REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-16

Rev. May/2017

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

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

References:

(a) ***International Convention for the Safety of Life at Sea (SOLAS), Consolidated Edition 2014,*** **as amended**

(b) ***International Ship and Port Facility Security (ISPS) Code*****, 2012 Edition, as amended**

(c) ***International Safety Management (ISM) Code*****, 2014 Edition, as amended**

(d) **IMO Resolution MSC.74(69),** ***Annex 3, Recommendation on Performance Standards for Universal Automatic Identification System (AIS)*****, adopted 12 May 1998**

(e) **IMO Resolution MSC.147(77),** ***Revised Performance Standards for a Ship Security Alert System*****, adopted 29 May 2003**

(f) **IMO Circular MSC/Circ.1097,** ***Guidance Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code*****, dated 6 June 2003**

(g) **IMO Circular MSC/Circ.1072,** ***Guidance on Provision of Ship Security Alert Systems*****, dated 26 June 2003**

(h) **Maritime Safety Transportation Security Act of 2002 (MTSA)**

(i) **USCG Final Rules, Vessel Security, 22 October 2003 (FRs)**

(j) **RMI Marine Notice 2-011-12,** ***Implementation of IMO Unique Company and Registered Owner Identification Number Scheme***

(k) **RMI Marine Notice 2-011-17,** ***Automatic Identification Systems (AIS)***

(l) **RMI Marine Notice 2-011-18,** ***Ship Security Alert System***

(m) **RMI Marine Notice 2-011-19,** ***Continuous Synopsis Record***

(n) **RMI Marine Notice 2-011-20,** ***Notice of Intended Entry into Port***

(o) **RMI Marine Notice 2-011-25 and RMI Marine Guideline 2-11-4,** ***Long Range Identification and Tracking of Ships***

(p) **RMI Marine Notice 2-011-39,** ***Piracy, Armed Robbery, and the Use of Armed Security***

PURPOSE:

This Notice provides the Republic of the Marshall Islands (RMI) National requirements for compliance with the International Ship and Port Facility Security (ISPS) Code. It details the RMI Maritime Administrator's (the "Administrator") policies and interpretations on the application, implementation and enforcement of the ISPS Code, including hardware requirements, for Companies and vessels seeking ISPS Code certification.

The RMI National requirements are not intended to be all-inclusive or to prohibit a Company from incorporating or requiring items in its Safety Management System (SMS) and Ship Security Plan (SSP) beyond those contained here.

This Notice also addresses certain amendments to the International Convention for the Safety of Life at Sea (SOLAS), Consolidated Edition 2014, that are relevant to ISPS Code implementation. It 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 (U.S.) and Europe.

This Notice supersedes Rev. 2/12 and reflects the deletion of the form in Appendix 4 and the updating and hyperlinking of the referenced form in section 2.2.2, along with the hyperlinking of all referenced documents where possible.

BACKGROUND:

The ISPS Code was adopted 12 December 2002 at a Diplomatic Conference held at the International Maritime Organization (IMO) in London from 9-13 December 2002. During this Conference, amendments to SOLAS were also adopted. The ISPS Code and SOLAS amendments are a series of international maritime security measures that have a significant impact on the operation of ship owning companies, ships, their operators, and the port facilities they call on.

It is important to note that in many countries, the ISPS Code is overlaid by substantive national requirements. For example, the U.S. adopted the Maritime Transportation Security Act of 2002, which was implemented by the U.S. Coast Guard through a series of publications in the *Federal Register* on October 22, 2003 (see 68 FR 60448 and as codified, 33 *Code of Federal Regulations* Part 104) to protect U.S. ports and waterways from a terrorist attack by mandating compliance with the ISPS Code and with enhanced security requirements. Similarly, the European Union (EU) adopted regulations (No. 725/2004, as amended) not only to enhance security within the European Community, but to provide a harmonized interpretation of the ISPS Code by making certain recommended practices in Part B of the Code mandatory. Ships operating in counties with these additional requirements need to be aware of and in compliance with them, as applicable.

APPLICABILITY:

The provisions governing the applicability of the ISPS Code to RMI flagged ships are contained in Section 4.0 of this Marine Notice.

