Recommendation 81

Guidance on the ISPS Code for Maritime Security Auditors

Introduction

1. Scope and Application

This guidance is intended for use by IACS Member Societies' auditors when performing certification audits under the ISPS Code, unless the relevant Administration has provided special instructions that indicate otherwise.

This document is also intended to facilitate audits' consistency and uniformity among IACS by providing examples, which, however are not to be interpreted as prescriptive solutions or checklists.

Reference is made to the following documents adopted by the International Maritime Organisation (IMO):

- SOLAS Chapter V
- SOLAS XI-1 and XI-2
- ISPS Code Parts A and B

The ISPS Code comprises Parts A and B. IMO has defined Part A as mandatory, Part B as Guidance to the Provisions of SOLAS Chapter XI-2 and Part A.of the ISPS Code. IACS considers, together with major Flag Administrations, that it is not possible to implement the provisions of part A without application of the relevant sections of Part B. In this regard, part B is to be considered mandatory by IACS auditors.

The term "should" when used in the above documents shall be taken to mean the same as "shall" and be construed to be a mandatory requirement.

2. Application of the ISPS Code by Companies

By design, the ISPS Code supports and encourages the development of a security culture in shipping. The content of the Ship Security Assessment and Security Plan will therefore be affected by the Company commitment, values and beliefs that cannot be enforced through the regulatory process. In carrying out the Ship Security Assessment (SSA) and developing the Ship Security Plan (SSP) Companies will have used guidance from Administrations, Industry Groups, IACS Societies and armed forces.

As with the ISM Code, assessing detailed compliance from detailed prescriptive management system solutions is not practical and is inconsistent with the concept of risk based approach. Each Company will develop solutions for its ships, individually tailored to meet their unique needs and trading patterns, whilst meeting internationally agreed standards for maritime security.

As an auditor, it is important to recognise that each Company develops and maintains a security management system that is most appropriate for the Company and their particular ships.

3. Certification Process

The verification of compliance with the mandatory rules and regulations, required as part of the ISPS Code, neither duplicates nor replaces the surveys required by other statutory surveys. Compliance with the ISPS Code does not relieve the Company, the Master or any other entity or

person involved in the management or operation of the ship of their responsibilities.

The verification process of compliance with the ISPS Code is an audit process involves interviews of shipboard personnel and a review of security assessment and Plan documentation and associated records. Audit is a sampling process and is not exhaustive in nature. Issuance of certification is based upon verification that the sample taken demonstrates that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of Chapter XI-2 of the Convention and Part A of the ISPS Code.

4. Editorial Principles

For convenience, this document incorporates the actual text of Part A and part B of the ISPS Code, followed by the relevant recommended guidance for IACS auditors. The document will be updated as necessary consistent with IACS Member Societies' experience in the audit process.

CHAPTER XI-2
SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

Regulation 1
Definitions

1 For the purpose of this chapter, unless expressly provided otherwise:

.1 *Bulk carrier* means a bulk carrier as defined in regulation IX/1.6.

.2 *Chemical tanker* means a chemical tanker as defined in regulation VII/8.2.

.3 *Gas carrier* means a gas carrier as defined in regulation VII/11.2.

.4 *High-speed craft* means a craft as defined in regulation X/1.2.

.5 *Mobile offshore drilling unit* means a mechanically propelled mobile offshore drilling unit, as defined in regulation IX/1, not on location.

.6 *Oil tanker* means an oil tanker as defined in regulation II-1/2.12.

.7 *Company* means a Company as defined in regulation IX/1.

.8 *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.

.9 *Port facility* is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.

.10 *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.

.11 *Designated Authority* means the organization(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.

.12 *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 Organization, provided that:

.1 amendments to part A of the Code are adopted, brought into force and take effect in accordance with article VIII of the present Convention concerning the amendment procedures applicable to the Annex other than chapter I; and

.2 amendments to part B of the Code are adopted by the Maritime Safety Committee in accordance with its Rules of Procedure.

.13 *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.

.14 *Security level* means the qualification of the degree of risk that a security incident will be attempted or will occur.

.15 *Declaration of security* means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.

.16 *Recognized security organization* means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by this chapter or by part A of the ISPS Code.

2 The term "ship", when used in regulations 3 to 13, includes mobile offshore drilling units and high-speed craft.

3 The term “all ships”, when used in this chapter, means any ship to which this chapter applies.

4 The term “Contracting Government”, when used in regulations 3, 4, 7, 10, 11, 12 and 13 includes a reference to the “Designated Authority”.

Regulation 2
Application

1 This chapter applies to:

.1 the following types of ships engaged on international voyages:

.1.1 passenger ships, including high-speed passenger craft;

.1.2 cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and

.1.3 mobile offshore drilling units; and

.2 port facilities serving such ships engaged on international voyages.

2 Notwithstanding the provisions of paragraph 1.2, Contracting Governments shall decide the extent of application of this chapter and of the relevant sections of part A of the ISPS Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

2.1 Contracting Governments shall base their decisions, under paragraph 2, on a port facility

security assessment carried out in accordance with the provisions of part A of the ISPS Code.

2.2 Any decision which a Contracting Government makes, under paragraph 2, shall not compromise the level of security intended to be achieved by this chapter or by part A of the ISPS Code.

3 This chapter does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

4 Nothing in this chapter shall prejudice the rights or obligations of States under international law.

Regulation 3
Obligations of Contracting Governments with respect to security

1 Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag. When changes in security level occur, security level information shall be updated as the circumstance dictates.

2 Contracting Governments shall set security levels and ensure the provision of security level information to port facilities within their territory, and to ships prior to entering a port or whilst in a port within their territory. When changes in security level occur, security level information shall be updated as the circumstance dictates.

B/Responsibilities of Contracting Governments

B/1.6 Contracting Governments have, under the provisions of chapter XI-2 and part A of this Code, various responsibilities, which, amongst others, include:

- setting the applicable security level;
- approving the Ship Security Plan and relevant amendments to a previously approved plan;
- verifying the compliance of ships with the provisions of chapter XI-2 and part A of this Code and issuing to ships the International Ship Security Certificate;
- determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port Facility Security Plan;
- ensuring completion and approval of the Port Facility Security Assessment and of any subsequent amendments to a previously approved assessment;
- approving the Port Facility Security Plan and any subsequent amendments to a previously approved plan; and
- exercising control and compliance measures**;**
- testing approved plans; and
- communicating information to the International Maritime Organization and to the shipping and port industries.

B/1.7 Contracting Governments can designate, or establish, Designated Authorities within Government to undertake, with respect to port facilities, their security duties under chapter XI-2 and Part A of this Code and allow Recognised Security Organisations to carry out certain work with respect to port facilities but the final decision on the acceptance and approval of this work should be given by the Contracting Government or the Designated Authority. Administrations may also delegate the undertaking of certain security duties**,** relating to ships, to Recognised Security Organizations. The following duties or activities cannot delegated to a Recognized Security Organization:

- setting of the applicable security level;
- determining which of the port facilities located within the territory of a Contracting Government

are required to designate a Port Facility Security Officer and to prepare a Port Facility Security Plan;
- approving a Port Facility Security Assessment or any subsequent amendments to a previously approved assessment;
- approving a Port Facility Security Plan or any subsequent amendments to a previously approved plan;
- exercising control and compliance measures; and
- establishing the requirements for a Declaration of Security.

B/Setting the Security Level

B/1.8 The setting of the security level applying at any particular time is the responsibility of Contracting Governments and can apply to ships and port facilities. Part A of this Code defines three security levels for international use. These are:

- Security Level 1, normal; the level at which ships and port facilities normally operate;
- Security Level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and
- Security Level 3, exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

Regulation 4
Requirements for Companies and ships

1 Companies shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

B/The Company and the Ship

B/1.9 Any Company operating ships to which chapter XI-2 and part A of this Code apply has to designate a Company Security Officer for the Company and a Ship Security Officer for each of its ships. The duties, responsibilities and training requirements of these officers and requirements for drills, and exercises are defined in part A of this Code.

