C C S 通 函

Circular

China Classification Society
（2010）Circ.No.5 Tot. No.5
Jan.. 27, 2010 （total 2 Pages ）

TO: Related departments of Headquarter; Branches and Offices; ship owners&operators

Notice of implementation of

Administration requirement AR1.21.2 of

Malta Maritime Authority

Merchant Shipping Directorate

The Malta Maritime Authority Merchant Shipping Directorate issued the Administration requirement AR1.21.2l on Dec.21, 2009 which mentioned the EU Regulations on enhancing ship and port facility security include sections of part B of the ISPS Code as mandatory. The sections related to ship security are to be considered as mandatory for Maltese ships. Companies are also reminded that a number of contracting governments will be enforcing certain paragraphs of part B of the ISPS Code thus making the vessel (entering into their ports facilities) subject to port State control inspection vis-à-vis part A and certain paragraphs of part B of the ISPS code. The Administration requires that particular consideration be taken for, paragraphs 8.1 to 13.8 of part B of the ISPS Code in order for an ISSC to be issued. Please refer to the attachment.

SUMMARY

Malta Maritime Authority Merchant Shipping Directorate issued the special requirement of ISPS code.

ACTION REQUESTED

All the CCS Branches and Offices are required to organize the study and training of this circular to the auditors, and forward this circular to relevant companies. The company should

be reminded to comply with the requirements accordingly. And the auditors should pay more attention about these special requirements while carrying out on site verification.

Attachment：1. Administration requirement AR1.21.2，16 pages.

For any problem please contact the **Certification Management Dept.** without hesitation

The Administration takes into consideration that although part B of the ISPS Code is recommendatory all Companies are still required to consider the guidance in part B in order to comply with the requirements of SOLAS Chapter XI-2 and the ISPS Code. The EU Regulations[1] on enhancing ship and port facility security include sections of part B[2] of the ISPS Code as mandatory. The sections related to ship security are to be considered as mandatory for Maltese ships. Companies are also reminded that a number of contracting governments will be enforcing certain paragraphs of part B of the ISPS Code thus making the vessel (entering into their ports facilities) subject to port State control inspection vis-à-vis part A and certain paragraphs of part B of the ISPS code. The Administration requires that particular consideration be taken for paragraphs 8.1 to 13.8[3] of part B of the ISPS Code in order for an ISSC to be issued.

APPLICABLE SHIP TYPE

The Administration requirements and guidelines in this notice are applicable to the following Maltese ships engaged in international voyages;

- Passenger ships, including high-speed craft
- Cargo Ships, including high speed craft, of 500 gross tonnage and upwards
- Mobile Offshore Drilling Units

ENTRY INTO FORCE

The Administration requirements including guidelines are to be implemented by the first intermediate or renewal verification on or after 2nd June 2006. Cargo ships of 500 gross tonnage and upwards[4] engaged on international voyages which on the grounds of national tonnage rules have not been required by this Administration to comply with the provisions of SOLAS chapter XI-2, the ISPS Code and this Administration requirements including guidelines, shall now comply by not later than 1st July 2008 unless such cargo ships are already compliant.

[1] Regulation (EC) N6 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (entry into force 1st July 2004).
[2] Part B Paragraph 1.12, 4.1, 4.4, 4.5, 4.8, 4.14-4.16, 4.18, 4.24, 4.28, 4.41, 4.45, 6.1, 8.3-8.10, 9.2, 9.4, 13.6, 13.7
[3] Ref to MSC/Circ. 1097 paragraph 8 – 9 and IACS procedural requirements No. 24
[4] As determined under the provisions of the International Convention on the Tonnage Measurement of Ships 1969.

DEFINITIONS

Administration for the purposes of this notice the term Administration shall mean the Merchant Shipping Directorate of the Malta Maritime Authority.

Drill means a training event that tests at least one component of the ship security plan and is used to maintain a high level of security readiness.

Emergency response services means the medical, paramedical and ambulance personnel, fire and rescue personnel, and at sea search and rescue (SAR) units responding to or participating in SAR operations.

Exercise means a comprehensive training event that involves several of the functional elements of the ship security plan and tests communications, coordination, resource availability, and response.

Failure means an observed situation where objective evidence indicates the non-fulfilment of a specified requirement of the ISPS Code and Administration requirements.

