSO meets the qualifications requirements of the Code.

20.3. 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.

20.4. A subsequent consecutive Interim ISSC shall not be issued to a ship if, in the judgment of the Administration 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.

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

21.1. Any failure of security equipment or systems, or suspension of a security measure that compromises the ship's ability to operate at security levels 1, 2 or 3 shall be reported immediately to the Administration or the ship's RSO and to the appropriate authorities responsible for any port facility the ship is using, or the authorities of any coastal State through whose territorial seas the ship has indicated it intends to transit, and instructions requested.

21.2. 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 Administration 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.

21.3. The ship's RSO, on instructions from the Administration, 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.

21.4. Flag State Inspectors are not allowed access to the SSP. However, they will determine to the extent possible that there is an effective safety and security management system in place on board. If non-compliance issues are identified, then the Administration shall be notified and the ship's RSO dispatched to review the situation before the vessel is allowed to proceed.

22. Port Facility Requirements

22.1. The Administration highly recommends that shipowners read Port Facility requirements and become familiar with them.

22.2. Just like ships, port facilities must have a:
22.2.1. Port Facility Security Officer (PFSO);

22.2.2. Port Facility Security Assessment (PFSA); and

22.2.3. Port Facility Security Plan (PFSP).

22.3. Although, the ISPS Code refers to CSO and SSO coordination with the PFSO, the primary interface for the Company will be the SSO. However, this Administration strongly recommends that shipowners contact the port facilities with which they routinely do business and establish liaison now between the CSO and PFSO to begin coordinating activities.

22.4. Numerous references in the ISPS Code necessitate PFSO/SSO/CSO coordination to ensure that actions by ships and port facilities with regard to maritime security are complementary, and recommend that the CSO/SSO liaise at the earliest opportunity with the PFSO of the port facility where a ship intents to call to establish the security level for the ship and port facility interface. After the ship establishes contact with the PFSO, the PFSO should advise the ship of any subsequent change in the port facility's security level and provide the ship with any relevant security information and instructions.

22.5. Generally, port facilities set the MARSEC Level based upon the Level set by the Contracting Government (Port State). However, ships arriving with a higher MARSEC Level must notify the PFSO who should undertake an assessment of the situation and in consultation with the CSO or SSO agree on appropriate security measures with the ship.

Yours sincerely,

Deputy Registrar
Tuvalu Ship Registry