

Luxembourg, 12<sup>th</sup> September 2006

**CIRCULAR CAM 05/2006.**

The present circular replaces and withdraws circular CAM 05/2004 dated 28<sup>th</sup> May 2004.

**To : ALL ACCREDITED SHIPPING MANAGERS**

**O/Ref : AH/49249**

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

**1. Introduction**

The diplomatic Conference on Maritime Security held in London in December 2002 adopted new provisions to the International Convention for the safety of Life at Sea (SOLAS), 1974 and the International Code for the Security of Ships and of Port Facilities (ISPS Code) to enhance maritime security. The ISPS Code is entering into effect internationally on the 1<sup>st</sup> of July 2004 and is consisting of Part A (the provisions of which shall be treated as mandatory) and Part B (the provisions of which shall be treated as recommendatory).

The purpose of the Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities.

The term "*company*" used in this circular 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 owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code ( SOLAS 74 Regulation IX/1).

**2. Purpose**

The ISPS Code and the adopted amendments to SOLAS 74 leave several issues up to the Administration of the Member States to decide or to clarify. This circular should serve as guidance and advice in order to enable companies and all other involved actors to implement the new requirements on Luxembourg flagged vessels and make the necessary arrangements to ensure prompt and completed compliance with the Code.

However this circular, which does not cover port facilities but only addresses ships, is not intended to be all-inclusive or to prevent companies from incorporating procedures that go beyond the Code when developing a ship's security program on board their vessels.

### **3. Additional European Requirements**

At European level, Regulation (EC) N° 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security is now in force. This regulation harmonizes the implementation of the ISPS Code within Member States and renders elements of Part B of the Code mandatory. All companies have to comply with the whole regulation.

It is reminded that the following paragraphs of Part B of the ISPS Code have to be considered mandatory for ships flying the Luxembourg flag:

- 1.12 : revision of ship security plans;
- 4.1 : protection of the confidentiality of security plans and assessments;
- 4.4 : Recognised Security Organisation (RSO);
- 4.5 : minimum competencies of RSO (to be documented);
- 4.8 : setting the security level;
- 4.16 : contact points and information on port facility security plans (contact details will be provided when available);
- 4.18 : identification documents;
- 4.24 : ship's application of the security measures recommended by the States in whose territorial waters they are sailing;
- 4.28 : manning levels;
- 4.41 : communication of information when entry into port is denied or the ship is expelled from port:
- 6.1 company's obligation to provide the Master with information on the ship's operator;
- 8.3 to 8.10 : minimum standards for the ship security assessment;
- 9.2 : minimum standards for the ship security plan;
- 9.4 : independence of RSO;
- 13.6 and 13.7 : frequency of security drills and exercises for ships' crews and for company and ship security officers (CSO and SSO).

### **4. Generalities**

#### **4.1 Recognised Security Organizations recognized by the State**

The following classification societies have been authorised to act as a RSO on behalf of Luxembourg: ABS, BV, DNV, GL, LRS, NKK, RINA. The following related duties have been delegated :

- the approval of ship security plan, or amendments thereto ;
- the on-board verification and certification of compliance of ships with the requirements of chapter XI-2 and Part A (and selected items) of the ISPS Code ;
- RSOs may also advise or provide assistance to companies on security matters, including the ship security assessments (SSA) and the ships security plans (SSP). However if a RSO has done so, that RSO will not be authorized to approve those documents nor to issue the required certificate on behalf of Luxembourg.

## **4.2 Validity of an international ship security certificate**

In principle the certificate follows the validity of any other SOLAS certificate. A full term period shall not exceed 5 years. However if the ship is at sea when the certificate expires, Section 19.3.5 Part A of the ISPS Code, allows for an extension.

## **4.3 The National Focal Point for security matters**

The National Focal Point for security matters is:

### **COMMISSION FOR MARITIME AFFAIRS**

26, place de la Gare - L1616 Luxembourg

Tel. : + 352 478 44 53 (during office hours: 08h00 – 17h00)

Fax : + 352 29 91 40

Tel. : + 352 621 350 490 (after office hours)

Email : [cam@cam.etat.lu](mailto:cam@cam.etat.lu)

Web page: <http://www.etat.lu/CAM>

Note that a list of all national focal points will be made available by the IMO on its public website ([www.imo.org](http://www.imo.org)).