Public authorities[5] means the agencies or officials in a State responsible for the application and enforcement of the laws, regulations, orders and decrees of that State.

LIST OF ABBREVIATIONS

CSO	Company Security Officer
CSR	Continuous Synopsis Record
DOS	Declaration of Security
IMO	International Maritime Organization
ISM	International Safety Management
ISSC	International Ship Security Certificate
PFSO	Port Facility Security Officer
RSO	Recognized Security Organization
SMS	Safety Management System
SSA	Ship Security Assessment
SSO	Ship Security Officer
SSP	Ship Security Plan

[5] IMO MSC/Circ. 1156

1) SETTING OF SECURITY LEVEL

The setting of security level for Maltese ships is the responsibility of this Administration. The Administration will communicate the security level information as and when deemed necessary to the Company by MSD Notices. Whenever a higher security is set by this Administration, the CSO shall confirm the change in the security level onboard ships falling under his/her responsibility furthermore the CSO shall notify the Administration of security related matters that may effect the security level onboard.

2) RECOGNIZED SECURITY ORGANIZATION

The following RSOs have been authorized to act on, for and behalf of the Administration, to approve SSPs and carry out verification and certification on Maltese ships in accordance with section 19.1 of part A of the ISPS Code and the applicable requirements of SOLAS Chapter XI-2;

- American Bureau of Shipping,
- Bureau Veritas,
- China Classification Society,
- Class NK,
- Det Norske Veritas,
- Germanischer Lloyd,
- Polish Register of Shipping
- Korean Register of Shipping,
- Lloyd's Register of Shipping,
- Registro Italiano Navale,
- Russian Maritime Registry of Shipping,

RSO shall require specific authorization prior to the ISPS verification and certification. A letter of authorization will be issued by this Administration on a ship-by-ship basis. The authorisation letter will be issued once and will be applicable for the initial audit and subsequent periodical/renewal audits including approval of the SSP.

All RSOs must ensure that training of all their ISPS auditors conforms to the requirements of IACS procedural requirement 25.

3) DURATION OF CERTIFICATE

The validity of ISSC issued after the initial verification shall be for a period of not more than five years and subject to one intermediate verification and renewal verification by the end of the five-year period. If the Company wishes to harmonize the ISSC with the expiry date of the SMC issued in accordance with the ISM Code, the ISSC may be issued for a shorter period. Any additional verification shall be carried out as deemed necessary by the Administration or RSO.

4) INTERIM ISSC

An Interim ISSC valid for six months shall be issued following;

- SSA has been completed,
- The ship has been provided with the SSP,
- The SSP has been reviewed by the CSO and submission for approval by RSO,
- The company and the ship are operating in accordance with the provisions of the plan. Necessary arrangements have been carried out for the maintenance of records, drills, crew familiarization, crew security training, internal audits, maintenance, calibration and testing of security equipment, including the ship security alert system'
- At least one drill specified in the SSP has been either carried out or planned by the SSO/CSO before the ship's departure.

An interim ISSC may not be extended beyond the six months stipulated in ISPS A/19.4.4. The issuance of subsequent consecutive interim ISSC shall only be considered by the Administration on a case-by-case basis following specific requests by RSO.

5) REVISING ENTRIES ON THE ISSC

In instances of change of particulars, additional verification will be carried out to confirm necessary amendments to security documentation.

6) INVALIDATION OF THE ISSC

In addition to ISPS Code Section A 19.3.8, the Administration may cancel or suspend an ISSC when;

- Remedial actions for failures set out at the intermediate or additional verification have not been completed within the agreed time period,
- The ship security plan has been amended without approval,

The ISSC is to be reinstated upon satisfactory completion of verification in the scope of initial verification.

7) FAILURES

The ISSC will not be issued in cases where the initial or renewal security verification has identified, by objective evidence, failures from the approved plan or requirements of SOLAS Chapter XI-2, ISPS Code and Administration requirements. The RSO carrying out the verification is to inform the Administration and a copy of the Statement of Failure is to be forwarded to the Administration, to the company and to the ship. Even if these failures do not compromise the ship's ability to operate at security levels 1 to 3, the ISSC will not be issued until all failures have been rectified.

