MAY 20, 2003

CIRCULAR NO. 9/03

TO MEMBERS OF THE ASSOCIATION

Dear Member:

MARITIME SECURITY – NEW REQUIREMENTS UNDER SOLAS

As a result of a Diplomatic Conference which took place in London in December 2002, the International Maritime Organization (IMO) has made significant amendments to the Safety of Life at Sea (SOLAS) Convention in order to enhance maritime security.

Many of the new regulations take effect next year and are mandatory. Since there is relatively little time before these measures come into force, and since there is unlikely to be an extension of the date from which they will be applied, Members are advised to begin their preparations for compliance as soon as possible.

Several of the major changes are reviewed in the remainder of this Circular. However, the information contained herein is not exhaustive and Members are urged to refer directly to the amended regulations for a complete view of their requirements.

Automatic Information Systems (AIS)

SOLAS, Chapter V (Safety of Navigation), Regulation 19 sets out a new timetable for the fitting of AIS. Vessels, other than passenger vessels and tankers, of 300 GT and above, but less than 50,000 GT, are required to fit AIS not later than the first safety equipment survey after July 1, 2004 or by December 31, 2004, whichever occurs earlier.

Existing AIS compliance dates for passenger vessels (not later than July 1, 2003), for tankers (not later than the first survey for safety equipment on or after July 1, 2003) and for other ships of 50,000 GT and above (not later than July 1, 2004) remain unchanged.

Vessels equipped with AIS are to operate them at all times except where international agreements, rules or standards provide for the protection of navigational information.

Ship Identification Numbers (SIN)

Chapter XI of SOLAS (entitled *Special Measures to Enhance Maritime Safety*) has been renumbered as Chapter XI-1. A modification to regulation 3 requires an SIN to be marked in a visible place on the stern, or on both sides of the hull amidships, or on the front of the superstructure. Passenger vessels may carry the marking on a horizontal surface visible from the air. The SIN is also to be marked on one of the end transverse bulkheads in the machinery space, or on one of the hatchways, or in the pump room or, if the vessel is a Ro-Ro, on one of the end transverse bulkheads in the cargo space.

All digits comprising the SIN are to be not less than 200 mm in height externally and not less than 100 mm internally, painted in a contrasting color and are to be permanently carved or raised. It would also appear that the SIN may need to be prefixed by the letters IMO. Existing vessels are to comply with this requirement no later than the first scheduled dry-docking after July 1, 2004.

Continuous Synopsis Records (CSR)

Regulation 5 of SOLAS Chapter XI-1, requires vessels to maintain a CSR with effect from July 1, 2004. Responsibility for the issuance of this document falls to flag administrations.

The CSR is intended to chronicle a vessel's history. It will contain information such as the vessel's name, identification number, flag state, date of registration, port of registry, classification society, name and address of company and address from where a company's safety management activities are conducted, name of the owner(s) and their address(es), name of the bareboat charterer(s) and their address(es) and name of the organization(s) which issued the company's Document of Compliance, the vessel's Safety Management Certificate and the International Ship Security Certificate.

All changes are to be recorded in the CSR which is to be retained on board throughout a vessel's life regardless of changes in management or ownership. A CSR must be available for inspection at all times.

Ship Security Alert Systems (SSAS)

A new Chapter XI-2 has been added to SOLAS entitled *Special Measures to Enhance Maritime Security*. Regulation 6 of this Chapter stipulates that all passenger vessels of any size, as well as oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft of 500 GT and above are to be fitted with an SSAS not later than the first survey of the radio installation after July 1, 2004.

All other cargo vessels of 500 GT and above are to fit such equipment not later than the first survey of the radio installation after July 1, 2006.

The SSAS must be capable of being triggered from the bridge and from at least one other location. It is to be capable of transmitting, when activated, a ship-to-shore security alert to a "*competent authority*", designated by the flag administration, identifying the vessel and its location. It would appear that many flag administrations will take a vessel's operator to be a "*competent authority*" for these purposes.

