GUIDELINES FOR SHIPPING COMPANIES

DEVELOPMENT AND IMPLEMENTATION OF A SHIP SECURITY PLAN

(in compliance with the International Ship and Port Facility Security (ISPS) Code)

Content:

A. General

1. Scope of application

These guidelines apply to the development and implementation of ship security plans (SSP) in accordance with the requirements of the International Ship and Port Facility Security (ISPS) Code.

Additional GL Guidance:

The ISPS Code specifies that the following types of ships engaged on international voyages have to implement and maintain an approved SSP:

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

Reference: ISPS Code A/3.1.1

2. Objective

The objective of these guidelines is to provide practical assistance to shipping companies for the development, implementation and maintenance of a ship security plan by giving recommendations for:

.1 its design, structure and content;

.2 integrating the particular features of the ship, the potential threats and vulnerabilities identified during the ship security assessment (SSA);

.3 interfacing the SSP with the existing company Safety Management System;

.4 procedures for internal verification, review and assessment of the SSP to ensure its compliance with the requirements and its continuing effectiveness;

.5 procedures to carry out amendments to the SSP subsequent to its approval;

.6 familiarisation of company staff with the SSP and related procedures

The documented security assessment is an essential and integral part for developing and updating the ship security plan (SSP) and a pre-condition for its approval by the flag State administration or Recognised Security Organisation (RSO).

3. Functional requirements

The ISPS Code contains, the following functional requirements related to the SSP:

.1 requirements for shipping companies to develop, implement and maintain a SSP for each of their ships which should be based upon security assessments;

.2 requirements for training drills and exercises to ensure familiarity with security plans and procedures

4. Definitions

.1 *International Ship and Port Facility Security (ISPS) Code* means the International Code for the Security of Ships and of Port Facilities 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), as adopted, on 12 December 2002, by resolution 2 of the

Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organisation;

.2 *Convention* means the International Convention for the Safety of Life at Sea, 1974, as amended;

.3 *Company* means the owner of the ship or any other organisation 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;

.4 *Ship Security Assessment (SSA)* means an assessment of the security risks of the operation of a ship;

.5 *Ship Security Plan (SSP)* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident;

.6 *Company Security Officer (CSO)* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained, and for liaison with port facility security officers and the ship security officer;

Additional GL Guidance:

Although the definition of a CSO is similar to that for the "Designated Person" in the ISM Code, the word ashore is not included. This will clarify the matter with regard to instances where the master is also the owner of the vessel and there is no company infrastructure ashore. In such cases the master may be both the company security officer and the ship security officer.

.7 *Ship Security Officer (SSO)* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers;

.8 *Security incident* means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity;

.9 *Security Level (SL)* means the qualification of the degree of risk that a security incident will be attempted or will occur;

.10 *Ship/port interface* means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship;

.11 *Ship-to-ship activity* means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another;

.12 *Recognised Security Organisation (RSO)* means an organisation with appropriate expertise in security and anti-terrorism matters recognized by the Administration (or designated authority) and authorised by it to carry out assessment, verification, approval and certification required by Part A of this Code, on its behalf;

.13 *Designated Authority* means the organisation(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility;

.14 *Contracting Government* means the Contracting Government, related to port facility security, within whose territory the port facility is located and includes a reference to the Designated Authority;

.15 *Port facility* means a location, as determined by the Contracting Government or designated authority, where interaction takes place between a ship and a port.

5. References

These Guidelines are based on:

.1 SOLAS 1974 as amended Chapter XI-2 Special measures to enhance maritime security;

.2 International Ship and Port Facility Security (ISPS) Code Parts A and Part B;

.3 United States Coast Guard (USCG) Navigation and Vessel Inspection Circular (NVIC) 10-02, Security Guidelines for Vessels;

.4 MSC/Circ.443, Measures to Prevent Unlawful Acts against Passengers and Crew on Board Ships;

.5 MSC/Circ.623, Piracy and Armed Robbery against Ships, guidance to ship owners and ship operators, ship masters and crews on preventing and suppressing acts of piracy and armed robbery against ships;

.6 International Safety Management (ISM) Code.