REQUIREMENTS:

1.0 Compliance

1.1 In accordance with SOLAS, 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.

1.2 The Point of Contact for the Administrator is:

Marine Safety Administrator
Republic of the Marshall Islands Maritime Administrator
Telephone: +1-571-441-1885
Duty Officer Fax: +1-703-860-2284
Email: dutyofficer@register-iri.com and inspections@register-iri.com

2.0 SOLAS Amendments

2.1 Various

There are a number of SOLAS amendments that impact the safety and security of a ship and are necessary elements of an ISPS Ship Security Plan (SSP). Some of these measures are explained within the context of this Marine Notice. However, many are more extensive, and as a result, are the subject of the following separate Marine Notices and Marine Guidelines:

- MN-2-011-12, *Unique Company and Registered Owner Identification Scheme* [SOLAS Chapter XI-1, Regulation 3]
- MN-2-011-17, *Automatic Identification Systems (AIS)* [SOLAS Chapter V, Regulation 19]
- MN-2-011-18, *Ship Security Alert System (SASS)* [SOLAS Chapter XI-2, Regulation 6]
- MN-2-011-19, *Continuous Synopsis Record (CRS)* [SOLAS Chapter XI-1, Regulation 5]
- MN-2-011-25, *Long Range Identification and Tracking of Ships* [SOLAS Chapter V, Regulation 19/1] and MG-2-11-4, *Long Range Identification and Tracking*
- MN-2-011-39, *Piracy, Armed Robbery, and the Use of Armed Security* [Internationally Accepted Best Management Practices]

ISPS Code Certification is subject to compliance with the requirements listed above, as applicable.

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

2.2.1 Details

.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 w of 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.

.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.

.3 "Clear grounds" is a series of potential factors that indicates to the port State control 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. Shipowners are cautioned to consider how this may impact their operations, business, and financial health and to take necessary precautions. The ISPS Code is relatively straightforward. This is not and will require very careful management and execution.

2.2.2 RMI requirements

.1 Any port State action taken upon an RMI 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. There can be no satisfactory resolution of a security issue unless the Administrator is directly involved.

.2 SSPs are not to be inspected by officers duly authorized by a Contracting Government to carry out control and compliance measures save 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.

.3 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. 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 Administrator and the Contracting Government concerned.

.4 If, during an expanded port State control examination in the U.S., those sections of the SSP the port State authority is allowed to review are not written in English, a vessel may be delayed while translator services are acquired.

.5 Further clarification of this issue is provided in MN-2-011-20, *Notice of Intended Entry into Port.*

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

2.3.1 Details

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 RMI Requirements

As a matter of principle it is believed that this should only be undertaken in exceptional and unique circumstances. Close coordination with the Administrator is necessary for the evaluation and approval of any such equivalencies. 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.

3.0 ISPS Code

3.1 Objectives

The objectives of the ISPS Code are:

.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;

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

.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 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:

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

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

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

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

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

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

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

3.3 Definitions

.1 "Convention" means the International Convention for the Safety of Life at Sea (SOLAS), Consolidated Edition 2014, as amended.

.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.

.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.

.4 "International Ship and Port Facility Security (ISPS) Code" or "Code" means the ISPS Code consisting of Part A and Part B as adopted.

.5 "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.

.6 "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.

.7 "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).

.8 "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.

.9 "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.

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

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

.12 "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.

.13 "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).

.14 "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.

.15 "Regulation" means a regulation in the Convention.

.16 "Chapter" means a chapter in the Convention.

.17 "Section" means a section of Part A of the ISPS Code.

.18 "Paragraph" means a paragraph of Part B of the ISPS Code.

.19 "Ship" when used in this Code, includes unassisted mechanically propelled mobile offshore drilling units that are not on location and high-speed craft as defined in Chapter XI-2/1.

.20 "Certain Dangerous Cargo" (CDC) means the same as defined in the U.S. 33 CFR 160.203, as amended by the USCG Final Rules dated 1 July 2003 (see Appendix 1).

.21 "Hazardous Condition" means the same as defined in the U.S. 33 CFR 160.203, as amended by the USCG Final Rules dated 1 July 2003 (see Appendix 1).

.22 "Passenger Ship" means any vessel over 100 gross registered tons, carrying more than 12 passengers for hire, which makes voyages lasting more than 24 hours of which any part is on the high seas.

.23 "Non-compliance" means non-fulfillment of a specified requirement or the subject matter is inappropriate for the ship.

.24 "Verification" means 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.

.25 "MI" means Marshall Islands or the Maritime Administration.

.26 "USCG" means the United States Coast Guard.

.27 "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.

4.0 Application of the ISPS Code

4.1 The ISPS Code applies to:

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft and yachts engaged in trade, of 500 gross tonnage (ITC 69) and upwards;
- Special Purpose Ships of 500 gross tonnage;
- Self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location.

