INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE

Technical Notice SLS.10 Rev.3

Notice to Shipowners, Ship Operators, Managers, Masters, Owners' Representatives and Recognised Organisations

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

This Technical Notice and guidelines 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

[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

DEFINITIONS

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

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 mean 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 this Technical Notice.

Public authorities[4] mean 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

[4] IMO MSC/Circ. 1156

1) SETTING OF SECURITY LEVEL

The setting of security level for Maltese ships is the responsibility of the Administration. The Administration will communicate the security level information as and when deemed necessary to the shipping community by MS Notices. Whenever a higher security level is set by the Administration, the CSO shall confirm the change in the security level onboard ships falling under his/her responsibility. Furthermore, the CSO shall, at all times notify the Administration of security related matters that may affect the security level onboard.

2) RECOGNIZED SECURITY ORGANIZATIONS

The following RSOs have been authorized to act for and on 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,
- Croatian Register of Shipping,
- DNV,
- Korean Register of Shipping,
- Lloyd's Register of Shipping,
- Polish Register of Shipping,
- Registro Italiano Navale,
- Indian Register of Shipping

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

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 submitted 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.
- Notification to the Administration of the designated CSO including contact details as provided in para.14 of this TN.

In accordance to ISPS A/19.4.4 an interim ISSC may not be extended beyond six months. 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 to 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, failure(s) from the approved plan or requirements of SOLAS Chapter XI-2, ISPS Code and this Technical Notice. 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. The ISSC will not be issued/endorsed before failure(s) that compromise the ship's ability to operate at security levels 1 to 3 are rectified.

In the case of a failure(s) 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, the failure(s) shall be reported immediately to the Administration by the RSO concerned. Unless identified failure(s) 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 failure(s) 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, the failure(s) 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(s) 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 assess the operating system in its entirety.

The RSOs are to adopt IACS Procedural Requirements for ISPS Code Certification (IACS PR no. 24 including no. 18 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. 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[5] 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 and Part B[2] of the ISPS Code.

In accordance to the scope and objective of the convention such established procedures are to be incorporated within the SSP and not cross-referred within the SMS with the exception of cyber security as provided in MSC 101/24 paragraph 4.10. 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 ship is put out of service and/or the ship is undergoing conversion but still manned. Such procedures would also focus on 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.

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

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;
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 person(s) 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 when the ship is unable to identify the security person(s) 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. Security requirements 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 the provisions therein, and to claim, in any circumstance and regardless of what is required by the applicable security level, the 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

The Administration requires 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 against 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 the carriage on board the ship of weapons, dangerous substances and devices intended for use against persons, ships or ports;
- Identification of the restricted areas and measures for the prevention of unauthorized access;
- 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 that Contracting Governments may issue whilst at security level 3;
- Procedures for auditing security activities;
- Procedures for associated training, drills and exercises;
- Procedures for interfacing with port facility security activities;
- Procedures for the periodic review and 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 and 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) 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 the CSO to third parties. It is to be borne in mind 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 appointment of a CSO / DCSO requires, the Company to complete and submit the form outlined in Annex I of this Technical Notice, providing information with regards to the designated CSO. Companies that appoint a Deputy / Alternate CSO to assist the CSO shall complete Annex 2 accordingly.

15) SELECTING A SHIP SECURITY OFFICER

Any member of the ship's personnel, including the Master, may be designated as the SSO, provided that the selected member of the ship's personnel is duly trained and has a sound understanding of his duties and responsibilities and in possession of a certificate of proficiency for Ship Security Officers issued under the provisions of the STCW convention. 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 designated as the SSO.

Companies are reminded that it is a fundamental requirement that the SSO should be familiar with the security arrangements of 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 familiarize himself with the particular ship and the approved SSP.

It is prudent to point out that the workload presented to the ship personnel through the development and implementation of the SSP should not infringe hours of rest, which could promulgate fatigue. Notwithstanding the requirements of the minimum safe manning certificate, the Company shall ensure that sufficient number of personnel is onboard to implement the security measures outlined in the SSP. Human resource availability shall be evaluated during the SSA.

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

16) DECLARATION OF SECURITY

Unless specifically instructed otherwise by the Administration, CSO or SSO, the Master is not obliged to complete the DOS when 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 Code specifies instances when a ship can request completion of a DOS.

17) 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. The 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.

18) 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 minimum period of three (3) years.