B. Ship Security Plan (SSP)

1. Purpose

The purpose of a SSP is to ensure the application of measures on board the ship established to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

Additional GL Guidance:

- *The results of the security assessment provide the basis for measures which are essential to develop, implement, maintain and update the SSP.*
- *The SSP should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1.*
- *The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so.*
- *Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.*

Reference: ISPS Code Part A/2.1.5, 8.1; Part B/1.11

2. Responsibilities

2.1 The Company

.1 The Company shall appoint:

.1 a Company Security Officer (CSO) for the Company;

.2 a Ship Security Officer (SSO) for each ship.

Additional GL Guidance:

The Company may appoint more than one CSO provided it is clearly stated in the SSP for which ship or ships each individual CSO is responsible.

.2 The Company shall ensure:

.1 development and implementation of a SSP based on the performance of a documented SSA by, or on behalf of, the CSO;

.2 availability of security procedures and records as objective evidence for the effective implementation of the SSP;

.3 provision of necessary support that the CSO, the Master and the SSO are able to perform their duties and responsibilities in compliance with the ISPS Code;

.4 a clear statement in the SSP emphasising the master's overriding authority and responsibility to make decisions with respect to the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary;

.5 provision and control of documented information to the vessel as required by Regulation XI-2/5;

.6 performance of internal audits and reviews of security activities;

.7 review of the SSA and SSP if required.

Additional GL Guidance:

Company support shall include but is not limited to provision of:

- *financial and personnel resources to establish, implement and maintain the SSP;*
- *training, drills and exercises to ensure the effective implementation of the SSP and to improve the security knowledge and consciousness;*
- *security installations, equipment, tools and its maintenance*

Provision of information shall include:

- *parties responsible for appointing ship personnel (ship management companies, manning agents, contractors, etc.),*
- *parties responsible for deciding employment of the vessel (charter or charterers),*
- *in cases when the ship is employed under terms of a charter party, details of the charter including time or voyage.*

Performance of audits and reviews:

- *internal audits and reviews of security activities to be carried out at least once every twelve (12) months onboard each ship;*
- *the Company shall also review the SSA and SSP should it be identified during training, drills or following an incident that the SSA and/or SSP are inappropriate.*

Audit records to be available:

- *records of any non-conformances identified*
- *any corrective action applied relative to non-conformances*
- *copy of internal audit report maintained on board the vessel*

Reference: ISPS Code Part A/6.1, 6.2, 11.1, 12.1; Part B/1.9, 1.10; 6

2.2 The Company Security Officer (CSO)

The duties and responsibilities of the CSO include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization (RSO);

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirement;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

Reference: ISPS Code Part A/11.2

2.3 The Ship Security Officer (SSO)

The duties and responsibilities of the CSO include, but are not limited to:

.14 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.15 maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;

.16 coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;

.17 proposing modifications to the ship security plan;

.18 reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

.19 enhancing security awareness and vigilance on board;

.20 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.21 reporting all security incidents;

.22 coordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

.23 ensuring that security equipment, if any, is properly operated, tested, calibrated and maintained.

Reference: ISPS Code Part A/11.2

ISPS Code requirements for the SSP

2.3 General requirements

.1 each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in the ISPS Code.

Reference: ISPS Code Part A/9.1

Guidance Part B/9.1:

.1 the CSO has the responsibility of ensuring that a SSP is prepared and submitted for approval.

.2 the content of each individual SSP should vary depending on the particular ship it covers.

.3 the Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail.

.4 Administrations may prepare advice on the preparation and content of a SSP.

Guidance Part B/9.2

Details to be addressed in the SSPs:

.1 detail the organizational structure of security for the ship;

.2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

.3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;

.4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;

.5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;

.6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

.7 reporting procedures to the appropriate Contracting Governments contact points

Guidance Part B/9.3

Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

Additional GL Guidance:

Companies may wish to produce a generic Ship Security Plan (SSP) that covers the management of security across a part of their fleet, or their entire fleet. Such an approach is acceptable provided

- *an "on site security survey" has been carried out on each ship and*
- *both the SSP and the SSA on which it is based reflect all relevant ship specific aspects.*

.2 a RSO may prepare the ship security plan for a specific ship.