## **4.4 Ships security alert system**

### ***4.4.1 National competent authority for receiving the SSAS alert***

The requirements of the ship security alert system specified in SOLAS chapter XI-2 Regulation 6 requires a national competent authority responsible for receiving ships security alert messages to be designated. In regard to Regulation 6.2.1., the ships security alert system when activated by a Luxembourg registered ship, shall initiate and transmit the ship-to-shore security alert to the POLICE GRAND DUCALE, identifying the ship, its location and indicating the security of the ship is under threat or it has been compromised. The contact mode is as follows:

### **POLICE GRAND DUCALE, Centre d'intervention national**

Email: [CIN@police.etat.lu](mailto:CIN@police.etat.lu)

### ***4.4.2 Confirmation of an alert***

The ship-to-shore security alert shall be addressed to the company. It is the duty of the company to confirm to the Commission for Maritime Affairs that an alert signal has been sent by one of their ship.

### ***4.4.3 False alert***

Companies shall provide their ship with a mean of detecting and cancelling false security alert system activations. If a false alert occurs, it will have to be lifted by the Company by

contacting without delay the Commission for Maritime Affairs by phone. This cancellation shall later be confirmed by fax or Email.

#### **4.5 Security level**

Until further notice, security level to be maintained on all ships flying the flag of the Grand-Duchy of Luxembourg is: SECURITY LEVEL 1

Based on threat information, competent Luxembourg governmental authorities will undertake changes of security levels for Luxembourg ships. The Commissioner for Maritime Affairs is responsible for communicating those changes to the companies, which will then have to forward the information to their respective ships.

The competent Coastal State Authorities or the Port Security Officers of the ports that the ship is visiting may upgrade the security level to a higher state for Luxembourg ships. The company shall immediately forward such changes to the Commission for Maritime Affairs by fax or Email.

Whenever an authority requests from a Luxembourg ship to adopt security level 3, the company shall immediately inform the Commission for Maritime Affairs.

#### **5. SOLAS Amendments**

As declared in circular n° 02/2003, all requirements related to SOLAS Chapter V and to SOLAS Chapter XI-1, shall directly be dealt with by the **classification societies** except for the implementation of Regulation 5 of SOLAS Chapter XI-1 (Continuous Synopsis Record).

##### **5.1 Chapter V : Safety of Navigation**

###### ***5.1.1 Regulation 19 : Carriage Requirements for Shipborne Navigational Systems and Equipment***

The AIS shall be maintained in operation at all times. Masters should be aware of Regulation 8 of Chapter XI-2 titled, “Master’s discretion for ship safety and security”. This regulation reinforces and provides the Master with significant discretion concerning the safety and security of his or her ship.

##### **5.2 Chapter XI-1 : Special Measures to Enhance Maritime Safety**

###### ***5.2.1 Regulation 3 : Ships Identification Number***

All passenger ships above 100 GT and all cargo ships above 300 GT must place the IMO number in a visible location on the ship. Specific details concerning character size are contained in the regulation. It is important to note that the IMO number must include the prefix letters, “IMO”.

Companies operating commercial yachts above 300 GT are reminded that an IMO number request must be applied through Lloyd’s Register so that it may be programmed into the AIS, as required.

Due to the limited size and to the exclusive purpose of a yacht commercially operated carrying a maximum of 12 passengers, it may be allowed that the identification number of this type of ship will be similar as for a passenger ship. Notification of this marking arrangement shall be communicated to the Commission for Maritime Affairs.

### ***5.2.2 Regulation 5 : Continuous Synopsis Record***

All the below-mentioned "constructions" are required to maintain a Continuous Synopsis Record on board, which also includes a history of ownership and management of the ship. The company is responsible for keeping the Commission for Maritime Affairs informed of any changes regarding this record.

The CSR requirements apply to:

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft, of 500 GT and upwards;
- Yachts commercially operated of 500 GT and upwards;
- Mobile offshore drilling units (MODU).

It does not apply to:

- Cargo ships of less than 500 GT;
- Ships not propelled by mechanical means;
- Wooden craft of primitive origins;
- Yachts commercially operated of less than 500 GT;
- Private pleasure yachts not engaged in trade.

The specific details and processes required to implement this requirement have been deliberated at the IMO. The outcome can be found in Assembly Resolution A.959(23) on Format and Guidelines for the Maintenance of the Continuous Synopsis Record as amended by Resolution MSC. 198(80), adopted on may 20<sup>th</sup> 2005.