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

19) LAID UP SHIPS

In the case of a ship that 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 lay-up is for a period of not more than three (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 is for a period exceeding three (3) month but not more twelve (12) months, the RSO is required to carry out prior to re-entry into service an 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 is to be approved prior to re-entry into service.

20) 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. During the fitting of security equipment and related electrical installations, the Company shall give due consideration to the safety issues highlighted by SOLAS Regulation II-1/45. Security equipment provided is to be clearly identified in the SSP and procedures have to be included therein for the operation, maintenance, calibration and testing of the security equipment.

21) POSSESSION OF FIREARMS ONBOARD MALTESE REGISTER SHIPS

The Administration has adopted a no firearms policy on board Maltese ships. Considerations are given to applications as provided in MS Notice 106 - Placement of Privately Contracted Armed Security Personnel (PCASP) onboard Maltese ships, when ships are operating in high risk areas as defined.

22) ISPS CODE PUBLICATION

The Administration requires that a copy of the latest edition of ISPS Code shall be retained onboard Maltese ships.

23) SHIP SECURITY ALERT SYSTEM

The SSAS, when activated, shall initiate and transmit a ship-to-shore security alert to at least, the mailbox address of the Administration - alert.isps@transport.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 outlined in Resolution MSC.136(76), as amended by Resolution MSC.147(77). Further guidance in relation to the design of the SSASs is provided in MSC/Circ.1072.

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 accessible only to the Master, SSO and senior management 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 the radio survey required by SOLAS Chapter I. The radio survey is an integral part of the statutory survey and certification process undertaken by the recognized organization.

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 of Ship, the IMO Ship Identification Number, the Call Sign and the Maritime Mobile Service Identity may be added to the signal or message transmitted by the shipborne equipment. The SSAS is to be tested twice a year and whenever there is a change in the details or the programming of the unit.

24) 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;

- Name of ship
- IMO number
- Details of Company Security Officer
- Details of Ship Security Officer
- Type of security incident
- Location of ship
- Cargo on board
- Last port of call
- Next port of call
- Copy of crew list

25) POINT OF CONTACT

Transport Malta
Merchant Shipping Directorate
Malta Transport Centre
Ħal-Lija, LJA 2021
Malta

Tel: +356 21 250360

E-mail (General ISPS matters): comms.isps@transport.gov.mt
E-mail (Security Alerts): alert.isps@transport.gov.mt

Name	AOH	Email
Mr. R Aquilina	+356 99434318	ray.aquilina@transport.gov.mt
Alternate point of contact;		
	+356 79434317	
	+356 99494318	
	+356 79434316	

Merchant Shipping Directorate 17 April 2023

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 (CSO) for the ship/s. In line with the above the undersigned hereby declares that:

Name of CSO .....

Telephone No. (AOH) .....

ISM Company details:

Name of Company _____

Company Address _____

_____

_____

Telephone 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):

Name of Ship	IMO Number
_____	....
_____	....
_____	....
_____	....
_____	....
_____	....
.....	_____

_____ _____

(Signed) Company Security officer Date

_____ _____

Company Signatory Name and position of Company Signatory

Malta Transport Centre,
Ħal Lija LJA 2021

Tel: +356 2125 0360
Email: isps.comms@transport.gov.mt
www.transport.gov.mt/ship-registration

ANNEX 2

NOTIFICATION OF DEPUTY / ALTERNATE COMPANY SECURITY OFFICER

DEPUTY / ALTERNATE COMPANY SECURITY OFFICER (D/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 Deputy / Alternate Company Security Officer (D/CSO) for the ship/s. In line with the above the undersigned hereby declares that:

Name of D/CSO .....

Telephone No. (AOH) .....

ISM Company details:

Name of Company _____

Company Address _____

_____

_____

Telephone No. _____

E-mail ....

is the Deputy Company Security Officer, who shall deputies the Designated CSO over duties and responsibility imposed by the ISPS Code, for the following named ship(s):

Name of Ship	IMO Number
_____	....
_____	....
_____	....
_____	....
_____	....
_____	....
.....	_____

_____ _____

(Signed) Deputy Company Security officer Date

_____ _____

Company Signatory Name and position of Company Signatory

Malta Transport Centre,
Ħal Lija LJA 2021

Tel: +356 2125 0360
Email: isps.comms@transport.gov.mt
www.transport.gov.mt/ship-registration