Reference: ISPS Code Part A/9.1.1

.3 the Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to RSOs.

Reference: ISPS Code Part A/9.2

.4 the RSO undertaking the review and approval of a SSP, or its amendments, for a specific ship, shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review;

Reference: ISPS Code Part A/9.2.1

Guidance Part B/9.4

All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses an RSO to review or approve the SSP the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan

Additional GL Guidance:

If an RSO has been involved in the preparation of a SSP, it can not approve such a SSP or issue an ISSC to a ship that has implemented the plan.

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

Reference: ISPS Code Part A/9.3

Additional GL Guidance:

- *the ship security assessment (SSA) is an essential and integral part of the process of developing and updating the ship security plan (A/8.1);*
- *see GL guidelines for shipping companies for the development and implementation of a methodology for the performance of a ship security assessment.*

.6 such a plan shall be developed, taking into account the guidance given in part B of the ISPS Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included.

Reference: ISPS Code Part A/9.4

Additional GL Guidance:

GL recommend a translation in English language in order to facilitate PSC inspections. The language requirement applies also to the SSA documentation.

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

Reference: ISPS Code Part A/9.4.1

Guidance Part B/9.5

The CSO and SSO should develop procedures to:

.1 assess the continuing effectiveness of the SSP; and

.2 prepare amendments of the plan subsequent to its approval.

Additional GL Guidance:

The SSP should contain details of how the CSO intends to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

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

Reference: ISPS Code Part A/9.5

.9 the nature of the changes to the SSP or the security equipment that have been specifically approved by the Administration, pursuant to paragraph 3.1.8 (above), shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

Reference: ISPS Code Part A/9.5.1

Additional GL Guidance:

The approval and implementation of amendments to the approved SSP should be verified at each verification audit. This verification should cover every amendment to the approved SSP that has been approved by the Administration since the previous verification audit, or since the SSP was originally approved. Additional verifications for the implementation of amendments will be at the instruction of the Administration.

.10 the SSP may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

Reference: ISPS Code Part A/9.6

Additional GL Guidance:

Arrangements should be in place to ensure:

- *that SSP details kept in electronic format are protected against unauthorised deletion, destruction or amendment;*
- *availability of a protected updated back up SSP version;*
- *prevention of unauthorised access to the data (e.g. password system)*

.11 the SSP shall be protected from unauthorized access or disclosure;

Reference: ISPS Code Part A/9.7

Additional GL Guidance:

Arrangements should be in place to ensure:

- *that access to the details of the SSP is provided on the need to know, need to have and need to take basis;*
- *that all interested parties have sufficient access to the relevant sections of the SSP to allow them to effectively discharge their duties under the SSP. This includes arrangements to allow officers duly authorised by Contracting Governments, as stated in SOLAS XI-2/9 ("Port State Control"), access to the plan as allowed in ISPS A/9.8.1*

2.4 Port State control inspections

.1 Ship security plans are not subject to inspection by officers duly authorised by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9, save in circumstances specified in paragraph 3.2.2 below.

Reference: ISPS Code Part A/9.8

.2 If the officers duly authorised by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to ISPS A/9.4 subsections .2, .4, .5, .7, .15, .17 and .18 are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

Reference: ISPS Code Part A/9.8.1

Additional GL Guidance:

Details considered as confidential information which should not be subject to inspection unless otherwise agreed by the Contracting Governments concerned include:

- *identification of the restricted areas and measures for the prevention of unauthorised 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;*
- *duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;*
- *procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any;*
- *identification of the locations where the ship security alert system activation points are provided; and*
- *procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts. Administrations may allow, in order to avoid compromising the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.*

2.5 Details of the SSP

The plan should give detailed information of the security organisation on the ship including at least the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorised from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

Additional GL Guidance:

Measures are decided as a result from the SSA. Measures may be procedural or otherwise.

