



VMS MB 110  
APRIL 2003

## MARITIME SECURITY

By: Dr. James Cowley

### Republic of Vanuatu Maritime Bulletin

The primary purpose of this Bulletin is to inform Vanuatu's shipowners, ship operators and ships' personnel of the recently produced mandatory requirements relating to Maritime Security adopted at a Diplomatic Conference and the urgent need to take action on their implementation. This Bulletin should not be used as a substitute for a detailed study of the Regulations.

#### Background to the New Security Requirements

##### *Terrorism*

The International Maritime Organization (IMO) has recognised the vulnerability of shipping to unlawful acts in its existing legislation. However, the increased scale of terrorist activities, as exemplified by the unprecedented carnage of the attacks on September 11, 2001, led IMO to initiate more comprehensive regulatory measures.

##### *Unanimity*

At the IMO Assembly in December 2001, the Member Countries unanimously adopted Resolution A.22/924, which requested the Maritime Safety Committee (MSC), the Legal Committee and the Facilitation Committee to revise existing legislation and prepare new measures for the protection of shipping and seafarers.

Following these decisions, the work of the Committees and their Working Groups led to a Diplomatic Conference, at IMO, in December 2002. The Conference adopted the comprehensive legislation outlined in the following pages of this Bulletin. In addition, the Legal Committee established a Correspondence Group charged with updating the existing Instruments i.e., the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Transport (SUA Convention) and its Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (SUA PROT).

Vanuatu's former Permanent Representative participated in these meetings and the Diplomatic Conference and served on the Correspondence Group.

##### *Legislative Measures*

These new Security Regulations will be included in a revised SOLAS chapter XI entitled "Special Measures to Enhance Safety and Maritime Security", divided into two parts as follows:

SOLAS XI-1: Special Measures to enhance Maritime Safety (existing text); and  
SOLAS XI-2: Special Measures to enhance Maritime Security (new text).

The regulations of SOLAS XI-2 refer to "The International Ship and Port Facility Security (ISPS) Code". This Code is in two parts – A and B. Part A is made mandatory and will be subject to amendment only by the provisions of article VIII of SOLAS using the same processes as for the parent chapter. Part B is recommendatory but some Contracting Governments may make it mandatory in their ports and ships. Some Conference delegates at IMO said that Part B should be treated as "quasi mandatory". Part B will be subject to amendment through the Maritime Safety Committee's Rules of Procedure. **N.B.** To avoid repetition in various sections of this Bulletin, it must



be recognized that in implementing these requirements account should always be taken of the guidance given in Part B of the ISPS Code.

### ***Wider Aspects***

The provisions of chapter XI-2 and the ISPS Code apply to ships and the essential aspects of ship/port interface. It is essential, therefore, that readers with shipping-related interests read and understand the sections of the requirements for ports and vice-versa. The provisions do not include the wider aspects of port security. The Joint ILO/IMO Working Group on Port Security will cover the latter and prepare a report for the parent bodies.

Also, the new provisions do not extend to the actual response to terrorist attacks or to any clean-up activities after attacks.

### **Application Date and Urgency**

#### ***Date***

The new requirements apply as from 1 July 2004.

#### ***No Extensions***

Neither chapter XI-2 of the Convention nor the ISPS Code provide for any extension of the implementation dates for the introduction of the special measures concerned to enhance maritime security. This means that Contracting Governments must, as a matter of high priority, finalize any legislative or administrative arrangements, which are required at the national level, to give effect to the requirements of the adopted amendments to the Convention (and the ISPS Code).

#### ***Submissions***

Contracting Governments should establish submission dates by which requests are made for:

- review and approval of ship security plans;
- verification and certification of ships; and
- review and approval of port facility security assessments and of port facility security plans.

These submission dates should be well in advance of the application date of 1 July 2004 to allow Contracting Governments, Administrations and recognized security organizations time to complete the review and approval and the verification and certification processes and for Companies, ships and port facilities to rectify any non-compliances.