In the case of failures that have been identified objectively during an intermediate or additional verification and which compromise the ship's ability to operate at security levels 1 to 3, these shall be reported immediately to the Administration by the RSO concerned. Unless identified failures can be immediately rectified the company is to implement alternative security measures and develop an action plan including time scale to address identified failure/s. The auditor shall verify the implementation of alternative measures before the ship sails. A copy of the statement of failure together with a full report including company's action plan is to be forwarded to the Administration. The Administration may request an additional verification to verify that the action plan has been completed. If the approved action plan is not followed or alternative arrangements not implemented, the Administration may withdraw the ISSC.

In the case of failures that have been identified objectively during an intermediate or additional verification and which do not compromise the ship's ability to operate at security levels 1 to 3, these shall be reported immediately to the Administration by the RSO concerned. The company is to forward an action plan, detailing corrective measures including time scale for correction and any alternative security measures that will put in place to address the failure identified. The completion of the action plan shall be verified no later than the next scheduled verification.

8) CERTIFICATION AND VERIFICATION PROCESS

Based on the initial authorization an ISSC may be issued subject to the following;

- The ship has an approved SSP,
- Satisfactory onboard initial verification by a RSO,
- The Company and the ship are operating in accordance with the provisions of the approved plan and that the ship security management system has been operating for at least two months from the date the SSP is logged as received onboard from the CSO. Operation in accordance with the provisions of the approved plan prior to certification should be verified on activity basis i.e. the RSO auditor should verify security related activities such as maintenance of records, drills, crew familiarization, crew security training and internal audits have been carried out. In addition maintenance, calibration and testing of security equipment, including the ship security alert system to be verified,
- All the technical equipment referenced in SSP has been verified,
- Satisfactorily operational security measures verified by sample audit of sufficient level necessary to asses the operating system in its entirety.
- Notification to the Administration of the designated CSO including contact details.

The RSOs are to adopt IACS Procedural Requirements for ISPS Code Certification (IACS PR no. 24 including no. 27 in case of transfer of certification).

9) SHIP SECURITY ASSESSMENT

The SSA is an integral part of the process of developing the SSP. Although provisions are made within the ISPS Code to develop a fleet security plan, the Administration requires that the plan for each ship reflects ship-specific information accurately. The only way to ensure that the information gathered during the SSA is accurate; the SSA is to be carried out by appropriately skilled personnel. Furthermore technical ship security information shall only be achieved by carrying out the on-scene security survey onboard each and every ship of the fleet, including sister ships. A copy of the current SSA is to be retained onboard at all times. The Master and/or SSO shall ensure the protection of the SSA from unauthorized access.

10) DEVELOPMENT OF SHIP SECURITY PLAN

The Company may choose to develop the SSP (including the SSA) using adequately trained SSO and/or a Security Consultant and/or RSO.

Within the ISPS code no provisions are set for any RSO to assist in the development of the SSP (including the SSA). If a Company chooses to use a RSO to assist in the development of the plan, then that RSO shall not be authorized to approve the SSP or conduct the verification.

In cases where the company has already adopted security procedures[6] within the safety management system of the ship, such established procedures are to be reviewed and if need be amended to reflect the requirements of Chapter XI-2 and part A of the ISPS Code.

It is recommended that such established procedures be incorporated within the SSP and not cross-referred within the SMS. This would provide smoother verification process of the SSP and such procedures would be protected from unauthorized access or disclosure.

It is recommended by the Administration that procedures are to be included within the SSP to address circumstances when the vessel is put out of service and/or ships are under conversion but still manned. Such procedures would also focus on the revitalizing the ship security prior entry into service. Particular care shall be taken with regards the availability of sufficient personnel remaining onboard thereby ensuring that security duties outlined in the approved SSP are not compromised. Furthermore in the case when the ship is located in the shipyard the sharing of security responsibilities between the ship and the shipyard will have to be agreed and this involves the conclusion of a DOS.

If the statutory certificates of the ship, including the ISSC, are suspended or revoked, responsibility for the security of the ship would, in practice, rest with the shipyard.

The SSP shall establish, as applicable, details of the procedures and security measures the ship should apply when:

1. it is at a port of a State which is not a Contracting Government;
2. it is interfacing with a ship to which the ISPS Code does not apply;

[6] Example security procedures to address security related incidents such as stowaways, piracy and armed robbery and access of visitors.