4.2 The ISPS Code does not apply to:

- Government-operated ships used for non-commercial purposes;
- Cargo ships, including commercial yachts of less than 500 gross tonnage (ITC 69), voluntary compliance as of 1 July 2006 (see section 4.4 below);
- Ships not propelled by mechanical means;
- Wooden craft of primitive origins;
- 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 whilst 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).

4.3 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 above into consideration.

4.4 Voluntary Compliance

Vessels not subject to mandatory compliance with the ISPS Code may do so voluntarily. It is highly recommended that cargo ships, including yachts engaged in trade, 300 or more but less than 500 gross tonnage (ITC 69) 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. Such is the case in U.S. territorial waters wherein foreign commercial vessels greater than 100 gross registered tons not subject to SOLAS are subject to Part 104 of the USCG Final Rules. Such vessels should consider adopting the appropriate Alternative Security Plan provided by groups representing specialized marine sectors within the U.S.

5.0 Mandatory Compliance

5.1 Regulation 4 of Chapter XI-2

5.1.1 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.

5.1.2 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.

5.1.3 The Administrator has made certain provisions of Part B mandatory for RMI flagged ships operating in U.S. waters or EU waters. These requirements are contained in Appendix 2 and Appendix 3 of this Notice, respectively.

5.2 International Safety Management (ISM) Code

5.2.1 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.

5.2.2 Failure of an RMI flagged vessel 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.

5.2.3 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.

6.0 Recognized Security Organizations

6.1 Details

6.1.1 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 called Recognized Security Organizations (RSOs), and specific experience and qualification requirements must be met prior to approval by administrations. Utilizing the guidelines developed by the RMI and promulgated by IMO MSC/Circ.1074 as well as the authority provided in the ISPS Code, the Administrator has delegated by written agreement to certain RSOs specific security related duties under Chapter XI-2.

6.1.2 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.

6.2 MI Requirements

6.2.1 The Administrator, utilizing the MSC guidelines that it helped to formulate and the authority provided in the ISPS Code, has carefully chosen, through a selective individual interview process, certain of its 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. Certified ISPS Code Auditors trained to the requirements of IACS Procedural Rule 25 must be made available to Marshall Islands shipowners. A list of the authorized RMI RSOs with contact points has been circulated by means of an RMI Marine Safety Advisory, which updated as necessary.

6.2.2 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, provided that, the ship safety management audits and security assessments are conducted separately, and in addition to, existing ship statutory certification and classification survey functions. Services shall be provided in accordance with IACS Procedural Rule (PR) 24.

6.2.3 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 reverification audit by the RSO.

6.2.4 Companies may choose from any of the RMI designated 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, the Administrator will expect 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 the Administrator.

6.2.5 The Administrator highly recommends in keeping with the previous section 6.2.3 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.

7.0 Declaration of Security

7.1 Details

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 any time the Administrator, a Contracting Government, PFSO, CSO or SSO deems it necessary. This requirement is similar to the existing U.S. practice for vessel-to-facility oil transfer proceedings.

7.2 RMI Requirements

7.2.1 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.

7.2.2 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.

7.2.3 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:

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

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

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

7.2.4 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.

7.2.5 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.

7.2.6 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 7.3 below), the proposed DoS executed by the SSO and retained for the record and the incident properly logged.

7.2.7 Generally, port facilities set the Maritime Security 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.

7.2.8 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.

7.2.9 It is advisable that a DoS always be requested at every port call.

7.3 Non-compliant Ports and Port Facilities

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

.1 Implement measures per the ship’s security plan equivalent to Security Level 2;

.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 CSO.

.3 Attempt to execute a Declaration of Security; and

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

7.3.2 Masters are advised that the US Coast Guard is imposing conditions of entry on vessels arriving from non-compliant ports it has recognized. Any vessel arriving in the United States that has called in a non-compliant port during its previous five port calls must take actions 1 through 4 listed above. A report of actions taken must be notified to the cognizant U.S. Coast Guard Captain of the Port (COTP) prior to arrival in the United States. An RMI Ship Security Advisory is maintained and updated as necessary to provide the USCG list of ports.

8.0 Obligations of the Company

8.1 Details

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.

8.2 RMI Requirements

8.2.1 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.

8.2.2 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:

.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;

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

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

8.2.3 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.

9.0 Ship Security Assessment (SSA)

9.1 Details

9.2.1 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.

9.2.2 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.

9.2 RMI Requirements

9.2.1 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.

9.2.2 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.

9.2.3 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.