Shipowners should now be urgently preparing to meet these submission dates and the requirements which include: Marking of Ship Identification Numbers on their ships; Automatic Identification Systems; Ship Security Alarm Systems; and Continuous Synopsis Records; etc., outlined under "Amendments to SOLAS" later in this Bulletin.

#### ***Acceptance of Plans and Certificates***

Other Contracting Governments (e.g. as port States), on and after 1 July 2004, should recognize and accept as valid and as meeting the requirements of chapter XI-2 of the Convention and part A of the ISPS Code any: Ship security plans approved and International Ship Security Certificates issued, prior to 1 July 2004, in accordance with the provisions of part A of the ISPS Code, by Administrations (e.g. flag States) or, on their behalf, by recognized security organizations.

It is vital that all necessary infrastructure is in place in time for the effective implementation of the new measures to enhance maritime security on board ships and ashore or ships will be subject to detention.

### ***Personnel Matters***

Prior to 1 July 2004, Companies must appoint and provide training and instructions in maritime security matters for the company security officer, the ship security officer and other relevant personnel.

### ***Application***

The new requirements apply to:

(a) the following types of ships engaged on international voyages:

- .1 passenger ships including passenger high-speed craft; and
- .2 cargo ships, including cargo high speed craft, of 500 gross tonnage and upwards; and
- .3 mobile offshore drilling units; and

(b) port facilities serving such ships engaged on international voyages.

### **Communication of Information to IMO**

#### ***Details of Contact Points***

NOT LATER THAN 1 July 2004, Contracting Governments have to communicate to IMO and make available for the information of Companies and ships:

- the names and contact details of their national authority or authorities responsible for ship and port facility security;
- the locations within their territory covered by the approved port facility security plans;
- the names and contact details of the competent authority designated to be available at all times to receive and act upon ship-to-shore security alerts;
- the names and contact details of those who have been designated to be available at all times to receive and act upon any communications from Contracting Governments exercising control and compliance measures; [N.B. these contact details are analogous to those provided by flag States to receive reports of detentions by Port State Control Officers];
- the names and contact details of the contact point(s) designated to be available at all times to provide advice or assistance to ships and to whom ships can report any security concerns.

#### ***Details of RSOs***

Contracting Governments must communicate to IMO names and contact details of any recognized security organizations (RSOs) authorized to act on their behalf together with details of the specific responsibility and conditions of authority delegated to such organizations. Vanuatu intends to recognize the security organizations of the full Members of IACS.

#### ***Security Plans***

Also, Contracting Governments have to provide IMO with a list showing the approved port facility security plans for the port facilities located within their territory together with the locations covered by each such plan and the corresponding date of approval.

#### ***Updating***

The above information must be updated as and when significant changes are made and, in any case, revised and updated lists of port facility security plans must be provided at subsequent five-year intervals.



### ***Circulation***

IMO will circulate relevant particulars relating to the above communications to other Contracting Governments for the information of their officers.

### **The International Ship and Port Facility Security (ISPS) Code**

The Objectives of the ISPS Code are:

- to establish an international framework involving co-operation between, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;
- 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;
- to ensure the early and efficient collection and exchange of security-related information;
- to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
- to ensure confidence that adequate and proportionate maritime security measures are in place.

The Functional Requirements of the ISPS Code include:

- gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
- requiring the maintenance of communication protocols for ships and port facilities;
- preventing unauthorized access to ships, port facilities and their restricted areas;
- preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;
- providing means for raising the alarm in reaction to security threats or security incidents;
- requiring ship and port facility security plans based upon security assessments; and
- requiring training and drills to ensure familiarity with security plans and procedures.

### **Security Levels and Declaration of Security**

Ships and ports will operate according to one of three security levels, as follows:

**Security level 1:** means the level for which minimum appropriate protective security measures shall be maintained at all times.

**Security level 2:** means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

**Security level 3:** means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

### ***Declaration of Security***

A Declaration of Security is a form of agreement that addresses the security requirements to be shared between a port facility and a ship (or between ships), which must state the responsibilities that each Party will undertake in accordance with the provisions of their respective security plans.

Contracting Governments determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment.