B/1.10 The Company Security Officer's responsibilities include, in brief amongst others, ensuring that a Ship Security Assessment is properly carried out, that a Ship Security Plan is prepared and submitted for approval by, or on behalf of, the Administration and thereafter is placed on board each ship to which part A of this Code applies and in respect of which that person has been appointed as the Company Security Officer.

2 Ships shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code, and such compliance shall be verified and certified as provided for in part A of the ISPS Code.

3 Prior to entering a port or whilst in a port within the territory of a Contracting Government, a ship shall comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship.

4 Ships shall respond without undue delay to any change to a higher security level.

5 Where a ship is not in compliance with the requirements of this chapter or of part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

B/1.11 The Ship Security Plan 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.

B/1.12 The ships to which the requirements of chapter XI-2 and part A of this Code apply are required to have, and operated in accordance with, a Ship Security Plan approved by, or on behalf of, the Administration. The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan**,** for which the Administration has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation by the ship.

B/1.13 The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of this Code. Part A of this Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

B/1.14 When a ship is at a port or is proceeding to a port of a Contracting Government, the Contracting Government has the right, under the provisions of regulation XI-2/9, to exercise various control and compliance measures with respect to that ship. The ship is subject to port State control inspections but such inspections will not normally extend to examination of the Ship Security Plan itself except in specific circumstances. The ship may, also, be subject to additional control measures if the Contracting Government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

B/1.15 The ship is also required to have onboard information, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship.

Regulation 5
Specific responsibility of Companies

The Company shall ensure that the master has available on board, at all times, information through which officers duly authorised by a Contracting Government can establish:

.1 who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;

.2 who is responsible for deciding the employment of the ship; and

.3 in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

B/6.1	Regulation XI-2/5 requires the company to provide the master of the ship with information to meet the requirements of the Company under the provisions of this regulation. This information should include items such as:
.1	parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries, for example, retail sales outlets, casinos etc;
.2	parties responsible for deciding the employment of the ship including, time or bareboat charterer(s) or any other entity acting in such capacity; and
.3	in cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers
B/6.2	In accordance with regulation XI-2/5 the Company is obliged to update and keep this information current as and when changes occur.
B/6.3	This information should be in English, French or Spanish language.
B/6.4	With respect to ships constructed before [1 July 2004], this information should reflect the actual condition on that date.
B/6.5	With respect to ships constructed on or after [1 July 2004] and for ships constructed before [1 July 2004] which were out of service on [1 July 2004], the information should be provided as from the date of entry of the ship into service and should reflect the actual condition on that date.
B/6.6	After [1 July 2004] when a ship is withdrawn from service the information should be provided as from the date of re-entry of the ship into service and should reflect the actual condition on that date.
B/6.7	Previously provided information that does not relate to the actual condition on that date need not be retained on board.
B/6.8	When the responsibility for the operation of the ship is assumed by another Company, the information relating to the Company, which operated the ship, are not required to be left on board.

Regulation 6
Ship security alert system

1 All ships shall be provided with a ship security alert system, as follows:

.1 ships constructed on or after 1 July 2004;

.2 passenger ships, including high-speed passenger craft, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;

.3 oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first

survey of the radio installation after 1 July 2004; and

.4 other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.

2 The ship security alert system, when activated, shall:

.1 initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration**,** which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;

.2 not send the ship security alert to any other ships;

.3 not raise any alarm on-board the ship; and

.4 continue the ship security alert until deactivated and/or reset.

3 The ship security alert system shall:

.1 be capable of being activated from the navigation bridge and in at least one other location; and

.2 conform to performance standards not inferior to those adopted by the Organization.

4 The ship security alert system activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert.

5 The requirement for a ship security alert system may be complied with by using the radio installation fitted for compliance with the requirements of chapter IV, provided all requirements of this regulation are complied with.

6 When an Administration receives notification of a ship security alert, that Administration shall immediately notify the State(s) in the vicinity of which the ship is presently operating.

7 When a Contracting Government receives notification of a ship security alert from a ship which is not entitled to fly its flag, that Contracting Government shall immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

Regulation 7
Threats to ships

1 Contracting Governments shall set security levels and ensure the provision of security level information to ships operating in their territorial sea or having communicated an intention to enter their territorial sea.

B/Threats to ships and other incidents at Sea
B/4.21 Contracting Governments should provide general guidance on the measures considered

appropriate to reduce the security risk to ships flying their flag when at sea. They should provide specific advice on the action to be taken in accordance with security levels 1 to 3, if:

.1 there is a change in the security level applying to the ship while it is at sea, e.g. because of the geographical area in which it is operating or relating to the ship itself; and

.2 there is a security incident or threat thereof involving the ship while at sea.

Contracting Governments should establish the best methods and procedures for these purposes. In the case of an imminent attack the ship should seek to establish direct communication with those responsible in the flag State for responding to security incidents.

2 Contracting Governments shall provide a point of contact through which such ships can request advice or assistance and to which such ships can report any security concerns about other ships, movements or communications.

B/4.22 Contracting Governments should also establish a point of contact for advice on security for any ship:

.1 entitled to fly their flag; or

.2 operating in their territorial sea or having communicated an intention to enter their territorial sea.

3 Where a risk of attack has been identified, the Contracting Government concerned shall advise the ships concerned and their Administrations of:

.1 the current security level;

.2 any security measures that should be put in place by the ships concerned to protect themselves from attack, in accordance with the provisions of part A of the ISPS Code; and

.3 security measures that the coastal State has decided to put in place, as appropriate.

B/4.23 Contracting Governments should offer advice to ships operating in their territorial sea or having communicated an intention to enter their territorial sea, which could include advice:

1 to alter or delay their intended passage;

2 to navigate on a particular course or proceed to a specific location;

3 on the availability of any personnel or equipment that could be placed on the ship;

4 to co-ordinate the passage, arrival into port or departure from port, to allow escort by patrol craft or aircraft (fixed-wing or helicopter).

Contracting Governments should remind ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, of any temporary restricted areas that they have published.

B/4.24 Contracting Governments should recommend that ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, implement expeditiously, for the ship's protection and for the protection of other ships in the vicinity, any security measure the Contracting Government may have advised.

B/4.25 The plans prepared by the Contracting Governments for the purposes given in paragraph 4.22

should include information on an appropriate point of contact, available on a 24-hour basis, within the Contracting Government including the Administration. These plans should also include information on the circumstances in which the Administration considers assistance should be sought from nearby coastal States, and a procedure for liaison between port facility security officers and ship security officers.

Regulation 8
Master's discretion for ship safety and security

1 The master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgement of the master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

2 If, in the professional judgement of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship. In such cases, the master may implement temporary security measures and shall forthwith inform the Administration and, if appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures under this regulation shall, to the highest possible degree, be commensurate with the prevailing security level. When such cases are identified, the Administration shall ensure that such conflicts are resolved and that the possibility of recurrence is minimised.

Regulation 9
Control and compliance measures

B/Control and Compliance Measures [4]

4 Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution [3], inviting, amongst others, the Organisation to review Assembly Resolutions A.787(19) and A.882(21).

B/General

B/4.29 Regulation XI-2/9 describes the control and compliance measures applicable to ships under chapter XI-2. It is divided into three distinct sections; control of ships already in a port, control of ships intending to enter a port of another Contracting Government, and additional provisions applicable to both situations.