10.0 Ship Security Plan (SSP)

10.1 Details

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.

10.2 RMI Requirements

10.2.1 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.

10.2.2 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.

10.2.3 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. The Administrator recommends that the plan review process take 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.

10.2.4 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.

10.2.5 If, during an expanded port State control examination in the U.S., those sections of the SSP the port State is allowed to review are not written in English, a vessel may be delayed while translation services are acquired. (See Section 1.3.4.2 (ii) and (iii), Regulation 9, "Control and Compliance Measures" in this Notice.)

10.3 Best Management Practices (BMPs)

10.3.1 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 "Live Piracy Report" 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.

10.3.2 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.

10.3.3 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 resubmitted 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:

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

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

.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.

11.0 Records

11.1 Details

11.1.1 Records of activities detailed in Part A, Section 10.1 shall be addressed in the SSP and kept onboard for a minimum period specified by the Administrator. 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.

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

11.2 RMI Requirements

11.2.1 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.

11.2.2 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.

11.2.3 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 port State control 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 Administrator, both of which shall be made in writing.

12.0 CSO

12.1 Details

The CSO is the person designated by the Company and recognized by the Administrator 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.

12.2 RMI Requirements

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

12.2.2 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. The Company shall use the RMI Combined Declaration Form (MI-297B) for this purpose.

12.2.3 Taking into account the professional background and security related training of the Company selected CSO, the Administrator shall retain right to deny affirmation of the CSO based on any one or combination of elements the Administrator feels the CSO to be deficient.

12.2.4 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.

12.2.5 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.

12.2.6 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.

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

13.0 Ship Security Officer

13.1 Details

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.

13.2 RMI Requirements

13.2.1 The SSO shall be a management level officer. It is advisable that this be the Master, holding a valid RMI Certificate of Competence, 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.

13.2.2 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.

14.0 Training and Certification

14.1 Details

14.1.1 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.

14.1.2 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.

14.2 RMI Requirements

14.2.1 The Administrator 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 the Administrator or an RSO designated by the Administrator.

14.2.2 The CSO must assure that persons to be appointed as SSO have received formal course training provided by a recognized training facility endorsed by the Administrator or one (1) of its RSOs. 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.

14.2.3 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, 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).

14.2.4 Companies may elect to establish their own training programs; however, prior to implementation, such programs shall be presented to the Administrator or RSO for review and endorsement. A CSO conducting such courses must meet the requirements of paragraph 14.2.1 above and have some experience with training to be endorsed.

14.2.5 Persons holding a valid RMI Certificate of Competence seeking to be Company appointed SSOs have the option of being provided an RMI Special Qualification Certificate (SQC) acknowledging the formal SSO course training they have received up to 31 December 2007. As of 1 January 2008, the certification shall become mandatory.

14.2.6 Management level officers, holding a valid RMI Certificate of Competence, who have demonstrated knowledge and understanding of the ISPS Code to the satisfaction of a CSO through an endorsed Administration, RSO or Company training program, will be recognized for the issuance of the optional RMI SQC as an SSO.

14.2.7 Other individuals with a background and training in security or law enforcement who can demonstrate a knowledge and understanding of the ISPS Code, or who have been certified as a qualified SSO by a Contracting Government with a system of training approved by the IMO, may also qualify for certification as an SSO at the discretion of the Administrator.

14.2.8 Provided this criterion is met, the Administrator will issue an SQC to the SSO to acknowledge that training. Details concerning the procedures and requirements for the issuance of these SQCs are provided in a Marine Safety Advisory, which shall soon be replaced by a separate Marine Notice now that the IMO STW subcommittee has determined the training and competency requirements for this position and the IMO MSC has approved its recommendation for mandatory status.

15.0 Drills and Exercises

15.1 Details

15.1.1 Objective of Security Drills and Exercises

.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.

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

.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.

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

15.1.2 Drill and Exercise Frequency

.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.

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

15.2 RMI Requirements

15.2.1 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 port State control officials if so requested.

15.2.2 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.

15.2.3 The Administrator will recognize Company participation in exercises with another Contracting Government.

16.0 SSP Onboard Verification Audits for Issuance of the ISSC

16.1 Details

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.

16.2 RMI Requirements

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

16.2.2 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.

16.2.3 Initial verification shall include finding objective evidence demonstrating:

.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;

.2 that all technical equipment specified in the SSP is 100% operational;

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

.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 Administrator's RSO.

16.2.4 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.

16.2.5 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.

16.2.6 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.