Also, a ship can request completion of a Declaration of Security when:

- the ship is operating at a higher security level than the port facility or another ship it is interfacing with;
- there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
- there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
- the ship is at a port which is not required to have and implement an approved port facility security plan; or
- the ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.

The Declaration of Security must be completed by:

- the master or the ship security officer on behalf of the ship(s); and, if appropriate,
- the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

On receipt of a request for the completion of a Declaration of Security, the applicable port facility or ship, as appropriate, must acknowledge receipt of the request.

## Obligations of Contracting Governments

### ***Setting Security Levels***

It is for Contracting Governments to set security levels and provide guidance for protection from security incidents. When making their decisions on security levels to ships operating in their territorial seas or ports or on their own ships, they should take into consideration:

- the degree that the threat information is credible;
- the degree that the threat information is corroborated;
- the degree that the threat information is specific or imminent; and
- the potential consequences of such a security incident.

When setting security level 3, Contracting Governments must issue appropriate instructions and provide security-related information to the ships and port facilities that may be affected.

### ***Direct Responsibilities***

Contracting Governments are, themselves, responsible directly for carrying out the following tasks:

- setting of the applicable security level;
- approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;
- determining the port facilities which will be required to designate a Port Facility Security Officer;
- approving a Port Facility Security Plan and subsequent amendments to an approved plan;
- exercising control and compliance measures pursuant to regulation XI-2/9; and
- establishing the requirements for a Declaration of Security.



Other tasks may be delegated to a recognized security organization but Contracting Governments must test the effectiveness of the Ship or the Port Facility Security Plans they have approved or, in the case of ships, of Plans that have been approved on their behalf.

### **Obligations of the Company- Personnel and Ship Security**

#### ***Company Security Officer***

The Company must designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate, designate several persons as company security officers provided it is clearly identified for which ships each person is responsible. The duties and responsibilities of the company security officer include:

- advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- ensuring that ship security assessments are carried out;
- ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- arranging for internal audits and reviews of security activities;
- arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;
- ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
- enhancing security awareness and vigilance;
- ensuring adequate training for personnel responsible for the security of the ship;
- ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;
- ensuring consistency between security requirements and safety requirements;
- ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

#### ***Ship Security Officer***

A ship security officer must be designated on each ship whose duties and responsibilities include:

- undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
- coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
- proposing modifications to the ship security plan;
- reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
- enhancing security awareness and vigilance on board;

- ensuring that adequate training has been provided to shipboard personnel, as appropriate;
- reporting all security incidents;
- coordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and
- ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

### ***Training***

The company security officer, appropriate shore-based personnel and the ship security officer must have requisite knowledge and have received training, taking into account the guidance given in part B of the ISPS Code.

Shipboard personnel having specific security duties and responsibilities must understand their responsibilities for ship security as described in the ship security plan and must have sufficient knowledge and ability to perform their assigned duties.

To ensure the effective implementation of the ship security plan, drills must be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances.

The company security officer must ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals.

### ***Master's Authority***

The Company must ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company must establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

The Company must ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfill their duties and responsibilities.

### ***Ship Security***

A ship is required to act upon the security levels set by Contracting Governments as set out below taking into consideration the guidance given in part B of the ISPS Code.

**Security Level 1:** The following activities must be carried out, through appropriate measures, on all ships in order to identify and take preventive measures against security incidents:

- ensuring the performance of all ship security duties;
- controlling access to the ship;
- controlling the embarkation of persons and their effects;
- monitoring restricted areas to ensure that only authorized persons have access;
- monitoring of deck areas and areas surrounding the ship;
- supervising the handling of cargo and ship's stores; and
- ensuring that security communication is readily available.

**Security Level 2:** The additional protective measures, specified in the ship security plan, must be implemented for each activity detailed above for security level 1.



**Security Level 3:** Further specific protective measures, specified in the ship security plan must be implemented for each activity detailed above for security level 1.

N.B. The ISPS Code specifies detailed provisions regarding notification, acknowledgment and co-operation whenever security levels 2 or 3 are specified.