B/4.30 Regulation XI-2/9.1, control of ships in port, implements a system for the control of ships while in the port of a foreign country where duly authorised officers of the Contracting Government (duly authorized officers) have the right to go on board the ship to verify that the required certificates are in proper order. Then if there are clear grounds to believe the ship does not comply, control measures such as additional inspections or detention may be taken. This reflects current control systems [5].

Regulation XI-2/9.1 builds on such systems and allows for additional measures (including expulsion of a ship from a port to be taken as a control measure) when duly authorized officers have clear grounds for believing that a ship is in non-compliance with the requirements of chapter XI-2 or part A of this Code. Regulation XI-2/9.3 describes the safeguards that promote fair and proportionate implementation of these additional measures.

See regulation I/19 and regulation IX/6.2 of SOLAS 74 as amended, article 21 of LOADLINE 66 as modified by the 1988 LOADLINE Protocol, articles 5 and 6, regulation 8A of Annex I, regulation 15 of Annex II of MARPOL 73/78 as amended, article X of STCW 78 as amended and IMO Assembly Resolutions A.787(19) and A.882(21).

B/4.31 Regulation XI-2/9.2 applies control measures to ensure compliance to ships intending to enter a port of another Contracting Government and introduces an entirely different concept of control within chapter XI-2, applying to security only. Under this regulation measures may be implemented prior to the ship entering port, to better ensure security. Just as in regulation XI-2/9.1, this additional control system is based on the concept of clear grounds for believing the ship does not comply with chapter XI-2 or part A of this Code, and includes significant safeguards in regulations XI-2/9.2.2 and XI-2/9.2.5 as well as in regulation XI-2/9.3.

B/4.32 Clear grounds that the ship is not in compliance means evidence or reliable information that the ship does not correspond with the requirements of chapter XI-2 or part A of this Code, taking into account the guidance given in this part of the Code. Such evidence or reliable information may arise from the duly authorized officer's professional judgement or observations gained while verifying the ship's International Ship Security Certificate or Interim International Ship Security Certificate issued in accordance with part A of this Code (certificate) or from other sources. Even if a valid certificate is on board the ship, the duly authorized officers may still have clear grounds for believing that the ship is not in compliance based on their professional judgment.

B/4.33 Examples of possible clear grounds under regulations XI-2/9.1 and XI-2/9.2 may include, when relevant:

1 evidence from a review of the certificate that it is not valid or it has expired;

2 evidence or reliable information that serious deficiencies exist in the security equipment, documentation or arrangements required by chapter XI-2 and part A of this Code;

3 receipt of a report or complaint which, in the professional judgment of the duly authorized officer, contains reliable information clearly indicating that the ship does not comply with the requirements of chapter XI-2 or part A of this Code;

4 evidence or observation gained by a duly authorized officer using professional judgment that the master or ship's personnel is not familiar with essential shipboard security procedures or cannot carry out drills related to the security of the ship or that such procedures or drills have not been carried out;

5 evidence or observation gained by a duly authorized officer using professional judgment that key members ship's personnel are not able to establish proper communication with any other key members of ship's personnel with security responsibilities on board the ship;

6 evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another ship where either the port facility or the other ship is in violation of chapter XI-2 or part A of this Code, and the ship in question has not completed a Declaration of Security, nor taken appropriate, special or additional security measures or has not maintained appropriate ship security procedures;

7 evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another source (e.g., another ship or helicopter transfer) where either the port facility or the other source is not required to comply with chapter XI-2 or part A of this Code, and the ship has not taken appropriate, special or additional security measures or has not maintained appropriate security procedures; and

8. the ship holds a subsequent, consecutively issued Interim International Ship Security Certificate as described in section A/19.4, and if, in the professional judgment of an officer duly authorized, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and part A of this Code beyond the period of the initial interim certificate as described in section A/19.4.4.

B/4.34 The international law implications of regulation XI-2/9 are particularly relevant, and the regulation should be implemented with regulation XI-2/2.4 in mind, as the potential exists for situations where either measures will be taken which fall outside the scope of chapter XI-2, or where rights of affected ships, outside chapter XI-2, should be considered. Thus, regulation XI-2/9 does not prejudice the Contracting Government from taking measures having a basis in, and consistent with, international law, to ensure the safety or security of people, ships, port facilities and other property in cases where the ship, although in compliance with chapter XI-2 and part A of this Code, is still considered to present a security risk.

B/4.35 When a Contracting Government imposes control measures on a ship, the Administration should, without delay, be contacted with sufficient information to enable the Administration to fully liaise with the Contracting Government.

1 Control of ships in port

1.1 For the purpose of this chapter, every ship to which this chapter applies is subject to control when in a port of another Contracting Government by officers duly authorised by that Government, who may be the same as those carrying out the functions of regulation I/19. Such control shall be limited to verifying that there is onboard a valid International Ship Security Certificate or a valid Interim International Ship's Security Certificate issued under the provisions of part A of the ISPS Code (Certificate), which if valid shall be accepted, unless there are clear grounds for believing that the ship is not in compliance with the requirements of this chapter or part A of the ISPS Code.

1.2 When there are such clear grounds, or where no valid Certificate is produced when required, the officers duly authorized by the Contracting Government shall impose any one or more control measures in relation to that ship as provided in paragraph 1.3. Any such measures imposed must be proportionate, taking into account the guidance given in part B of the ISPS Code.

1.3 Such control measures are as follows: inspection of the ship, delaying the ship, detention of the ship, restriction of operations including movement within the port, or expulsion of the ship from port. Such control measures may additionally or alternatively include other lesser administrative or corrective measures.

B/Control of ships in port

B/4.36 Where the non-compliance is either a defective item of equipment or faulty documentation leading to the ship's detention and the non-compliance cannot be remedied in the port of inspection, the Contracting Government may allow the ship to sail to another port provided that any conditions agreed between the port States and the Administration or master are met.

2 Ships intending to enter a port of another Contracting Government

2.1 For the purpose of this chapter, a Contracting Government may require that ships intending to enter its ports provide the following information to officers duly authorized by that Government to ensure compliance with this chapter prior to entry into port with the aim of avoiding the need to impose control measures or steps:

.1 that the ship possesses a valid Certificate and the name of its issuing authority;

.2 the security level at which the ship is currently operating;

.3 the security level at which the ship operated in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.5 that the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified in paragraph 2.3; or

.6 other practical security related information (but not details of the ship security plan), taking into account the guidance given in part B of the ISPS Code.

If requested by the Contracting Government, the ship or the Company shall provide confirmation, acceptable to that Contracting Government, of the information required above.

B/4.37 Regulation XI-2/9.2.1 lists the information Contracting Governments may require from a ship as a condition of entry into port. One item of information listed is confirmation of any special or additional measures taken by the ship during its last ten calls at a port facility.

Examples could include:
1 records of the measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments; and
2 any Declarations of Security that were entered into with port facilities or other ships.

B/4.38 Another item of information listed, that may be required as a condition of entry into port, is confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility. It would not normally be required to include records of transfers of pilots, customs, immigration, security officials nor bunkering, lightering, loading of supplies and unloading of waste by ship within port facilities as these would normally fall within the auspices of the Port Facility Security Plan. Examples of information that might be given include:
1 records of the measures taken while engaged in a ship to ship activity with a ship flying the flag of a State which is not a Contracting Government especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;
2 records of the measures taken while engaged in a ship to ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions

of chapter XI-2 and part A of this Code such as a copy of any security certificate issued to that ship under other provisions; and

3 in the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of this Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of this Code to provide States with enough appropriate information to maintain their security integrity.

B/4.39 Examples of other practical security related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

1 information contained in the Continuous Synopsis Record;
2 location of the ship at the time the report is made;
3 expected time of arrival of the ship in port;
4 crew list;
5 general description of cargo aboard the ship;
6 passenger list; and
7 information required to be carried under regulation XI-2/10.