.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

Additional GL Guidance:

Internal audits should be conducted at least once every 12 months. Copies of internal audit reports should be retained onboard, for a minimum period of 5 years, treated as confidential information and protected against unauthorised disclosure

.9 procedures for training, drills and exercises associated with the plan;

Additional GL Guidance:

The schedule of drills and training should reflect the risks to security identified in the SSA.

.10 procedures for interfacing with port facility security activities

.11 procedures for the periodic review of the plan and for updating;

Additional GL Guidance:

The SSP should be reviewed at least once every 12 months in conjunction with the SSA. In addition should it be identified during training, drills or following an incident that the SSP, and hence the SSA, are inappropriate, they should be reviewed and amended accordingly. Records should be maintained of the review process.

.12 procedures for reporting security incidents;

Additional GL Guidance:

The incident reporting system in place may be utilised.

.13 identification of the ship security officer;

Additional GL Guidance:

Identification of the SSO can be by name or function.

.14 identification of the company security officer including 24-hour contact details;

Additional GL Guidance:

Identification of the CSO can be by name or position. Auditors may, as part of the verification process test the 24hr contact details supplied for the CSO.

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any;

Additional GL Guidance:

The objective of testing, calibration and maintenance should be to ensure that the equipment is "fit for purpose" and should be in accordance with manufacturers' recommendations.

.16 frequency for testing or calibration any security equipment provided on board, if any;

.17 identification of the locations where the ship security alert system activation points are provided; and

.18 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.

Additional GL Guidance:

Administrations may allow, in order to avoid any compromising of the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

Reference: ISPS Code Part A/9.4.1-9.4.18

Guidance Part B/9.6

The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and Part A of this Code will be carried out. Otherwise the process of issue to the ship of the required International Ship Security Certificate cannot be carried out. If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by, the Administration.

3. Organisation and Performance of Ship Security Duties

.1 In addition to the guidance given in Part B/9.2, (see 3.1.1 above) the SSP should establish the following which relate to all security levels:

.1 the duties and responsibilities of all shipboard personnel with a security role;

Additional GL Guidance:

Security responsibilities and duties of the crew for the three security levels (SL) may be defined in a function matrix developed by the CSO. The designation of security duties should be based upon the results of the on-scene survey taking into account the characteristics of the ship, its operational parameters and the constellation of the crew available. The Master and the Ship Security officer may revise the instruction as needed, based upon the crew available and the surrounding circumstances.

.2 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

Additional GL Guidance:

Communication procedures should be developed by the CSO based upon the results of the on-scene survey taking into account the characteristics of the ship, its operational parameters and the constellation of the crew available. The following should be considered

- *availability and readiness of transmitters, including satellite earth stations for immediate use on distress and security frequencies.*
- *measures when ships are in, or approaching areas where attacks occur or may occur.*
- *radio operational procedures prior to entering areas where attacks have occurred or where intelligence indicated attacks may occur*
- *where an INMARSAT ship each station is provided it may be appropriate to draft and store "standard messages" for ready use in an emergency.*
- *a special code for piracy / armed robbery/attack is available for use on digital selective calling (DSC) equipment. DSC equipment shall be modified to incorporate this facility.*
- *CSO and the SSO should communicate with Coast State and Port Authorities to develop a list of contacts needed to establish a plan that works.*
- *the Master, radio operators and watch keepers should be aware that potential attackers might be monitoring ship to shore communications and using intercepted information to select targets. When transmitting information on cargo, valuables and even status of ship's stores, caution is advised.*
- *constant radio watch should be maintained with appropriate naval or shore side authorities in areas where attacks have occurred or intelligence indicated attacks are imminent on all distress and safety frequencies: VHF Channel 16 and 2182 kHz.*
- *monitoring of all Maritime Safety Information Broadcasts. It is anticipated that INMARSAT's enhanced group calling will normally be used for such broadcasts using the SafetyNET(SM) service.*
- *reporting suspicious movements which may result in imminent attack, an Piracy, Armed Robbery or Terrorist attacks to the Cognisant Rescue Coordination Centre using a reporting checklist.*
- *communication in the case of direct threat to the ship or a danger to navigation in general.*
- *measures to activate the Security Alert and to notify the cognisant Rescue Coordination Centre*
- *authorisation to broadcast of an "All Stations" "Urgency Message"*
- *measures when an attack has occurred and the crew and ship are in danger requiring immediate assistance*
- *Master shall bear in mind that the distress signal is provided for use in cases of imminent danger and it shall not be used for less urgent purposes.*