3. it is interfacing with a fixed or floating platform or a mobile drilling unit on location;
4. it is interfacing with a port or port facility which is not required to comply or which is not complying with chapter XI-2 and part A of the ISPS Code;

If the ship's approved SSP does not already include provisions as listed in 1 to 4 above, the ship should attempt to conclude a Declaration of Security or to take the following action:

- record the actions taken by the CSO and/or SSO to establish contact with the PFSO, and/or any other persons responsible for the security of the port and/or port facility, ship or platform being interfaced;
- record the security measures and procedures put in place by the ship, bearing in mind the security level set by the Administration and any other available security related information; and complete and sign, on behalf of the ship alone, a DOS (particularly in circumstances that the ship is unable to identify the security person responsible for a particular port facility);
- implement and maintain the security measures and procedures set out in the DOS throughout the duration of the interface;
- report the actions taken to the CSO and through the CSO to the Administration; and
- request the CSO to inform the authorities responsible for the exercise of control and compliance measures (regulation XI-2/9) and the PFSO(s) at the next port(s) of call of the difficulties the ship experienced and of the actions the ship itself took.
- additional to the above it is recommended that prior to departure from port facilities which do not comply with the requirements of the ISPS Code searches are carried out in accordance with the approved SSP. Such additional security measures are to be documented.

Companies are reminded that during routine and normal ship/port interface and ship-to-ship activities it is usual for a variety of commercial, private and Governmental personnel to require access to a ship. Ship security contained in SOLAS chapter XI-2 and in the ISPS Code has been developed for the purpose of enhancing the security in the international maritime transport sector and should not be used to delay or inhibit unnecessary or unjustifiably the access on board of public authorities and emergency response services. The approved SSP does not create the right for either the ship or for those on board to invoke it's provisions, and to claim, in any circumstance and regardless of what is required by the applicable security level, that they have authority to prevent any public authority from boarding the ship when that ship is within the territory of another SOLAS Contracting Government or of another State.

11) COPIES OF THE APPROVED SHIP SECURITY PLAN

It is required by the Administration that a copy of the endorsed SSP (including any amendments) be retained in the office/s of the Company. The Company shall ensure the protection of the SSP from unauthorized access.

12) AMENDMENTS TO THE SHIP SECURITY PLAN

The following list identifies which changes to the SSP are to be forwarded to the RSO for approval.

- Procedures 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.
- 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 auditing 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;
- Procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board.
- 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.
- Procedures relating to security record keeping;
- Procedures aimed at preventing unauthorized access/disclosure, deletion, destruction or amendment.
- Procedures relating to the delivery of the ship's stores.

Those amendments, which significantly alter or change the security management system on board, shall be subject to an additional verification audit by the RSO.

13) INTERNAL AUDITS

Internal audits of security activities are to be carried out at least annually. Internal audits are not to be carried out by the personnel responsible of the activities being audited.

14) TRAINING OF COMPANY SECURITY OFFICER AND SHIP SECURITY OFFICER

ISPS B/13.1 to 13.8 provides guidance on the security training required for the CSO, SSO and shore bases Company personnel.

It is the responsibility of the company to ensure that Company Security Officers, other appropriate shore based personnel and Ship Security Officers are to receive the appropriate training.

The Guidelines on Training and Certification for Company Security Officers (IMO MSC/CIRC. 1154) are to be considered as the minimum requirements[7] in relation to the level of knowledge sufficient to enable a person to act as the designated CSO.

Ship Security Officers serving on board ship are required to be in possession of a certificate of proficiency issued in accordance with Regulation VI/5 of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978 and Section A-VI/5 of the STCW Code which sets out the specifications of minimum standards of proficiency for SSOs.
It is the Company who decides training method provided to the personnel involved in security matters but if determined by the company that in house training will be conducted by the CSO, it is recommended that CSO attend a "train the trainer" course.

Documentary evidence of any training attended or any training carried out is to be issued attesting the training received, particularly the training provided to the Ship Security Officer.