2.2 Every ship to which this chapter applies intending to enter the port of another Contracting Government shall provide the information described in paragraph 2.1 on the request of the officers duly authorized by that Government. The master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

2.3 The ship shall keep records of the information referred to in paragraph 2.1 for the last 10 calls at port facilities.

2.4 If, after receipt of the information described in paragraph 2.1, officers duly authorised by the Contracting Government of the port in which the ship intends to enter have clear grounds for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers shall attempt to establish communication with and between the ship and the Administration in order to rectify the non-compliance. If such communication does not result in rectification, or if such officers have clear grounds otherwise for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers may take steps in relation to that ship as provided in paragraph 2.5. Any such steps taken must be proportionate, taking into account the guidance given in part B of the ISPS Code.

2.5 Such steps are as follows:

.1 a requirement for the rectification of the non-compliance;

.2 a requirement that the ship proceed to a location specified in the territorial sea or internal waters of that Contracting Government;

.3 inspection of the ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter; or

.4 denial of entry into port.

Prior to initiating any such steps, the ship shall be informed by the Contracting Government of

its intentions. Upon this information the master may withdraw the intention to enter that port. In such cases, this regulation shall not apply.

B/4.40 Regulation XI-2/9.2.5 allows the master of a ship, upon being informed that the coastal or port State will implement control measures under regulation XI-2/9.2, to withdraw the intention for the ship to enter port. If the master withdraws that intention, regulation XI-2/9 no longer applies, and any other steps that are taken must be based on, and consistent with, international law.

3 Additional provisions

3.1 In the event:

.1 of the imposition of a control measure, other than a lesser administrative or corrective measure, referred to in paragraph 1.3; or

.2 any of the steps referred to in paragraph 2.5 are taken,

an officer duly authorized by the Contracting Government shall forthwith inform in writing the Administration specifying which control measures have been imposed or steps taken and the reasons thereof. The Contracting Government imposing the control measures or steps shall also notify the recognized security organization, which issued the Certificate relating to the ship concerned and the Organization when any such control measures have been imposed or steps taken.

3.2 When entry into port is denied or the ship is expelled from port, the authorities of the port State should communicate the appropriate facts to the authorities of the State of the next appropriate ports of call, when known, and any other appropriate coastal States, taking into account guidelines to be developed by the Organization. Confidentiality and security of such notification shall be ensured.

B/4.41 In all cases where a ship is denied entry or expelled from a port, all known facts should be communicated to the authorities of relevant States. This communication should consist of the following when known:

1 name of ship, its flag, the ship's identification number, call sign, ship type and cargo;
2 reason for denying entry or expulsion from port or port areas;
3 if relevant, the nature of any security non-compliance;
4 if relevant, details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage;
5 past port(s) of call and next declared port of call;
6 time of departure and likely estimated time of arrival at those ports;
7 any instructions given to ship, e.g., reporting on route;
8 available information on the security level at which the ship is currently operating;
9 information regarding any communications the port State has had with the Administration;
10 contact point within the port State making the report for the purpose of obtaining further information;
11 crew list; and
12 any other relevant information.

B/4.42 Relevant States to contact should include those along the ship's intended passage to its next

port, particularly if the ship intends to enter the territorial sea of that coastal State. Other relevant States could include previous ports of call, so that further information might be obtained and security issues relating to the previous ports resolved.

3.3 Denial of entry into port, pursuant to paragraphs 2.4 and 2.5, or expulsion from port, pursuant to paragraphs 1.1 to 1.3, shall only be imposed where the officers duly authorized by the Contracting Government have clear grounds to believe that the ship poses an immediate threat to the security or safety of persons, or of ships or other property and there are no other appropriate means for removing that threat.

3.4 The control measures referred to in paragraph 1.3 and the steps referred to in paragraph 2.5 shall only be imposed, pursuant to this regulation, until the non-compliance giving rise to the control measures or steps has been corrected to the satisfaction of the Contracting Government, taking into account actions proposed by the ship or the Administration, if any.

3.5 When Contracting Governments exercise control under paragraph 1 or take steps under paragraph 2:

.1 all possible efforts shall be made to avoid a ship being unduly detained or delayed. If a ship is thereby unduly detained, or delayed, it shall be entitled to compensation for any loss or damage suffered; and

.2 necessary access to the ship shall not be prevented for emergency or humanitarian reasons and for security purposes.

B/4.43 In exercising control and compliance measures, the duly authorized officers should ensure that any measures or steps imposed are proportionate. Such measures or steps should be reasonable and of the minimum severity and duration necessary to rectify or mitigate the non-compliance.

B/4.44 The word “delay” in regulation XI-2/9.3.3.1 also refers to situations where, pursuant to actions taken under this regulation, the ship is unduly denied entry into port or the ship is unduly expelled from port.

Regulation 10
Requirements for port facilities

1 Port facilities shall comply with the relevant requirements of this chapter and part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

2 Contracting Governments with a port facility or port facilities within their territory, to which this regulation applies, shall ensure that:

.1 port facility security assessments are carried out, reviewed and approved in accordance with the provisions of part A of the ISPS Code; and

.2 port facility security plans are developed, reviewed, approved and implemented in accordance with the provisions of part A of the ISPS Code.

3 Contracting Governments shall designate and communicate the measures required to be addressed in a port facility security plan for the various security levels, including when the

submission of a Declaration of Security will be required.

B/The Port Facility

B/1.16 Each Contracting Government has to ensure completion of a Port Facility Security Assessment for each of the port facilities**,** located within its territory, serving ships engaged on international voyages. The Contracting Government, a Designated Authority or a Recognized Security Organization may carry out this assessment. The completed Port Facility Security Assessment has to be approved by the Contracting Government or the Designated Authority concerned. This approval cannot be delegated. Port Facility Security Assessments should be periodically reviewed.

B/1.17 The Port Facility Security Assessment is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack. Security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.

The assessment must include the following components:

- the perceived threat to port installations and infrastructure must be determined;
- the potential vulnerabilities identified; and
- the consequences of incidents calculated.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk. The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan.

B/1.18 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to designate a Port Facility Security Officer. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

B/1.19 The Port Facility Security Plan should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the port facility 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 port facility could take to allow prompt response to the instructions that may be issued by those responding at security level 3 to a security incident or threat thereof.

B/1.20 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to have**,** and operate in accordance with, a Port Facility Security Plan approved by the Contracting Government or by the Designated Authority concerned. The Port Facility Security Officer should implement its provisions and monitor the continuing effectiveness and relevance of the plan, including commissioning internal audits of the application of the plan. Amendments to any of the elements of an approved plan, for which the Contracting Government or the Designated Authority concerned has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation at the port facility. The Contracting Government or the Designated Authority concerned may test the effectiveness of the plan. The Port Facility Security Assessment covering the port facility or on which the development of the plan has been based should be regularly reviewed. All these activities may lead to amendment of the approved plan. Any amendments to specified elements of an approved plan will have to be submitted for

approval by the Contracting Government or by the Designated Authority concerned.

B/1.21 Ships using port facilities may be subject to the port State control inspections and additional control measures outlined in regulation XI-2/9. The relevant authorities may request the provision of information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port. There may be circumstances in which entry into port could be denied.

Regulation 11
Alternative security agreements

1 Contracting Governments may, when implementing this chapter and part A of the ISPS Code, conclude in writing bilateral or multilateral agreements with other Contracting Governments on alternative security arrangements covering short international voyages on fixed routes between port facilities located within their territories.

2 Any such agreement shall not compromise the level of security of other ships or of port facilities not covered by the agreement.

3 No ship covered by such an agreement shall conduct any ship-to-ship activities with any ship not covered by the agreement.