.3 the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;

Additional GL Guidance:

- *The SSP to be reviewed at least annually and whenever required as a result of audits, drills and exercises and security incidents*
- *the existing procedures or measures of the Safety Management System may be utilised to perform audits, reviews and assessment, inspections and verifications to ensure the continuing effectiveness of the ship security system;*
- *the same applies to the current procedures to identify failures, deficiencies, system weaknesses or possibilities for improvements and to the implementation of corrective, preventive actions and improvements.*

.4 the procedures and practices to protect security sensitive information held in paper or electronic format;

Additional GL Guidance:

- *the SSP should be retained in a secure location;*
- *crewmen should be aware of the existence of plan and their roles in the security of the ship;*
- *the Master, SSO and CSO should be the only persons with access to the entire plan;*
- *copies of the plans shall be strictly controlled. Only the CSO and the SSO need retain copies of the SSP;*
- *surveyors, auditors from the Recognised Organisation, inspectors from the flag state, port authorities, port state inspectors and coastal state authorities should have limited access to the plan to make sure that it meets the intent of the regulations, however, no additional copies need to be provided.*

.5 the type and maintenance requirements, of security and surveillance equipment and systems, if any;

Additional GL Guidance:

List the security and surveillance equipment and systems and provide a maintenance routine for all listed items.

.6 the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and

.7 procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

Additional GL Guidance:

- *the existing incident reporting procedures of the SMS may be utilised or modified if required;*
- *the same applies for the procedures for the storage of dangerous goods or hazardous substances carried on board.*

.2 security measures that could be taken at each security level should cover:

.1 access to the ship by ship's personnel, passengers, visitors, etc;

.2 restricted areas on the ship;

.3 handling of cargo;

.4 delivery of ship's stores;

.5 handling unaccompanied baggage; and

.6 monitoring the security of the ship.

Reference: ISPS Code Part B/9.7; 9.8

4. Access to the ship

.1 The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

.1 access ladders;

.2 access gangways;

.3 access ramps;

.4 access doors, side scuttles, windows and ports;

.5 mooring lines and anchor chains; and

.6 cranes and hoisting gear.

.2 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

.3 The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship's personnel and visitors respectively. Any ship identification system should, when it is practicable to do so, be coordinated with that applying to the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

.4 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and to the national or local authorities with security responsibilities.

.5 The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Reference: ISPS Code Part B/9.9-9.13

5. Security Levels

5.1 Security Level 1

.1 At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

.1 checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc;

.2 in liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of people, baggage (including carry on items), personal effects, vehicles and their contents can take place;

.3 in liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;

.4 segregating checked persons and their personal effects from unchecked persons and their personal effects;

.5 segregating embarking from disembarking passengers;

.6 identification of access points that should be secured or attended to prevent unauthorized access;

.7 securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and

.8 providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

.2 At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

5.2 Security Level 2

.1 At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

.1 assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;

.2 limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;

.3 deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;

.4 establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;

.5 increasing the frequency and detail of searches of people, personal effects, and vehicles being embarked or loaded onto the ship;

.6 escorting visitors on the ship;

.7 providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and

.8 preparing for a full or partial search of the ship. (note – the ISPS Code is incorrect for this section and similar one at SL 3)

5.3 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.9 limiting access to a single, controlled, access point;

.10 granting access only to those responding to the security incident or threat thereof;

.11 directions of persons on board;

.12 suspension of embarkation or disembarkation;

.13 suspension of cargo handling operations, deliveries etc;

.14 evacuation of the ship;

.15 movement of the ship; and

.16 carrying out a full or partial search of the ship. (see .8 above)

Reference: ISPS Code Part B/9.14-9.17

6. Restricted areas on the ship

.1 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 prevent unauthorized access;

.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorised to be on board the ship;

.3 protect sensitive security areas within the ship; and

.4 protect cargo and ship's stores from tampering.