Companies are reminded that paragraph B/4.33 indicates that lack of training could give rise to clear grounds under regulations XI-2/9.1 and XI-2/9.2. Although the ISSC will be considered as prima facie evidence that the required training has been provided to the crew, as identified in MSC/Circ. 1097, if a port State control inspector detects a lack of training further action could be taken, resulting in the detainment of the vessel.

[7] By not later than 1st July 2009

Training of shore based and shipboard personnel is crucial.

The Administration requirements vis-à-vis the required security knowledge of the shipboard personnel at the stage of the initial verification, the Company must ensure those concerned, understand their role and responsibilities and have enough knowledge for performing ship security duties as outlined in chapter XI-2 and the ISPS Code and in the approved SSP.

Key members of the ship's personnel are able to communicate effectively with each other and that no communication barrier exists.

15) DESIGNATION OF THE COMPANY SECURITY OFFICER

In meeting its obligations in respect of the provisions contained in ISPS A/11 the Company shall not outsource responsibilities of CSO to third parties. It is reminded that the position of the CSO is a 24-hour responsibility. The Company must have the necessary arrangements to ensure that a line of communication (directly or indirectly) exists between the CSO and the ship on a 24-hour basis. The company must complete and submit the form outlined in Annex I of this notice, providing information with regards to the designated CSO.

16) SELECTING A SHIP SECURITY OFFICER

Any member of the ship's personnel, including the Master, may be designated as the SSO, provided that the SSO has the required training and understanding of his duties and responsibilities. Consideration needs to be given in relation to crew size. On ships with a small crew the Master may be the most appropriate choice to be the designated SSO.

Companies are reminded that it is a fundamental requirement that the SSO should be familiar with the security arrangements on the specific ship on which the SSO serves. In cases where the serving SSO is replaced it is the responsibility of the Company to ensure that the replacing SSO has the opportunity to become familiar with the particular ship and it's approved SSP.

It is prudent to point out that the workload presented to the ship personnel through the development and implementation of the SSP does not infringe hours of rest, which could promulgate fatigue. Notwithstanding the requirements of the minimum safe manning certificates the Company shall ensure that the sufficient number of

personnel is onboard to implement the security measures outlined in the SSP. Human resources availability shall be evaluated during the SSA.

In cases where the SSO is identified in the SSP specifically by name, Company procedures shall be in place to amend such details when change of SSO occurs.

17) DECLARATION OF SECURITY

Unless specifically instructed by the Administration, CSO or SSO the Master is not obliged to complete DOS when both the ship, port facility or other ship covered by the ISPS Code, are operating at security level 1. Section A/5.2 of the ISPS specifies when a ship can request completion of a DOS.

18) DRILLS AND EXERCISES

To ensure the effective implementation of the provisions of the SSP, the Administration requires that security drills should be conducted at least once every three months. In addition, in cases where more than 25% of the ship's personnel have been changed, at any one time, with personnel that have not previously participated in any drill on that ship within the last 3 months, a drill should be conducted within one week of the change. A tabletop security exercise, which would include the involvement of a port facility and/or the company, shall be carried out once a year. SSAS shall be tested at least twice a year. Security training and drills shall be reflected in the ship's training and drill programme. All drills carried out are to be recorded accordingly.

19) RECORD KEEPING

The documentary evidence and records, which need to be maintained, are specified in;

- Regulation XI-2/5;
- Regulation XI-2/9.2.1;
- Section A/10;
- Section A/5;

The Administration requires that all records identified above, including all verification records, shall be maintained by the Company and the ship for a period of three (3) years.

Bearing in mind the provisions of SOLAS regulation XI-2/9.2.3 DOS shall be kept onboard for a minimum period of three (3) years.

20) LAID UP SHIPS

In the case when a ship is laid up the validity of the ISSC depends on the ship's manning level but as a general rule Companies are to note the following;

- If the lay-up is for a period of 0 – 3 months, a security drill must be carried out within one week of re-entry into service. Additional requirements may be stipulated by the Administration as deemed necessary on a case-by-case basis.
- If lay-up period is for 3 – 12 months prior to re entry into service the RSO is required to carry out additional verification for the purpose of ensuring that the security system remains valid and in full compliance with the ISPS Code. The additional verification is to be reflected by endorsement of the ISSC.
- If lay-up period is for over 12 months interim certification is required and the SSP to be approved prior to re-entry into service.