4 Such agreements shall be reviewed periodically, taking into account the experience gained as well as any changes in the particular circumstances or the assessed threats to the security of the ships, the port facilities or the routes covered by the agreement.

B/Alternative Security Agreements

B/4.26 Contracting Governments, in considering how to implement chapter XI-2 and part A of this Code, may conclude one or more agreements with one or more Contracting Governments. The scope of an agreement is limited to short international voyages on fixed routes between port facilities in the territory of the parties to the agreement. When concluding an agreement, and thereafter, the Contracting Governments should consult other Contracting Governments and Administrations with an interest in the effects of the agreement. Ships flying the flag of a State that is not party to the agreement should only be allowed to operate on the fixed routes covered by the agreement if their Administration agrees that the ship should comply with the provisions of the agreement and requires the ship to do so. In no case can such an agreement compromise the level of security of other ships and port facilities not covered by it, and specifically, all ships covered by such an agreement may not conduct ship-to-ship activities with ships not so covered. Any operational interface undertaken by ships covered by the agreement should be covered by it. The operation of each agreement must be continually monitored and amended when the need arises and in any event should be reviewed every 5 years.

Regulation 12
Equivalent security arrangements

1 An Administration may allow a particular ship or a group of ships entitled to fly its flag to implement other security measures equivalent to those prescribed in this chapter or in part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Administration, which allows such security measures, shall communicate to the Organization particulars thereof.

2 When implementing this chapter and part A of the ISPS Code, a Contracting Government may allow a particular port facility or a group of port facilities located within its territory, other than those covered by an agreement concluded under regulation 11, to implement security measures equivalent to those prescribed in this chapter or in Part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Contracting Government, which allows such security measures, shall communicate to the Organization particulars thereof.

B/Equivalent arrangements for port facilities

B/4.27 For certain specific port facilities with limited or special operations but with more than occasional traffic, it may be appropriate to ensure compliance by security measures equivalent to those prescribed in chapter XI-2 and in part A of this Code. This can, in particular, be the case for terminals such as those attached to factories, or quaysides with no frequent operations..

Regulation 13
Communication of information

1 Contracting Governments shall, not later than 1 July 2004, communicate to the Organization and shall make available for the information of Companies and ships:

.1 the names and contact details of their national authority or authorities responsible for ship and port facility security;

.2 the locations within their territory covered by the approved port facility security plans.

.3 the names and contact details of those who have been designated to be available at all times to receive and act upon the ship-to-shore security alerts, referred to in regulation 6.2.1;

.4 the names and contact details of those who have been designated to be available at all times to receive and act upon any communications from Contracting Governments exercising control and compliance measures, referred to in regulation 9.3.1; and

.5 the names and contact details of those who have been designated to be available at all times to provide advice or assistance to ships and to whom ships can report any security concerns, referred to in regulation 7.2;

and thereafter update such information as and when changes relating thereto occur. The Organization shall circulate such particulars to other Contracting Governments for the information of their officers.

2 Contracting Governments shall, not later than 1 July 2004, communicate to the Organization the names and contact details of any recognized security organizations authorized to act on their behalf together with details of the specific responsibility and conditions of authority delegated to such organizations. Such information shall be updated as and when changes relating thereto occur. The Organization shall circulate such particulars to other Contracting Governments for the information of their officers.

3 Contracting Governments shall, not later than 1 July 2004 communicate to the Organization a

list showing the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval and thereafter shall further communicate when any of the following changes take place:

.1 changes in the location or locations covered by an approved port facility security plan are to be introduced or have been introduced. In such cases the information to be communicated shall indicate the changes in the location or locations covered by the plan and the date as of which such changes are to be introduced or were implemented;

.2 an approved port facility security plan, previously included in the list submitted to the Organization, is to be withdrawn or has been withdrawn. In such cases, the information to be communicated shall indicate the date on which the withdrawal will take effect or was implemented. In these cases, the communication shall be made to the Organization as soon as is practically possible; and

.3 additions are to be made to the list of approved port facility security plans.

In such cases, the information to be communicated shall indicate the location or locations covered by the plan and the date of approval.

B/4.14 Where a port facility has a PFSP that fact has to be communicated to the Organization and that information must also be made available to Company and Ship Security Officers. No further details of the PFSP have to be published other than that it is in place. Contracting Governments should consider establishing either central or regional points of contact, or other means of providing up to date information on the locations where PFSPs are in place, together with contact details for the relevant PFSO. The existence of such contact points should be publicised. They could also provide information on the recognized security organizations appointed to act on behalf of the Contracting Government, together with details of the specific responsibility and conditions of authority delegated to such recognised security organizations.

B/4.15 In the case of a port that does not have a PFSP (and therefore does not have a PFSO) the central or regional point of contact should be able to identify a suitably qualified person ashore who can arrange for appropriate security measures to be in place, if needed, for the duration of the ship's visit.

4 Contracting Governments shall, at five year intervals after 1 July 2004, communicate to the Organization a revised and updated list showing all the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval (and the date of approval of any amendments thereto) which will supersede and replace all information communicated to the Organization, pursuant to paragraph 3, during the preceding five years.

5 Contracting Governments shall communicate to the Organization information that an agreement under regulation 11 has been concluded. The information communicated shall include:

.1 the names of the Contracting Governments which have concluded the agreement;

.2 the port facilities and the fixed routes covered by the agreement;

.3 the periodicity of review of the agreement;

.4 the date of entry into force of the agreement; and

.5 information on any consultations which have taken place with other Contracting Governments;

and thereafter shall communicate, as soon as practically possible, to the Organization information when the agreement has been amended or has ended.

6 Any Contracting Government which allows, under the provisions of regulation 12, any equivalent security arrangements with respect to a ship entitled to fly its flag or with respect to a port facility located within its territory, shall communicate to the Organization particulars thereof.

7 The Organization shall make available the information communicated under paragraph 3 to other Contracting Governments upon request.

B/Information and Communication

B/1.22 Chapter XI-2 and part A of this Code require Contracting Governments to provide certain information to the International Maritime Organization and for information to be made available to allow effective communication between Contracting Governments and between Company/Ship Security Officers and the Port Facility Security Officers responsible for the port facility their ships visit.

B/4.17 Contracting Governments should also make the information indicated in paragraphs 4.14 to 4.16, available to other Contracting Governments on request.

Part A of
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS
AND OF PORT FACILITIES

PREAMBLE

AP/1 The Diplomatic Conference on Maritime Security held in London in December 2002 adopted new provisions in the International Convention for the Safety of Life at Sea, 1974 and this Code to enhance maritime security. These new requirements form the international framework through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

AP/2 Following the tragic events of 11th September 2001, the twenty-second session of the Assembly of the International Maritime Organization (the Organization), in November 2001**,** unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea**,** 1974 (known as the Diplomatic Conference on Maritime Security) in December 2002. Preparation for the Diplomatic Conference was entrusted to the Organization's Maritime Safety Committee (MSC) on the basis of submissions made by Member States, intergovernmental organizations and non-governmental organizations in consultative status with the Organization.

AP/3 The MSC, at its first extraordinary session, held also in November 2001, in order to accelerate the development and the adoption of the appropriate security measures established an MSC Intersessional Working Group on Maritime Security**.** The first meeting of the MSC Intersessional Working Group on Maritime Security was held in February 2002 and the outcome of its discussions was reported to, and considered by, the seventy-fifth session of the MSC in March 2002, when an *ad hoc* Working Group was established to further develop the proposals made. The seventy-fifth session of the MSC considered the report of that Working Group and recommended that work should be taken forward through a further MSC Intersessional Working Group, which was held in September 2002. The seventy-sixth session of the MSC considered the outcome of the September 2002 session of the MSC Intersessional Working Group and the further work undertaken by the MSC Working Group held in conjunction with the Committee's seventy-sixth session in December 2002, immediately prior to the Diplomatic Conference and agreed the final version of the proposed texts to be considered by the Diplomatic Conference.