.2 The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas them.

.3 The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

.4 Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;

.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

.3 ventilation and air-conditioning systems and other similar spaces;

.4 spaces with access to potable water tanks, pumps, or manifolds;

.5 spaces containing dangerous goods or hazardous substances;

.6 spaces containing cargo pumps and their controls;

.7 cargo spaces and spaces containing ship’s stores;

.8 crew accommodation; and

.9 any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.

6.1 Security Level 1

.1 At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:

.1 locking or securing access points;

.2 using surveillance equipment to monitor the areas;

.3 using guards or patrols; and

.4 using automatic intrusion detection devices to alert the ship's personnel of unauthorised access.

6.2 Security Level 2

.1 At security level 2, the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorised persons have access. The SSP should establish the additional security measures to be applied, which may include:

.1 establishing restricted areas adjacent to access points;

.2 continuously monitoring surveillance equipment; and

.3 dedicating additional personnel to guard and patrol restricted areas.

6.3 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:

.1 setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and

.2 searching of restricted areas as part of a search of the ship.

Reference: ISPS Code Part B/9.18-9.24

7. Handling of cargo

.1 The security measures relating to cargo handling should:

.3 prevent tampering, and

.4 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

.2 The security measures, some of which may have to be applied in liaison with the port facility, should include inventory control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.

7.1 Security Level 1

.1 At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:

.1 routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations;

.2 checks to ensure that cargo being loaded matches the cargo documentation;

.3 ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and

.4 checking of seals or other methods used to prevent tampering.

.2 Checking of cargo may be accomplished by the following means:

.1 visual and physical examination; and

.2 using scanning/detection equipment, mechanical devices, or dogs.

.3 When there are regular, or repeated, cargo movement the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

7.2 Security Level 2

.1 At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:

.1 detailed checking of cargo, cargo transport units and cargo spaces;

.2 intensified checks to ensure that only the intended cargo is loaded;

.3 intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships; and

.4 increased frequency and detail in checking of seals or other methods used to prevent tampering.

.2 Detailed checking of cargo may be accomplished by the following means:

.1 increasing the frequency and detail of visual and physical examination;

.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs;

.3 and coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

7.3 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.4 suspension of the loading or unloading of cargo; and

.5 verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Reference: ISPS Code Part B/9.25-9.32

8. Delivery of ship's stores

.1 The security measures relating to the delivery of ship's stores should:

.1 ensure checking of ship's stores and package integrity;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering; and

.4 prevent ship's stores from being accepted unless ordered.

.2 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

8.2 Security Level 1

.1 At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:

.1 checking to ensure stores match the order prior to being loaded on board; and

.2 ensuring immediate secure stowage of ship's stores.

8.3 Security Level 2

.1 At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

8.4 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting ship's stores to more extensive checking;

.2 preparation for restriction or suspension of handling of ship's stores; and

.3 refusal to accept ship's stores on board the ship.

Reference: ISPS Code Part B/9.33-9.37

9. Handling of unaccompanied baggage

.1 the SSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship. It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

9.1 Security Level 1

.1 At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

9.2 Security Level 2

.1 At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

9.3 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;

.2 preparation for restriction or suspension of handling of unaccompanied baggage; and

.3 refusal to accept unaccompanied baggage on board the ship.

Reference: ISPS Code Part B/9.38-9.41

10. Monitoring the security of the ship

.1 The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

.1 lighting;

.2 watch-keepers, security guards and deck watches including patrols, and

.3 automatic intrusion detection devices and surveillance equipment.

.2 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

.3 The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

10.1 Security Level 1

.1 At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

.2 The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary. While underway, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulation for the Prevention of Collisions at Sea in force. The following should be considered when establishing the appropriate level and location of lighting:

.1 the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;

.2 coverage should include the area on and around the ship;

.3 coverage should facilitate personnel identification at access points; and

.4 coverage may be provided through coordination with the port facility.