## **5.3 Chapter XI-2 : Special Measures to Enhance Maritime Security**

### ***5.3.1 Regulation 4 : Requirements for Companies and Ships***

Ships not in compliance with SOLAS or the ISPS Code or unable to comply with established security levels must notify the Commission for Maritime Affairs prior to conducting any ship/port interface or port entry. From the moment that a ship's Master or a CSO becomes aware that a ship is not compliant or cannot maintain compliance, the Commission for Maritime Affairs is to be immediately advised, with details including corrective action, temporary alternative arrangements and current status.

Companies should note that Section 9.4 of Part A of the ISPS Code, 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.

### **5.3.2 Regulation 6 : Ship Security Alert System (SSAS)**

The Ship Security Alert System is a new hardware requirement designed to provide a covert means of alerting authorities that the ship's security has been compromised or is under attack. Companies are reminded to pay particular attention to the scheduling of the annual radio survey because for certain types of ships the required installation date could be as soon early as 2<sup>nd</sup> July 2004.

Necessarily, the continued validity of a ship's initial ISSC will rely upon, among other things, compliance with the installation of an effective Ship Security Alert System by the applicable safety radio survey implementation date irrespective of when the ship security system may be due for intermediate or renewal audit.

Performance standards for ship security alert systems are given in IMO resolution MSC.136(76) as amended by MSC.147(77). MSC/Circ.1072 gives further guidance on the design of ship security alert systems provided to comply with the SOLAS regulation. Those documents may be found in annex.

A minimum of two activation points initiating the transmission of the security alert is to be provided on board, one of which is to be on the navigation bridge, the other to be located elsewhere and its location protected from disclosure. The location of the second activation point is to be specified in the Ship Security Plan and remains confidential. However, in order to avoid the possibility of compromising the objective of the Ship Security Alert System, the Commission for Maritime Affairs is recommending that this information be kept elsewhere on board in a document known only to the Master, SSO and other senior ship's personnel as may be decided by the CSO.

The Ship Security Alert System may utilise the GMDSS radio installation, or another radio system provided for general communications, or a dedicated radio system. Ship security alert messages are to be addressed to the CSO and the Luxembourg competent authority as mentioned in 4.5. The Luxembourg authorities will inform the Coastal States in the vicinity of the ship.

### **5.3.3 Regulation 8 : Master's discretion for ship safety and security**

This regulation is a carefully crafted provision that reinforces and strengthens the Master's authority and independence concerning actions taken to ensure the safety and security of the ship. It addresses potential conflict between security and safety measures and states that if conflicts arise between safety and security measures and requirements, the Master shall give effect to those requirements necessary to maintain the safety of the ship. It also provides authority to the Master to implement temporary security measures to address the problems with the attendant obligation to notify the Commission for Maritime Affairs

Companies shall ensure that the Master has overriding authority and responsibility to make decisions with respect to the security of the ship, and the company shall ensure that the CSO, Master and SSO are given necessary support.

### **5.3.4 Regulation 9 : Control and compliance measures**

This regulation addresses in a comprehensive manner Port State actions that may be taken concerning a ship either in port or intending to enter the port of a Contracting Government. Port State control of ships is intended to be limited to verifying that there is a valid International Ship Security Certificate (ISSC) on board unless there are “clear grounds” for believing the ship is not in compliance with SOLAS XI-2 or the ISPS Code.

Any Port State action taken against a Luxembourg flagged ship by a Contracting Government or its Designated Authority is to be immediately reported to the Commission for Maritime Affairs.

### **5.3.5 Regulation 12 : Equivalent security arrangements**

This regulation provides the mechanism for the consideration of arrangements and systems in lieu of those specifically prescribed by the regulation or the Code.

As a matter of principle it is believed that this should only be undertaken in exceptional and unique circumstances. Close coordination with the Commission for Maritime Affairs is necessary for the evaluation and approval of any such equivalencies. Companies are cautioned that specific approval must be obtained from the Commission for Maritime Affairs prior to the installation or activation of any systems intended to serve as an equivalent to those prescribed by SOLAS XI-2.

## **6. ISPS Code**

The ISPS Code applies to:

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft, of 500 GT and upwards;
- Yachts commercially operated of 500 GT and upwards;
- Mobile offshore drilling units (MODU).

It does not apply to:

- Cargo ships of less than 500 GT;
- Ships not propelled by mechanical means;
- Wooden craft of primitive origins;
- Yachts commercially operated of less than 500 GT;
- Private pleasure yachts not engaged in trade.

### **6.1 Recognized Security Organizations (RSO)**

Companies may choose from any of the RSOs listed in point 4.1 of the present document to conduct SSP review and approval, verification audit, issuance of the ISSC and SSP amendment approval, provided that the selected RSO has not provided consultative services with regard to preparation of the SSA. It is preferable to keep the same RSO performing the entire certification process.