AP/4 The Diplomatic Conference (9 to 13 December 2002) also adopted amendments to the existing provisions of the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) accelerating the implementation of the requirement to fit Automatic Identification Systems and adopted new Regulations in Chapter XI-1 of SOLAS 74 covering marking of the Ship's Identification Number and the carriage of a Continuous Synopsis Record. The Diplomatic Conference also adopted a number of Conference Resolutions including those covering implementation and revision of this Code, Technical Co-operation, and co-operative work with the International Labour Organization and World Customs Organization. It was recognised that review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these two Organizations.

AP/5 The provision of Chapter XI-2 of SOLAS 74 and this Code apply to ships and to port facilities. The extension of SOLAS 74 to cover port facilities was agreed on the basis that SOLAS 74 offered the speediest means of ensuring the necessary security measures entered into force and

given effect quickly. However, it was further agreed that the provisions relating to port facilities should relate solely to the ship/port interface. The wider issue of the security of port areas will be the subject of further joint work between the International Maritime Organization and the International Labour Organization. It was also agreed that the provisions should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack.

AP/6 In drafting the provision care has been taken to ensure compatibility with the provisions of the International Convention on Standards of Training, Certification and Watch-keeping and Certification for Seafarers, 1978, as amended, the International Safety Management (ISM) Code and the harmonised system of survey and certification.

AP/7 The provisions represent a significant change in the approach of the international maritime industries to the issue of security in the maritime transport sector. It is recognised that they may place a significant additional burden on certain Contracting Governments. The importance of Technical Co-operation to assist Contracting Governments implement the provisions is fully recognised.

AP/8 Implementation of the provisions will require continuing effective co-operation and understanding between all those involved with, or using, ships and port facilities including ship's personnel, port personnel, passengers, cargo interests, ship and port management and those in National and Local Authorities with security responsibilities. Existing practices and procedures will have to be reviewed and changed if they do not provide an adequate level of security. In the interests of enhanced maritime security additional responsibilities will have to be carried by the shipping and port industries and by National and Local Authorities.

AP/9 The guidance given in Part B of this Code should be taken into account when implementing the security provisions set out in Chapter XI-2 of SOLAS 74 and in Part A of this Code. However, it is recognised that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/or cargo.

AP/10 Nothing in this Code shall be interpreted or applied in a manner inconsistent with the proper respect of fundamental rights and freedoms as set out in international instruments, particularly those relating to maritime workers and refugees including the International Labour Organisation Declaration of Fundamental Principles and Rights at Work as well as international standards concerning maritime and port workers.

AP/11 Recognizing that the Convention on the Facilitation of Maritime Traffic, 1965, as amended, provides that foreign crew members shall be allowed ashore by the public authorities while the ship on which they arrive is in port, provided that the formalities on arrival of the ship have been fulfilled and the public authorities have no reason to refuse permission to come ashore for reasons of public health, public safety or public order, Contracting Governments when approving ship and port facility security plans should pay due cognisance to the fact that ship's personnel live and work on the vessel and need shore leave and access to shore based seafarer welfare facilities, including medical care.

No additional guidance

PART A

THE SAFETY OF LIFE AT SEA, 1974 AS AMENDED

MANDATORY REQUIREMENTS REGARDING THE PROVISIONS OF CHAPTER XI-2 OF THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974, AS AMENDED

1 GENERAL

A/1.1 Introduction

This part of the International Code for the Security of Ships and Port Facilities contains mandatory provisions to which reference is made in chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974 as amended.

B/General

B/1.1 The preamble of this Code indicates that chapter XI-2 and part A of this Code establish the new international framework of measures to enhance maritime security and through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

B/1.2 This introduction outlines, in a concise manner, the processes envisaged in establishing and implementing the measures and arrangements needed to achieve and maintain compliance with the provisions of chapter XI-2 and of part A of this Code and identifies the main elements on which guidance is offered. The guidance is provided in paragraphs 2 through to 19. It also sets down essential considerations, which should be taken into account when considering the application of the guidance relating to ships and port facilities.

B/1.3 If the reader's interest relates to ships alone, it is strongly recommended that this part of the Code is still read as a whole, particularly the sections relating to port facilities. The same applies to those whose primary interest are port facilities; they should also read the sections relating to ships.

B/1.4 The guidance provided in the following sections relates primarily to protection of the ship when it is at a port facility. There could, however, be situations when a ship may pose a threat to the port facility, e.g. because, once within the port facility, it could be used as a base from which to launch an attack. When considering the appropriate security measures to respond to ship-based security threats, those completing the Port Facility Security Assessment or preparing the Port Facility Security Plan should consider making appropriate adaptations to the guidance offered in the following sections.

B/1.5 The reader is advised that nothing in this Part of the Code should be read or interpreted in conflict with any of the provisions of either chapter XI-2 or part A of this Code and that the aforesaid provisions always prevail and override any unintended inconsistency which may have been inadvertently expressed in this Part of the Code. The guidance provided in this Part of the Code should always be read, interpreted and applied in a manner which is consistent with the aims, objectives and principles established in chapter XI-2 and part A of this Code.

No additional guidance

A/1.2 Objectives

The objectives of this Code are:

1 to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;

2 to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security;

3 to ensure the early and efficient collection and exchange of security-related information;

4 to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and

5 to ensure confidence that adequate and proportionate maritime security measures are in place.

The objective of the ISPS Code is to ensure an internationally agreed response to the threats posed by maritime security. To do this, the responsibilities of both Governments and Industry are to be defined and acknowledged. In addition a mechanism for the exchange of information between the interested parties is required. It is agreed that a qualitative risk based approach is adopted, the Code providing a methodology for performing the necessary risk assessments.

A/1.3 Functional requirements

In order to achieve its objectives, this Code embodies a number of functional requirements. These include, but are not limited to:

.1 gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;

.2 requiring the maintenance of communication protocols for ships and port facilities;

.3 preventing unauthorized access to ships, port facilities and their restricted areas;

.4 preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

.5 providing means for raising the alarm in reaction to security threats or security incidents;

.6 requiring ship and port facility security plans based upon security assessments; and

.7 requiring training, drills and exercises to ensure familiarity with security plans and procedures.

These are some of the requirements that must be satisfied if the objectives of the Code are to be met.

A/2 DEFINITIONS

A/2.1 For the purpose of this part, unless expressly provided otherwise:

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

.2 *Regulation* means a regulation of the Convention.

.3 *Chapter* means a chapter of the Convention.

.4 *Ship security plan* 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.

.5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons**,** cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

.6 *Ship security officer* 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.

.7 *Company security officer* 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.

Although this definition 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 the company security officer and the ship security officer.

.8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

.9 *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times.

.10 *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

.11 *Security level 3* means the level for which further specific protective security measures

shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The following additional definitions are used within PR 24 and this document:

The term *Non-compliance* means non fulfillment of a specified requirement or the subject is inappropriate for the ship

The term *Verification* means the audit of the SSP and associated procedures, checking the operational status of the Ship Security Alert System and checking a representative sample of associated security and surveillance equipment and systems mentioned in the SSP

2.2 The term “ship”, when used in this Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term “Contracting Government” in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the Designated Authority..

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

B/2.1 No guidance is provided with respect to the definitions set out in chapter XI-2 or part A of this Code.

B/2.2 For the purpose of this Part of the Code:
1 section. means a section of part A of the Code and is indicated as .section A/<followed by the number of the section>.;
2 paragraph. means a paragraph of this Part of the Code and is indicated as .paragraph <followed by the number of the paragraph>.; and
3 Contracting Government., when used in paragraphs 14 to 18, means the .Contracting Government within whose territory the port facility is located. and includes a reference to the Designated Authority..

