LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur

Commissariat aux Affaires Maritimes

Luxembourg, 15th January 2013

CIRCULAR CAM 01/2013.

The present circular replaces and withdraws circular CAM 05/2006 dated 12th September 2006.

To : ALL ACCREDITED SHIPPING MANAGERS

O/Ref : AH/101648

International Ship and Port Facility Security (ISPS) Code

1. Introduction

The ISPS Code entered into effect internationally on the 1 of July 2004 and consists of Part A (mandatory provisions) and Part B (recommended provisions).

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. Additional European Requirements

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 also applicable to all vessels flying the Luxembourg flag. This regulation harmonizes the implementation of the ISPS Code within Member States and renders some elements of Part B of the Code mandatory.

It is therefore reminded that the following paragraphs of Part B of the ISPS Code are 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).

Regulation (EC) N° 725/2004, previously mentioned, has been completed by Commission Regulation (EC) N° 324/2008 of 9 April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security.

3. Generalities

3.1 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, GL-DNV, 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.

3.2 The National Focal Point for security matters

The National Focal Point for security matters is the Luxembourg Maritime Administration:

Commissariat aux affaires maritimes (CAM)
19-21, Boulevard Royal
L-2449 Luxembourg

Tel. :	+ 352 2478 44 53 (during office hours: 09h00 – 12h00 and 14h00 – 17h00)
Fax :	+ 352 29 91 40
Tel. 24/7 :	+ 352 621 350 490 or +352 621 501 550 (after office hours and only in case of emergency)
Email :	cam@cam.etat.lu
Web page:	http://www.maritime.lu

Note that a list of all national focal points is available on the GISIS section of the IMO's public website (http://gisis.imo.org/Public/Default.aspx).

3.3 Ships security alert system

3.3.1 SSAS alerts

In regard to Regulation 6.2.1. of SOLAS, Chapter XI-2, **the ships security alert system, when activated by a Luxembourg registered vessel, shall initiate and transmit the ship-to-shore security alert to the Company Security Officer (CSO)**.

After having verified that the security alert is related to a real threat, the CSO must immediately forward the SSAS alert to:

POLICE GRAND DUCALE, Centre d'intervention national (CIN)

Email: CIN@police.etat.lu

This message must contain the following information:

- name and IMO number of the ship concerned
- latest ship's position
- type of threat sustained by the ship
- contact details of the CSO (in order to initiate immediate contact)

However, if at the time of the alert, the CSO does not have Internet access, the above mentioned information can be transmitted by phone to the CIN: **+352 4997 2346**.

As this procedure differs from the procedure detailed in the hereby cancelled Circular CAM 05/2006, Companies should make sure that the SSAS is properly and accordingly reprogrammed as soon as possible, **but not later than 1 March 2014**. After 1 March 2014, messages sent by vessels directly to CIN will be ignored.

3.3.2 Reporting of regular tests

Additionally, CSOs are requested to transmit to CAM, at least once a year, a report on the results of all SSAS tests messages sent by the Luxembourg flagged ships in their fleet.

3.3.3 False alert

Companies shall provide their ships with a mean of detecting and cancelling false security alert system activations. If nevertheless a false alert is transmitted to the Luxembourg authorities, it will have to be lifted by the Company by contacting without delay the CAM (by phone) and the CIN (by email).

4. 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. CAM 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 CAM by fax or Email.

Whenever an authority requests from a Luxembourg ship to adopt **SECURITY LEVEL 3**, the company shall immediately inform CAM.

5. ISPS Code

The following section serves as a general reminder as well as providing additional information related to the ISPS Code as it is applicable for Luxembourg flagged vessels.

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.

5.1 Recognized Security Organizations (RSO)

Companies may choose from any of the RSOs listed in point 3.1 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.

5.2 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.

5.3 Obligations of the Company

For all its ships, every company shall develop, implement, and maintain a functional SSP 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.

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:

- contact details for 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;

- contact details for 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), contact details of such charter party(ies).

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.

5.4 Ship Security Assessment (SSA)

The purpose of a SSA is to identify and analyze 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 compliment 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.

5.5 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 onboard the ship of measures 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, as well as all the vulnerabilities referenced in the SSA, are satisfactorily addressed. CAM 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 shall be made to the security system and any associated security equipment or approved security plan without the sanction of the acting RSO. However, in accordance with the ISPS Code, part A, section 9.5, minor changes to the contact data or to the onboard personal will not be required to be approved beforehand by CAM or by the acting RSO. These minor changes will however, in every case, have to be notified to CAM and to the acting RSO.

5.6 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 then 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.

5.7 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.

5.8 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 (preferably the Master).

5.9 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 of the ISPS Code.

All other shipboard personnel must have sufficient knowledge of and be familiar with relevant provisions of the SSP including the elements described in Part B, Section 13.4 of the ISPS Code. Regulation VI/6 of the STCW Convention, as amended, as well as Paragraphs 1-4 of Section A-VI/6 of the STCW Code, as amended, are also applicable.

5.10 Use of weapons

Carriage and use of weapons by seafarers on board 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.

5.11 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.

Various types of exercises, which may include participation of the CSO, PSO, relevant authorities of contracting governments as well as SSO, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resources availability and response. These exercises may be:

- full scale or live;
- table top simulations or seminars;
- combined with other exercises such as search and rescue or emergency response exercises

The participation of a company in an exercise with another contracting government is recognised by CAM.

5.12 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.

5.13 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) Robert BIWER
Commissaire du Gouvernement
aux affaires maritimes