Specific Responsibility of Companies

Regulation 5 of SOLAS Chapter XI-2 requires companies to provide the master with information so as to enable port state control officers to determine who is responsible for appointing members of the crew, who is responsible for deciding the employment of the vessel and, if the vessel is on charter, who are the parties to such agreement.

The Master's Discretion in Regard to Ship Safety and Security

Regulation 8 of SOLAS Chapter XI-2 confirms the authority of the master and emphasizes his responsibility for maintaining the safety and security of a vessel.

It further entitles masters to deny access to persons or their effects, or to refuse to load cargo in order to achieve this aim, and stipulates that the master should not be constrained in this respect by the owning company or the charterer.

Regulation 8 also provides that, in the event of a conflict between safety and security imperatives, the former shall take priority. In such circumstances, a master is to implement temporary security measures and to inform the flag administration. If appropriate, the master may also inform the authorities responsible for the port concerned.

The International Ship and Port Facility Security (ISPS) Code

The ISPS Code enters into force on July 1, 2004. It applies to passenger vessels of any size, cargo vessels and high speed craft of 500 GT and above, and to mobile offshore drilling units.

Part A of the ISPS Code is mandatory and contains detailed requirements for ships, companies, port authorities, flag administrations and governments. Part B of the ISPS Code is advisory and contains guidelines on how to comply with Part A.

However, Members should be aware that the US Coast Guard has announced that it plans to make compliance with Part B obligatory for vessels trading to US ports.

The remainder of this section contains a brief discussion of the salient features of the ISPS Code which is hoped will provide at least basic guidance to Members in regard to compliance requirements.

Introduction

The ISPS Code places a number of specific responsibilities on ship operators in regard both to security management procedures and to the arrangement of human resources to fulfill them.

As a basic requirement, shipping companies must appoint a Company Security Office (CSO) ashore and a Ship Security Officer (SSO) on board every vessel operated by them. These need not be exclusive positions, and existing personnel may be nominated.

A company is also responsible for insuring that a Ship Security Assessment (SSA) is carried out on board and must also prepare a Ship Security Plan (SSP) for each vessel thereafter. SSPs are to be submitted to flag administrations or to a Recognized Security Organization (RSO) authorized by the flag administration, for approval.

Once approved – and implemented – security arrangements on board are to be verified by the flag administration or RSO. Compliance will result in a vessel being issued with an International Ship Security Certificate. This must be obtained no later than July 1, 2004. Renewal verifications are to be obtained every five years with at least one interim verification between the second and third anniversary dates.

For their part, governments are required to carry out Port Facility Security Assessments (PFSA), produce Port Facility Security Plans (PFSP) and appoint Port Facility Security Officers (PFSO) in a similar manner. However, in the case of a port facility visited by ships engaged on international voyages only occasionally, the contracting government is at liberty to decide on the extent to which the ISPS Code will apply. As a consequence, it is possible that a PFSO will not necessarily be found in every port.

Company Security Officer (CSO)

The CSO's duties include coordinating the ship security assessments, overseeing the development, submission, approval, implementation and maintenance of the Ship Security Plan, informing vessels of the levels of threat likely to be encountered, arranging internal audits and reviews of security activities, insuring that any deficiencies are rectified and organizing the initial and subsequent procedures for compliance verification.

A company may appoint more than one CSO, provided this is clear for which vessel each CSO is responsible.

Ship Security Officer (SSO)

The SSO has a variety of duties under the Code. They include supervising the implementation of the Ship Security Plan, carrying out regular security inspections of the ship, liaising with the CSO and Port Facility Security Officers as the need may arise, reporting security incidents, checking that a vessel's security equipment is functioning correctly and ensuring that crewmembers are adequately familiarized with ship board security and the individual responsibilities they have arising from it.

Port Facility Security Officer (PFSO)

The PFSO has a responsibility for implementing the Port Facility Security Plan, undertaking security inspections of the port facility on a regular basis, modifying the Port Facility Security Plan in response to changes and deficiencies, reporting and recording occurrences which may threaten security, coordinating local security services and, where requested, assisting the SSO of a visiting ship to confirm the identity of those seeking to come on board.