## **6.2 Declaration of Security (DoS)**

The Ship Security Plan shall clearly state that the SSO must complete a DoS as described in the ISPS Code, Part A, paragraph 5.

## **6.3 Obligations of the Company**

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.

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 and to request assistance of the company or of any Contracting Government as may be necessary. The Master of the ship has the ultimate responsibility for both safety and security aboard the ship. This has been made very clear in the Code in both Parts A and B.

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:

- 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;
- the person or entity responsible for deciding the employment of that ship;
- in cases where the ship is employed under the terms of charter party(ies), who the parties to such charter party(ies) are.

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

## **6.4 Ship Security Assessment (SSA)**

The purpose of a SSA is to identify and analyse the security risks for a given type of ship in a trading area. The results of the security assessment provide the basis for measures which are essential to develop, implement, maintain and update the ship security plan. This assessment shall take into account the additional workload such measures will rise up.

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 complement and duties, structural configuration and security enhancements.

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.

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. Due to the potentially sensitive operational and security information contained therein, the SSA shall be protected from unauthorized disclosure.

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 that address vulnerabilities.

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.

### **6.5 Ship Security Plan (SSP)**

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 the risks of a security violation. Because of the potentially sensitive operational information contained therein, the SSP shall be protected from unauthorized disclosure.

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 that address those vulnerabilities. At completion of the 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.

The RSO shall review the SSP to ensure that each element required by Part A and the relevant provisions of Part B of the Code are satisfactorily addressed as well as all the vulnerabilities referenced in the SSA. The Commission for Maritime Affairs recommends that the plan review process has to take place in the company, if possible, with the direct interaction of the CSO and the RSO to preclude the need to transport this sensitive material by means out of their control.

Identification of the locations where the ship security alert system activation points are provided, and the 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, 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 management level officers on board.

After certification under Part A, Section 19.1.1 has been completed, no changes, except as provided below, shall be made in the security system and in any associated security equipment or approved security plan without the sanction of the acting RSO. Changes to the contact data, or changes of personal on board, where these have no impact on the security plan, will not be required to be approved by the Commission for Maritime Affairs or by the acting RSO. These data shall be maintained up to date by the CSO and by the SSO.

## **6.6 Records**

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

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

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.

Records required to be kept by SOLAS Chapter XI-2, Regulation 9.2.1, including DoS, for a period covering at least the last 10 calls at port facilities shall be maintained on board. The said period shall not be less than one month.

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.

## **6.7 Company Security Officer (CSO)**

The CSO is the person designated by the company 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.

## **6.8 Ship Security Officer (SSO)**

The SSO is the person designated by the company to perform the duties and responsibilities detailed in Part A, Section 12 and Part B, Sections 8, 9 and 13. The SSO shall have completed a training course regarding the requirements and recommendations of the ISPS Code.

The SSO shall be a management level officer. It is recommended that this be the Master, holding a valid Luxembourg endorsement of his Certificate of Competency.

## **6.9 Training and certification**

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.

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.

At this stage, as decided at MSC 77, any form of evidence witnessing the above required training will be accepted until stricter requirements are enforced.

## **6.10 Use of weapons**

Carriage and use of weapons on board by seafarers are not recommended. However, if the company decides to have weapons on board it should contact the Luxembourg Ministry of Justice for the purpose of necessary authorisations.

## **6.11 Drills and Exercises**

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.

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.

## **6.12 Frequency of searches**

Part B, Regulation 9.15 of the ISPS Code refers to the frequency of searches at security level 1. It has been decided that as Part B of the Code is not made mandatory, the intervals for search of boarding persons will be left at the discretion of the company until stricter requirements are enforced.

## **6.13 Possible non-compliance and suggested temporary measures**

With reference to MSC/Circular 1097, Annex, Paragraph 12 – 16 when a subsequent failure of security equipments or systems is discovered, a temporary measure may be accepted as an alternative measure. However, such alternative measures should be reasonable and be designed to meet the objectives of the ISPS Code to a degree found acceptable by the auditor. Auditors should be reminded of the reporting obligation found in article 4 of our agreement with classification societies concerning surveys and certification of seagoing ships.

This circular should be of interest to shipowners, managers, masters and officers. Accredited shipping managers are kindly requested to make sure that this circular is properly distributed to the respective staffs or companies intervening in the management of the ships.



(s) Marc GLODT  
Commissaire du Gouvernement  
aux affaires maritimes