16.2.7 The Administrator highly recommends that Initial, Intermediate or Renewal verification audits be carried out in conjunction with the ISM Code SMS audits of the ship.

16.2.8 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.

17.0 International Ship Security Certificate

17.1 Initial Issuance

17.1.1 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.

17.1.2 An ISSC shall only be issued when:

.1 the ship has an approved SSP;

.2 all technical equipment specified in the SSP is 100% operational; and

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

17.1.3 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.

17.2 Validity

17.2.1 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. However, the period of validity may be shorter than five (5) years if so requested by the CSO.

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

18.0 Failures of Security Equipment/Systems or Suspension of Security Measures

18.1 Details

18.1.1 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 Administrator 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.

18.1.2 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 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.

18.1.3 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.

18.2 RMI Requirements

RMI Nautical Inspectors are not allowed access to the SSP. However, they will be provided with guidelines that will allow them to determine to the extent possible that there is an effective safety and security management system in place on board. The guidelines will also serve to determine whether there are "clear grounds" to believe that there may be non-compliance issues. If such circumstances should arise, the Administrator shall be notified and the vessel's RSO dispatched to review the situation before the vessel is allowed to proceed.

19.0 Interim ISSC Certificate

19.1 Details

19.1.1 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:

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

.2 the transfer of a ship from the flag of a Contracting Government to the RMI;

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

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

19.1.2 Before an Interim Certificate may be issued, the Administrator's RSO must find that:

.1 an SSA has been completed;

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

.3 the ship is provided with a compliant SSAS;

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

.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, within six (6) months;

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

.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

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

19.1.3 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.

19.1.4 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.

19.2 RMI Requirements

There are no further requirements.

20.0 Port Facility Requirements

20.1 Shipowners should read Port Facility requirements and become familiar with them.

20.2 Just like ships, port facilities must have a:

- Port Facility Security Officer (PFSO);
- Port Facility Security Assessment (PFSA); and
- Port Facility Security Plan (PFSP).

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

20.4 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.

20.5 Generally, port facilities set the Maritime Security 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 should agree on appropriate security measures with the ship.

APPENDIX 1

U.S. 33 CFR Sec. 160.203, Certain Dangerous Cargoes and Hazardous Conditions – Definitions

Certain dangerous cargo includes any of the following:

(a) Division 1.1 or 1.2, explosive materials, as defined in 49 CFR 173.50.

(b) Division 5.1, Oxidizing materials, or Division 1.5, blasting agents, for which a permit is required under 49 CFR 176.415, or for which a permit is required as a condition of a Research and Special Programs Administration exemption.

(c) Division 4.3, Spontaneously Combustible products in excess of 60 metric tons per vessel.

(d) Division 6.1, Poison-Inhalation Hazard, products in bulk packagings.

(e) Class 7, highway route controlled quantity radioactive material, or fissile material, controlled shipment, as defined in 49 CFR 173.403.

(f) Each cargo under Table 1 of 46 CFR part 153 when carried in bulk.

(g) Each cargo under Table 4 of 46 CFR part 154 when carried in bulk.

(h) Butylene Oxide, Chlorine, and Phosphorous, elemental when carried in bulk.

Hazardous condition means any condition that may adversely affect:

(1) the safety of any vessel, bridge, structure, or shore area; or

(2) the environmental quality of any port, harbor, or navigable waterway.

It may, but need not, involve collision, allision, fire, explosion, grounding, leaking, damage, injury or illness of a person aboard, or manning-shortage.

APPENDIX 2

RMI Mandatory Requirements for Ships Operating in U.S. Waters

The Administrator has identified the following paragraphs (as indicated by numbers after the bullet) of ISPS Code Part B, which shall be considered mandatory for RMI registered ships operating in U.S. waters:

- 1.9, Designating, in writing, by name or title, a CSO and a Vessel Security Officer (VSO) for each vessel; identify how those officers can be contacted at any time; and ensuring these personnel receive training, drills, and exercises enabling them to perform their assigned security duties;
- 5.4, Achieving the main purpose of a DoS;
- 6.1, Companies providing the Master and the CSO, with the following information:
  - (i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractor, and concessionaires (for example, retail sales outlets, casinos, etc.);
  - (ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and
  - (iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters;
- 8.1, With respect to the responsibilities of the CSO, a CSO may perform other duties within the owner or operator's organization, provided he or she is able to perform the duties and responsibilities required of a CSO, and may delegate duties required by this part, but remains responsible for the performance of those duties;
- 8.3, An SSA addressing specified elements on board or within the ship;
- 8.4, Those involved in a SSA being able to draw upon expert assistance;
- 8.5, The CSO obtaining and recording listed information required to conduct an assessment;
- 8.6, The SSA examining each identified point of access, including open weather decks, and its potential for use by individuals who might seek to breach security;
- 8.7, The SSA considering the continuing relevance of existing security measures and guidance procedures and operations;
- 8.8, The SSA considering the persons, activities, service and operations that it is important to protect;
- 8.9, The SSA considering all possible threats, including the listed types of security incidents;
- 8.10, The SSA taking into account all possible vulnerabilities, including those listed in the Code;