Ship Security Assessment (SSA)

The ISPS Code stipulates that SSA's are to be carried out by "*persons with appropriate skills*". A company may use its own staff for this purpose if they are adequately trained and subject to confirmation by the relevant flag administration.

As an alternative course of action, a company may delegate this function to an RSO. All SSA's must be documented, retained and reviewed from time to time by the company. They must also be protected from unauthorized access or disclosure.

An important part of the SSA is the "*on-scene*" survey. This process is to be used to identify the existence of any on-going security measures, key shipboard operations which require protection as well as possible threats and potential vulnerability.

Part B of the ISPS Code gives detailed advice on the conduct of such exercises.

Ship Security Plan (SSP)

The ISPS Code provides that an SSP is to be developed for each vessel based on the outcome of the SSA. On completion, the plan must be submitted to the vessel's flag administration for approval.

Where a company has used an RSO to perform the assessment and/or prepare the plan, the same organization **cannot** approve the SSP on behalf of the flag administration, or carry out verifications for the purpose of issuing certificates.

The plan should identify the SSO and the CSO. It should also address issues such as the duties of shipboard personnel, the identification of restricted areas, measures to prevent unauthorized access and safeguards to counter the illegal carrying of weapons, dangerous substances and devices.

Additionally, procedures are required for training and drills, liaison with port facility security activities, reviewing and updating the plan, dealing with security threats, responding to security instructions given by governments, reporting incidents, evacuating the vessel, performing security audits – including internal audits of the plan – and the inspection, testing and maintenance of a vessel's security equipment.

The plan is also to identify vessel security alert activation points and incorporate procedures governing the use of such equipment. As an alternative measure, information on the ship security alert system may be kept elsewhere on board in a confidential document known only to the master, the SSO and other senior personnel within the company.

In normal circumstances, a vessel's SSP is not subject to inspection by port state control officers. However, if port state control officers believe that a vessel is not complying with SOLAS Chapter XI-2 or Part A of the ISPS Code, limited access may exceptionally be allowed subject to the consent of the flag administration or the master and only in circumstances where the sole means to verify or rectify the apparent non-compliance is to review the relevant parts of the SSP.

Levels of Security

Three levels of security are envisaged – and to be provided for – in the compilation of the SSP. They are as follows:

Level 1 (Normal): The level at which the vessel will normally operate. Minimum requirements include ensuring the performance of all vessel security duties, controlling access, checking identities, locking unattended spaces, monitoring deck areas, restricted areas and areas surrounding the vessel, supervising the handling of cargo and vessel stores, and ensuring that security communication is ready for use.

Level 2 (Heightened): The level applying for as long as there is a heightened risk of a security incident. This may entail deploying additional personnel to deter unauthorized access, stepping up security patrols, limiting the number of access points to the vessel, escorting visitors, carrying out searches and, in cooperation wit the port facility, establishing a restricted area ashore adjacent to the vessel and deterring waterside access.

Level 3 (Exceptional): The level applying for the period of time when there is the probable or imminent risk of a security incident. Maximum precautions may include establishing a single, controlled access point, suspending embarkation/disembarkation, granting access only to those

responding to the security situation, suspending cargo operations and deliveries, and moving or evacuating the vessel.

Levels of security will be set by Contracting Governments – being flag administrations or port states. If a flag administration requires shipboard security to be increased to Level 2 or Level 3 for a certain port or region, vessels affected are obligated to acknowledge receipt of such instructions.
Where a port requires Level 2 or Level 3 security, a vessel must acknowledge receipt of the order and contact the Port Facility Security Officer to confirm that the applicable measures in the SSP have been implemented to accomplish this status. In the event of compliance difficulties, the PFSO and SSO are to discuss and agree a suitable course of action.

Circumstances may occur where a flag administration requires a higher security level for a particular port than that set by the government of the country concerned. If so, a vessel is to notify the competent authority of the port state and the PFSO without delay. In addition, the SSO is to liaise with the PFSO and coordinate appropriate action.

This may include the making of a Declaration of Security. This is a formal agreement made between a vessel and a port facility concerning the security measures that each will apply and setting out their respective responsibilities. Either party may initiate the process if they consider such an undertaking to be needed.