10.2 Security Level 2

.1 At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

.1 increasing the frequency and detail of security patrols;

.2 increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;

.3 assigning additional personnel as security lookouts; and

.4 ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided.

.2 Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.

10.3 Security Level 3

.1 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 switching all lighting on, or illuminating the vicinity of, the ship;

.2 switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;

.3 maximizing the length of time such surveillance equipment can continue to record;

.4 preparation for underwater inspection of the hull of the ship; and

.5 initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

Reference: ISPS Code Part B/9.42-9.49

11. Differing security levels

.1 The SSP should establish details of the procedures and security measures the ship could adopt if the ship is at a higher security level than that applying to a port facility.

Reference: ISPS Code Part B/9.50

12. Activities not covered by the Code

.1 The SSP should establish 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 this Code does not apply
- .3 it is interfacing with fixed or floating platforms or a mobile drilling unit on location; or
- .4 it is interfacing with a port or port facility which is not required to comply with chapter XI-2 and part A of this Code.

Reference: ISPS Code Part B/9.51

13. Declarations of Security (DoS)

.1 The SSP should detail how requests for DoS from a port facility will be handled and the circumstances under which the ship itself should request a DoS.

Reference: ISPS Code Part B/9.52

14. Audit and review

.1 The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

Reference: ISPS Code Part B/9.53

15. Records

.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

- .1 training, drills and exercises;
- .2 security threats and security incidents;
- .3 breaches of security;
- .4 changes in security level;
- .5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- .6 internal audits and reviews of security activities;
- .7 periodic review of the ship security assessment;
- .8 periodic review of the ship security plan;
- .9 implementation of any amendments to the plan; and
- .10 maintenance, calibration and testing of security equipment, if any, including testing of the ship security alert system.

.2 The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

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

.4 The records shall be protected from unauthorized access or disclosure.

Guidance Part B/10

- .1 Records should be available to duly authorised officers of Contracting Governments to verify that the provisions of ship security plans are being implemented.
- .2 Records may be kept in any format but should be protect from unauthorized access or disclosure.

Additional GL Guidance:

Section 16 details the minimum records that must be retained onboard. It is unlikely that full compliance with the ISPS Code can be verified by these records alone. The company should have a procedure in place and implemented for the control of records.

16. Training, drills and exercises

.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of the Code;

.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of the Code;

.3 Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part B of the Code.

.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account guidance given in part B of the Code.

.5 The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

Reference: ISPS Code Part A/13

Guidance Part B/13.5-13.8

.3 The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security related deficiencies, which need to be addressed.

.4 To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel has been changed, at any one time, with personnel that has 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. These drills should test individual elements of the plan such as those security threats listed in paragraph 8.9.

.5 Various types of exercises which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as ship security officers, 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, resource availability, and response. These exercises may be:

.1 full scale or live;

.2 tabletop simulation or seminar; or

.3 combined with other exercises held such as search and rescue or emergency response exercises.

.6 Company participation in an exercise with another Contracting Government should be recognized by the Administration.

17. Approval of SSP and SSA documentation

.1 The SSP has to be developed on the basis of the results of the SSA. The SSP, or amendments thereto, and the documentation of the SSA or amendments, on which basis the plan has been developed, have to be submitted to the flag State administration or to the RSO for approval.

Reference: ISPS Code Part A/9.3

Additional GL Guidance:

Although there is no formal requirement for the SSA to be approved, it must accompany the SSP when the SSP is submitted for approval. The approval process for the SSP should include an evaluation of the SSA to verify that it is appropriate for the ship and that all the mandatory requirements for the SSA have been fulfilled.

18. Implementation, verification, certification

.1 The security measures specified in the SSP must be implemented, i.e. in operation, prior to the verification conducted by an RSO or flag State administration.

.2 Initial verification of compliance with the ISPS Code and issuance of the International Ship Security Certificate (ISSC) is dependent on the effective implementation of the SSP and the absence of non-compliances.

Reference: ISPS Code Part A/19

Additional GL Guidance:

Prior to initial verification for certification by an RSO or flag State administration, an internal security system verification (internal audit) is recommended to ensure its effective operation.

Reference: ISPS Code Part B/9.6