Throughout the Code the term “Administration” is used to refer to that part of a Government with responsibilities for merchant shipping flying their Flag, “Designated Authority” refers to that part of a Government with responsibilities for Port Facility Security under their jurisdiction and “Contracting Government” is used to refer to any part of the Government, including the “Administration” or the “Designated Authority”.

A/3 APPLICATION

A/3.1 This Code applies to:

1 the following types of ships engaged on international voyages:

1 passenger ships, including high-speed passenger craft;

2 cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and

3 mobile offshore drilling units; and

2 port facilities serving such ships engaged on international voyages.

B/3.4 The provisions of chapter XI-2 and part A of this Code are not intended to apply to port facilities designed and used primarily for military purposes.

A/3.2 Notwithstanding the provisions of section 3.1.2, Contracting Governments shall decide the extent of application of this part of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

A/3.2.1 Contracting Governments shall base their decisions, under section 3.2, on a port facility security assessment carried out in accordance with this part of the Code.

A/3.2.2 Any decision which a Contracting Government makes, under section 3.2, shall not compromise the level of security intended to be achieved by chapter XI-2 or by this part of the Code.

A/3.3 This Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

A/3.4 Sections 5 to 13 and 19 of this part apply to Companies and ships as specified in regulation XI-2/4.

A/3.5 Sections 5 and 14 to 18 of this part apply to port facilities as specified in regulation XI-2/10.

A/3.6 Nothing in this Code shall prejudice the rights or obligations of States under international law.

B/General

B/3.1 The guidance given in this Part of the Code should be taken into account when implementing the requirements of chapter XI-2 and part A of this Code.

B/3.2 However, it should be recognized that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship.

B/3.3 Similarly, in relation to the guidance on port facilities, the extent to which this guidance applies will depend on the port facilities, the types of ships using the port facility, the types of cargo and/or passengers and the trading patterns of visiting ships.

The Code is applicable to, but not restricted to, ships that are subject to the ISM Code

A/4 RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

A/4.1 Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

.1 the degree that the threat information is credible;

.2 the degree that the threat information is corroborated;

.3 the degree that the threat information is specific or imminent; and

.4 the potential consequences of such a security incident.

A/4.2 Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

A/4.3 Contracting Governments may delegate to a recognized security organization certain of their security related duties under chapter XI-2 and this part of the Code with the exception of:

1 setting of the applicable security level;

2 approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;

3 determining the port facilities which will be required to designate a Port Facility Security Officer;

4 approving a Port Facility Security Plan and subsequent amendments to an approved plan;

5 exercising control and compliance measures pursuant to regulation XI-2/9; and

6 establishing the requirements for a Declaration of Security.

A/4.4 Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

B/Security of Assessments and Plans

B/4.1 Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans, and to individual assessments or plans.

B/Designated Authorities

B/4.2 Contracting Governments may identify a Designated Authority within Government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of this Code.

B/Recognized Security Organizations

B/4.3 Contracting Governments may authorize a Recognized Security Organization (RSO) to undertake certain security related activities, including:

1 approval of Ship Security Plans, or amendments thereto, on behalf of the Administration;

2 verification and certification of compliance of ships with the requirements of chapter

XI-2 and part A of this Code on behalf of the Administration; and

3 conducting Port Facility Security Assessments required by the Contracting Government.

B/4.4 An RSO may also advise or provide assistance to Companies or port facilities on security matters, including Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans. This can include completion of a Ship Security Assessment or Plan or Port Facility Security Assessment or Plan. If an RSO has done so in respect of a ship security assessment or plan that RSO should not be authorised to approve that ship security plan.

B/4.5 When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

1 expertise in relevant aspects of security;

2 appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;

3 their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimise such risks;

4 their ability to maintain and improve the expertise of their personnel;

5 their ability to monitor the continuing trustworthiness of their personnel;

6 their ability to maintain appropriate measures to avoid unauthorised disclosure of, or access to, security sensitive material;

7 their knowledge of the requirements chapter XI-2 and Part A of this Code and relevant national and international legislation and security requirements; and

8 their knowledge of current security threats and patterns;

9 their knowledge on recognition and detection of weapons, dangerous substances and devices;

10 their knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;

11 their knowledge on techniques used to circumvent security measures; and

12 their knowledge of security and surveillance equipment and systems and their operational limitations.

When delegating specific duties to an RSO, Contracting Governments, including Administrations, should ensure that the RSO has the competencies needed to undertake the task.

B/4.6 A Recognized Organization, as defined in regulation I/6 and fulfilling the requirements of regulation XI-1/1, may be appointed as a RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

B/4.7 A Port or Harbour Authority or Port Facility operator may be appointed as an RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

B/Setting the Security Level

B/4.8 In setting the security level Contracting Governments should take account of general and specific threat information. Contracting Governments should set the security level applying to ships or port facilities at one of three levels:

- Security level 1: normal, the level at which the ship or port facility normally operates;
- Security level 2: heightened, the level applying for as long as there is a heightened risk of a

security incident; and

- Security level 3: exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

B/4.9 Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

B/4.10 At all times the Master of a ship has the ultimate responsibility for the safety of the ship. Even at security level 3 a Master may seek clarification or amendment of instructions issued by those responding to a security incident, or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

B/4.11 The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liase at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility. Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility.s security level and should provide the ship with any relevant security information.

B/4.12 While there may be circumstances when an individual ship may be operating at a higher security level than the port facility it is visiting, there will be no circumstances when a ship can have a lower security level than the port facility it is visiting. If a ship has a higher security level than the port facility it intends to use, the CSO or SSO should advise the PFSO without delay. The PFSO should undertake an assessment of the particular situation in consultation with the CSO or SSO and agree on appropriate security measures with the ship, which may include completion and signing of a Declaration of Security.

B/4.13 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly. Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to ship and CSO and SSO. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish means of notifying PFSOs of changes in security levels. Contracting Governments should compile and maintain the contact details for a list of those who need to be informed of changes in security levels. Whereas the security level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the type and detail of the information conveyed and the method by which it is conveyed, to SSOs, CSOs and PFSOs.

B/4.16 Contracting Governments should also provide the contact details of Government officers to whom an SSO, a CSO and a PFSO can report security concerns. These Government officers should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting Government. In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate. For this purpose, the contact details of the Government officers should be communicated to the International Maritime Organization.

B/Identification Documents

B/4.18 Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.

B/Fixed and Floating Platforms and Mobile Drilling Units on location

B/4.19 Contracting Governments should consider establishing appropriate security measures for fixed and floating platforms and mobile offshore drilling units on location to allow interaction with ships which are required to comply with the provisions of chapter XI-2 and part A of this Code[1].

[1] Refer to Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, Mobile Offshore Drilling Units on location and Fixed and Floating Platforms Not Covered by Chapter XI-2 of 1974 SOLAS Convention, adopted by the Conference on Maritime Security by resolution [7].

B/Ships which are not required to comply with part A of this Code

B/4.20 Contracting Governments should consider establishing appropriate security measures to enhance the security of ships to which this chapter XI-2 and part A of this Code does not apply and to ensure that any security provisions applying to such ships allow interaction with ships to which part A of this Code applies.

B/Manning Level

B/4.28 In establishing the minimum safe manning of a ship the Administration should take into account[2] that the minimum safe manning provisions established by regulation V/14[3] only address the safe navigation of the ship. The Administration should also take into account any additional workload which may result from the implementation of the ship's security plan and ensure that the ship is sufficiently and effectively manned. In doing so the Administration should verify that ships are able to implement the hours of rest and other measures to address fatigue which have been promulgated by national law, in the context of all shipboard duties assigned to the various shipboard personnel.