A Declaration of Security may be appropriate at higher security levels; where a vessel is operating at a higher security level than a port facility or another vessel with which it is interfacing; if there has been a security threat or security incident involving a specific vessel or port facility; where a vessel calls out of port lacking a PFSP; during ship-to-ship activities with a vessel which does not have or require an approved SSP; or if there is an agreement between Contracting Governments regarding certain international voyages or specific vessels engaged in such voyages.

Part B of the ISPS Code contains a specimen Declaration of Security form for Members' reference.

Training

SSOs and the CSO must be trained in accordance with the broad guidance summarized in Part B of the ISPS Code. The provision of training is a company responsibility and records must be maintained.

Although the ISPS Code does not specify how CSO/SSO training is to be conducted, IMO model courses are being developed. In the interim, however, it would appear that companies are free to make their own arrangements using in-house or external resources as they see fit. Members are advised to check whether their flag administration has introduced any additional requirements regarding the scope or duration of such training.

Shipboard personnel with security duties must be familiarized with their responsibilities as described in the SSP. All other crewmembers should be informed of those provisions relevant to them – e.g. the meaning of different security levels, knowledge of emergency procedures and techniques used to circumvent security. The SSO in the ordinary way will be expected to carry out this task and ensure that all details are recorded.

In conjunction with training, security drills are to be held on board at least once every three months to promote the effective implementation of the SSP. If more than one quarter of a vessel's crew is changed at any one time, the newly-joining personnel must take part in the security drill within their first week on board.

In addition, a company is required to organize a full scale exercise or "tabletop" simulation each year involving the CSO and as many other interested parties as possible. Not more than 18 months are to elapse between such exercises.

Maintaining Records

Subject to any additional flag administration requirements, records of the following activities are to be maintained on board a vessel as a minimum requirement of compliance:

- Training, drills and exercises.

- Security threats, security incidents and breaches of security.
- Changes in security levels.
- Communications relating to the direct security of the vessel.
- Internal audits and reviews of security activities.
- Periodic reviews of the SSA and SSP.
- Implementation of any amendments to the SSP.
- Maintenance, calibration and testing of any security equipment on board, including testing of the Ship's Security Alert System.

The new regulations require that the SSP and all security records are to be written in the working language of the vessel. If not English, French or Spanish, a translation into one of these languages is required. Should such information be held in electronic format, it is to be protected from unauthorized access or disclosure, and from unauthorized deletion, destruction or amendment.

Control and Compliance Provisions

Chapter XI-2, Regulation 9 of SOLAS sets out the action which may be taken by port state control authorities if a vessel is found to lack a valid International Ship Security Certificate, or if there are "*clear grounds*" for believing that the vessel does not comply with the relevant requirements. Such measures may entail inspection, delay, detention, restriction of operations, limitation of movement or expulsion.

Before entering port, a vessel may be asked to provide details of its International Ship Security Certificate, the names of the last ten port facilities is as visited and the security measures taken at each. Records must be maintained on board for this purpose.

If such information gives the port authorities "*clear grounds*" to think that a vessel is not in compliance, it may be required to rectify the non-compliance, proceed to a specified location within territorial limits or submit to an inspection. Alternatively, and in any event, entry of the vessel into port may be denied.

Further Action

As will be clear from the foregoing, these new maritime security requirements are extensive and operationally demanding. Once again, Members are urged – in view of the short lead time and the unlikely prospect of an extension – to start work on securing compliance without delay.

The Club is currently taking steps to see what further resources may be available to Members from industry publications in regard to the training of SSOs in particular. It is believed that certain organizations may be on the point of issuing instructional videos etc. in this respect and the Managers will be in further contact with Members as to their availability in due course.

In the meantime, and as always, the Managers will be pleased to respond to any inquires Members may have in regard to the foregoing, or generally.

Yours faithfully,
Joseph E.M. Hughes, Chairman & CEO
Shipowners Claims Bureau, Inc., Managers for
THE AMERICAN CLUB

CIRCULAR 9.03 5-20-03