### ***Ship Security Assessment***

It must be emphasized that: the ship security assessment is an essential and integral part of the process of developing and updating the ship security plan; and that the company security officer must ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with the ISPS Code. Subject to certain conditions, a recognized security organization may carry out the ship security assessment of a specific ship. The ship security assessment must include an on-scene security survey and, at least:

- the identification of existing security measures, procedures and operations;
- the identification and evaluation of key ship board operations that it is important to protect;
- the identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- the identification of weaknesses, including human factors in the infrastructure, policies and procedures.

The ship security assessment must be documented, reviewed, accepted and retained by the Company.

### ***Ship Security Plan***

Every ship must carry on board a ship security plan approved by the Administration that makes provision for the three security levels.

A recognized security organization may prepare the ship security plan for a specific ship.

The Administration may entrust the review and approval of ship security plans or of amendments to a previously approved plan, to a recognized security organization provided that the organization has not been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

The submission of a ship security plan, or of amendments to a previously approved plan, for approval must be accompanied by the security assessment on the basis of which the plans, or the amendments, have been developed.

The security plan must address, at least, the following:

- measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;
- identification of the restricted areas and measures for the prevention of unauthorized access to them;
- measures for the prevention of unauthorized access to the ship;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- procedures for responding to any security instructions Contracting Governments may give at security level 3;
- procedures for evacuation in case of security threats or breaches of security;



- duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- procedures for auditing the security activities;
- procedures for training, drills and exercises associated with the plan;
- procedures for interfacing with port facility security activities;
- procedures for the periodic review of the plan and for updating;
- procedures for reporting security incidents;
- identification of the ship security officer;
- identification of the company security officer including 24-hour contact details;
- procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
- frequency for testing or calibration of any security equipment provided on board;
- identification of the locations where the ship security alert system activation points are provided; and
- procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

### ***Internal Audits***

Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

### ***Changes***

The Administration must determine which changes to an approved ship security plan or to any security equipment specified in an approved plan must not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes must be at least as effective as those measures prescribed in chapter XI-2 and the ISPS Code.

### ***Electronic Format***

The plan may be kept in an electronic format. In such a case, it must be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. The plan must be protected from unauthorized access or disclosure.

### ***Control***

Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9 (Control) unless such officers have clear grounds for believing that the ship is not in compliance with the requirements of chapter XI-2 or part A of the ISPS Code and the non-compliance cannot otherwise be rectified.

### ***Records***

Records of the following activities addressed in the ship security plan must be kept on board for at least the minimum period specified by the Administration:

- training, drills and exercises;
- security threats and security incidents;
- breaches of security;
- changes in security level;
- communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- internal audits and reviews of security activities;
- periodic review of the ship security assessment;

- periodic review of the ship security plan;
- implementation of any amendments to the plan; and
- maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

The records may be kept in an electronic format. In such a case, they must be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment and unauthorized access or disclosure.

## Amendments to the SOLAS Convention

### Automatic Identification Systems

The requirements for automatic identification systems (AIS) are now extended to include ships, other than passenger ships and tankers, of 300 gross tonnage and upwards but less than 50,000 gross tonnage, not later than the first safety equipment survey\* after 1 July 2004 or by 31 December 2004, whichever occurs earlier. (NB \*The first safety equipment survey means the first annual survey, the first periodical survey or the first renewal survey for safety equipment, whichever is due first after 1 July 2004 and, in addition, in the case of ships under construction, the initial survey.)

Ships fitted with AIS must maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.

### Ship Identification Number

The ships identification number (IMO/LR No.) must be permanently marked and painted in a contrasting color not later than the first scheduled dry-docking of the ship after 1 July 2004:

- in a visible place either on the stern of the ship or on either side of the hull, amidships port and starboard, above the deepest assigned load line or either side of the superstructure, port and starboard or on the front of the superstructure or, in the case of passenger ships, on a horizontal surface visible from the air; and
- in an easily accessible place either on one of the end transverse bulkheads of the machinery spaces, or on one of the hatchways or, in the case of tankers, in the pump-room or, in the case of ships with ro-ro spaces, on one of the end transverse bulkheads of the ro-ro spaces.