21) SECURITY EQUIPMENT

The Administration does not require any specific security equipment to be provided on board Maltese ships, but the outcome of the SSA could result in the need of security equipment to be fitted or provided onboard. When fitting security equipment and related electrical installations, the Company shall give due considerations to the safety issues addressed by regulation 45 SOLAS chapter II-1. Security equipment provided is to be clearly identified in the SSP and procedures have to be included within the SSP for the operation, maintenance, calibration and testing of the security equipment.

22) POSSESSION OF FIREARMS ONBOARD MALTESE REGISTER SHIPS

The Administration has adopted a no firearm policy on board Maltese ships.

23) ISPS CODE PUBLICATION

It is a requirement of the Administration that a copy of the latest edition of ISPS Code, shall be retained onboard Maltese ships.

24) SHIP SECURITY ALERT SYSTEM

The SSAS, when activated, shall initiate and transmit a ship-to-shore security alert to, but not limited, the mailbox address of the Administration - alert.isps@mma.gov.mt and the Company, identifying the ship, its location and

indicating that the security of the ship is under threat or that it has been compromised.

The SSAS is to satisfy the functional requirements as outlined in IMO Resolution MSC. 136(76) as amended by MSC. 147(77). MSC/Circ 1072 provides further guidance in relation to the design of the SSASs.

Identification of the location of the activation points including operational instructions such as testing, deactivation and resetting are to be kept in a separate document known only to the Master, SSO and senior management level officers.

If the ship has already an approved SSP, the plan must be amended to address the SSAS and the amended parts must be present onboard for review and approval during the verification by the RSO after initial installation of the SSAS.

Once installed the SSAS would be subject to a dedicated verification by the RSO. This verification is not intended to replace a safety radio survey required by SOLAS Chapter I. The safety radio survey is carried out by the recognised organization issuing the safety radio certificate.

When the SSAS is activated, the security alert message should include the following information:

- Name of ship
- IMO Ship identification number
- Call Sign
- Maritime Mobile Service Identity
- GNSS position (latitude and longitude) of the ship
- Date and time of the GNSS position

Depending on the equipment, system and arrangements used, the name, the IMO Ship identification number, the Call Sign and the Maritime Mobile Service Identity of the ship may be added to the signal or message transmitted by the ship borne equipment. The SSAS is to be tested every time there is a change in the details or the programming of the unit.

25) REPORTING OF SECURITY INCIDENTS

Companies must immediately notify the Administration upon the activation of the SSAS and of any security incident. The following initial information is to be provided via fax and/or email;

- Ship's name
- IMO number
- Details of company security officer
- Details of ship security officer
- Type of security incident
- Ship's location
- Cargo on board
- Last port of call
- Next port of call
- Copy of crew list

26) POINT OF CONTACT

Malta Maritime Authority
Merchant Shipping Directorate
Maritime Trade Centre
Marsa MRS1917
Malta
Tel: +356 21 250360
Fax: +356 21 241460
E-mail: *comms.isps@mma.gov.mt*

Name	AOH Contact Numbers	Email
Capt. M. Chapelle	+356 99494318	mark.chapelle@mma.gov.mt
Mr. A. Gruppetta	+356 79434317	albert.gruppetta@mma.gov.mt
Mr. P. Zammit Endrich	+356 79434316	pierre.zendrich@mma.gov.mt
Mr. R Aquilina	+356 99434318	ray.aquilina@mma.gov.mt

Malta Maritime Authority
Merchant Shipping Directorate
Maritime Trade Centre
Marsa MRS 1917 MALTA

ANNEX I

NOTIFICATION OF COMPANY SECURITY OFFICER

DESIGNATION OF COMPANY SECURITY OFFICER (CSO)

Under Section 11.1 of the ISPS Code, the entity responsible for the management of the ship in accordance with the ISM Code shall designate a person, the Company Security Officer for the ship. In line with the above the undersigned hereby declares that:

Name .....
Address .....
.....
.....
.....
Telephone No. .....
Telephone No. (AOH) .....
Facsimile No. .....
E-mail .....

is the designated Company Security Officer, who has agreed to take over all duties and responsibility imposed by the ISPS Code, for the following named ship(s):

Ship	*IMO Number*

Name of Company Official *Date* *Signature of Company Official*