- 8.11, CSO and SSO giving particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods;
- 8.14, The on-scene security survey examining and evaluating existing shipboard protective measures, procedures and operations listed areas;
- 9.1 through 9.4, The SSP development, format, submission and approval;
- 9.7.5, The type and maintenance requirements of security and surveillance equipment and systems;
- 9.9, The SSP establishing the security measures covering all means of access to the ship identified in the SSA;
- 9.10, The identification of the types of restriction or prohibition to be applied and the means of enforcing them;
- 9.11, Establishing for each security level the means of identification required to allow access to the ship;
- 9.12, Denying access to the ship those who fail to identify themselves or account for their presence on board;
- 9.13, Establishing in the approved SSP the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis;
- 9.14, Security Level 1 security measures to control access to the ship;
- 9.15, Security Level 1 personal search procedures;
- 9.16, Security Level 2 heightened security measures to control access to the ship;
- 9.17, Security Level 3 additional security measures to control access to the ship;
- 9.18 through 9.24, Restricted Areas on the Ship;
- 9.25 through 9.32, Handling of Cargo;
- 9.33 through 9.37, Delivery of Ship's Stores;
- 9.38 through 9.41, Handling Unaccompanied Baggage;
- 9.42, through 9.49, Monitoring the Security of the Ship;
- 9.52, The SSP describing how a request for a DoS from a facility will be handled and the circumstances under which the ship itself should request a DoS;
- 10.1 and 10.2, Record keeping and availability of records;
- 13.1, CSO general knowledge, through training or equivalent job experience;

- 13.2, SSO general knowledge, through training or equivalent job experience;
- 13.3, Company and vessel personnel responsible for security duties having knowledge, through training or equivalent job experience to perform their assigned duties;
- 13.4, Regarding all other shipboard personnel having sufficient knowledge of and familiarity with relevant provisions of the SSP;
- 13.6, Drills;
- 13.7, Exercises;

  (i) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises;

  (ii) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response;

  (iii) Exercises are a full test of the security program and must include the substantial and active participation of relevant company and vessel security personnel, and may include facility security personnel and government authorities depending on the scope and the nature of the exercises; and

- 18.6, If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility's scheduled drill.

APPENDIX 3

RMI Mandatory Requirements for Ships Operating in European Community Waters

The Administrator has identified the following paragraphs (as indicated by numbers after the bullet) of ISPS Code Part B, which shall be considered mandatory for RMI registered ships operating in EU waters:

- 1.12, On continuous checking of the relevance of SSPs, and their revision;
- 1.16, On port facility security assessment;
- 4.1, On protection of the confidentiality of security plans and assessments;
- 4.4, On recognized security organizations;
- 4.5, On the minimum competency of the RSO which can be authorized by Member States to assess the security of port facilities and, on behalf of the competent administrations of the Member States, to approve and verify the SSPs and certify ships' conformity with regard to security;
- 4.8, On setting the security level;
- 4.14-4.16, On contact points and information on port facility security plans
- 4.18, On identity documents for government officials appointed to inspect security measures;
- 4.24, On ships' application of the safety measures recommended by the State in whose territorial waters they are sailing;
- 4.28, On observance of the new requirements generated by security tasks when ships' crews are selected;
- 4.41, On communication of information when entry into port is denied or the ship is expelled from port;
- 4.45, (On ships from a State whish is not party to the Convention
- 6.1, On the Company's obligation to furnish the Master with information on the ship's operators;
- 8.3 to 8.10, On the minimum standards to be observed with regard to assessment of the security of the ship;
- 9.2, On the minimum standards to be observed with regard to assessment of the SSP;
- 9.4, On independence of recognized security organizations;
- 13.6 and 13.7, On the frequency of security training, drills and exercises for ships' crews and for Company and Ship Security Officers; and
- 15.3-15.4, On minimum standards for port facility security assessment.

INDEX