### Continuous Synopsis Record

A Continuous Synopsis Record, intended to provide an on-board record of the history of the ship, must be issued by the Administration to each ship that is entitled to fly its flag and it must contain at least, the following information:

- the name of the State whose flag the ship is entitled to fly;
- the date on which the ship was registered with that State;
- the ship's identification number;
- the name of the ship;
- the port at which the ship is registered;
- the name of the registered owner(s) and their registered address(es);
- the name of the registered bareboat charterer(s) and their registered address(es), if applicable;



- the name of the Company, its registered address and the address(es) from where it carries out the safety management activities;
- the name of all classification society(ies) with which the ship is classed;
- the name of the Administration or of the Contracting Government or of the recognized organization which has issued the Document of Compliance to the Company operating the ship and the name of the body which has carried out the audit on the basis of which the document was issued, if other than that issuing the document;
- the name of the Administration or of the Contracting Government or of the recognized organization that has issued the Safety Management Certificate to the ship and the name of the body which has carried out the audit on the basis of which the certificate was issued, if other than that issuing the certificate;
- the name of the Administration or of the Contracting Government or of the recognized security organization that has issued the International Ship Security Certificate, as specified in the ISPS Code, to the ship and the name of the body which has carried out the verification on the basis of which the certificate was issued, if other than that issuing the certificate; and
- the date on which the ship ceased to be registered with that State.

Any changes relating to the entries must be recorded in the Continuous Synopsis Record so as to provide updated and current information together with the history of the changes.

For ships constructed before 1 July 2004, the Continuous Synopsis Record must, at least, provide the history of the ship as from 1 July 2004.

N.B. There are other requirements relating to the in-service use of the Continuous Synopsis Record.

### Ship Security Alert Systems

All ships must be provided with a ship security alert system, as follows:

- ships constructed on or after 1 July 2004;
- passenger ships, including high-speed passenger craft, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;
- oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004; and
- other cargo ships of 500 gross tonnage and upwards and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.

The ship security alert system, when activated, must:

- initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;
- not send the ship security alert to any other ships;
- not raise any alarm on-board the ship; and
- continue the ship security alert until deactivated and/or reset.

The ship security alert system must:

- be capable of being activated from the navigation bridge and in at least one other location; and
- conform to performance standards not inferior to those adopted by the Organization.

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

The requirement for a ship security alert system may be complied with by using the radio installation fitted for compliance with the requirements of SOLAS chapter IV, provided all requirements of this regulation are complied with.

When an Administration receives notification of a ship security alert, that Administration must immediately notify the State(s) in the vicinity of which the ship is presently operating.

When a Contracting Government receives notification of a ship security alert from a ship which is not entitled to fly its flag, that Contracting Government must immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

### Sources of Information

#### ***IACS***

To achieve consistency of the verification of compliance with the requirements of the ISPS Code, the IACS members have developed the following documents and are placing them on the IACS website ([www.iacs.org.uk](http://www.iacs.org.uk)):

**PR 24 Procedural Requirements for ISPS Code Certification**, which defines the verification, process, and describes how audits are to be conducted and reported.

**PR 25 Procedure for Training and Qualification of ISPS Code Auditors**, which defines the competency requirements for auditors, and describes the detailed theoretical and practical training to be undertaken.

**PR 26 Procedure for Reporting the List of Ships complying with the ISPS Code**, which defines the establishment of a list by which the Organization can be advised of the progress made by the IACS members acting as RSO's on behalf of the Contracting Governments in the verification of ships in compliance with the ISPS Code.

#### ***Lloyds register***

Lloyds register have published a comprehensive **IPSP Practical Pack** guide on their website ([www.lr.org](http://www.lr.org)) to assist owners and operators in meeting the new requirements.

#### ***Concluding Comment***

Maritime security procedures and legislation are continually being developed and already there is an unprecedented workload for all parties involved to meet the deadline of 1 July 2004. It is hoped that this Bulletin has been helpful to the reader.