[2] Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution [3], inviting, amongst others, the Organisation to review Assembly Resolution A.890(21) on Principles of Safe Manning. This review may also lead to amendments of regulation V/14.

[3] As was in force on the date of adoption of this Code.

B/Non-party ships and ships below convention size

B/4.45 With respect to ships flying the flag of a State which is not a Contracting Government to the Convention and not a Party to the 1988 SOLAS Protocol[6], Contracting Governments should not give more favourable treatment to such ships. Accordingly, the requirements of regulation XI-2/9 and the guidance provided in this Part of the Code should be applied to those ships.

[6] Protocol of 1988 relating to the International Convention for the Safety of Life at Sea, 1974.

B/4.46 Ships below Convention size are subject to measures by which States maintain security. Such measures should be taken with due regard to the requirements in chapter XI-2 and the guidance provided in this Part of the Code.

Contracting Governments may delegate authority to "Recognised Security Organisations" (RSOs) to undertake the following function on their behalf:

- **Approving "Ship Security Plans" (SSPs),**
- **Verifying implementation of the SSP onboard ships**
- **Issuing International Ship Security Certificates (ISSCs), including Interim ISSCs on their behalf.**

RSOs may also assist in the conducting of Ship Security Assessment (SSAs) and in the preparation of SSPs. In such circumstances the RSO must not approve the SSP, verify its implementation onboard or issue an ISSC to a ship in respect of the implementation.

A/5 DECLARATION OF SECURITY

A/5.1 Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses to people, property or the environment.

B/5.1 A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary or when a ship deems it necessary.

B/5.1.1 The need for a DoS may be indicated by the results of the Port Facility Security Assessment (PFSA) and the reasons and circumstances in which a DoS is required should be set out in the Port Facility Security Plan (PFSP).

B/5.1.2 The need for a DoS may be indicated by an Administration for ships entitled to fly its flag or as a result of a ship security assessment and should be set out in the ship security plan.

A/5.2 A ship can request completion of a Declaration of Security when:

.1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;

.2 there is an agreement on Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;

.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

.4 the ship is at a port which is not required to have and implement an approved port facility security plan; or

.5 the ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.

B/5.2 It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, or another ship with which it interfaces, and for ship/port interface or ship to ship activities that pose a higher risk to persons, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors.

B/5.2.1 In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the Port Facility Security Officer (PFSO) or Ship Security Officer (SSO)

should acknowledge the request and discuss appropriate security measures.

A/5.3 Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.

B/5.3 A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous goods or hazardous substances. The PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

A/5.4 The Declaration of Security shall be completed by:

.1 the master or the ship security officer on behalf of the ship(s); and, if appropriate,

.2 the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

B/5.4 The main purpose of a DoS is to ensure agreement is reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans.

B/5.4.1 The agreed DoS should be signed and dated by both the port facility and the ship(s), as applicable, to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level, or levels and the contact points.

B/5.4.2 A change in the security level may require that a new or revised DoS be completed.

A/5.5 The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

A/5.6 Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

A/5.7 Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

B/5.5 The DoS should be completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships, as applicable.

B/5.6 A model DoS is included in Appendix 1 to this Part of the Code.

Appendix 1 of ISPS Part B contains a pro forma "Declaration of Security" (DOS) which contains details of security arrangements which will normally be shared between the ship and the Port Facility. Although Administrations will specify the length of time that a DOC must be retained on board, the DOS should be kept on board for at least 10 ship/port or ship/ship interfaces to meet the requirements of ISPS A/10 and SOLAS XI-2/9.2.3.

The DOS can be likened to a ship / shore checklist.

A/6 OBLIGATIONS OF THE COMPANY

A/6.1 The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company shall establish in the ship security plan that the master has the 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.

There should be no conflict between the statement of "overriding authority" and the requirement in SOLAS XI-2/8 "Master's Discretion" and the requirements to act on instructions given by Contracting Governments at Security Level 3. It should be clear that when a conflict between "security" and "safety", then the requirement for "safety" shall prevail (SOLAS XI-2/8.2).

A/6.2 The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this part of the Code.

Manning the ship in accordance with the Safe Manning Document may not be sufficient to demonstrate that this requirements has been met. Auditors should ensure that security, and all other shipboard duties, are being effectively carried out and that requirements for work/rest times are being met.

A/7 SHIP SECURITY

A/7.1 A ship is required to act upon the security levels set by Contracting Governments as set out below.

A/7.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship security duties;

.2 controlling access to the ship;

.3 controlling the embarkation of persons and their effects;

.4 monitoring restricted areas to ensure that only authorized persons have access;

.5 monitoring of deck areas and areas surrounding the ship;

.6 supervising the handling of cargo and ship's stores; and

.7 ensuring that security communication is readily available.

A/7.3 At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

A/7.4 At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

It is not acceptable for a ship to claim that it operates at the highest state of security alertness regardless of the security level set by the Contracting Governments. There must be a progression from the measures employed at security level 1 through security level 2 to the measures employed at security level 3, or from level 1 direct to level 3.

A/7.5 Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

In order to verify that this requirement has been met, records of this acknowledgement should be kept on board. This will be in addition to the requirement in ISPS A/10.1.4 which requires records to be maintained of changing security levels. This record may be in the form of a logbook, or similar, entry.

A/7.6 Prior to entering a port, or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liase and co-ordinate the appropriate actions.

Records of this acknowledgement should be retained onboard.

A/7.7 If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

Records should be retained onboard.

A/7.7.1 In such cases, the ship security officer shall liase with the port facility security officer and co-ordinate appropriate actions, if necessary.

A/7.8 An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

A/7.9 When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

A/7.9.1 When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in the part B of this Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

Relevant guidance is provided under sections 8, 9 and 13.

A/8 SHIP SECURITY ASSESSMENT

A/8.1 The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

Companies may wish to produce a generic Ship Security Assessment (SSA) that covers the assessment of security risks 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 the SSA reflects all relevant ship specific aspects.

A/8.2 The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this section, taking into account the guidance given in part B of this Code.

B/8.1 The Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each of the ships in the Company's fleet which is required to comply with the provisions of chapter XI-2 and part A of this Code for which the CSO is responsible. While the CSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.

B/8.2 Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs. Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment. The CSO should follow any specific guidance offered by the Contracting Governments.

A/8.3 Subject to the provisions of section 9.2.1, a recognised security organisation may carry out the ship security assessment of a specific ship.

A RSO carrying out such a ship security assessment (SSA), whether in whole or in part, can not approve a SSP based on the SSA or certify a ship implementing the SSP.

A/8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key ship board operations that it is important to protect;

.3 identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

.4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

B/8.3 A SSA should address the following elements on board or within the ship:

1 physical security;
2 structural integrity;
3 personnel protection systems;
4 procedural policies;
5 radio and telecommunication systems, including computer systems and networks;
6 other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations on board the ship or within a port facility.

B/8.4 Those involved in a SSA should be able to draw upon expert assistance in relation to:

1 knowledge of current security threats and patterns;
2 recognition and detection of weapons, dangerous substances and devices;
3 recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
4 techniques used to circumvent security measures;
5 methods used to cause a security incident;
6 effects of explosives on ship's structures and equipment;
7 ship security;
8 ship/port interface business practices;
9 contingency planning, emergency preparedness and response;
10 physical security;
11 radio and telecommunications systems, including computer systems and networks;
12 marine engineering; and
13 ship and port operations.

B/8.5 The CSO should obtain and record the information required to conduct an assessment, including:

1 the general layout of the ship;
2 the location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.;
3 the location and function of each actual or potential access point to the ship;
4 changes in the tide which may have an impact on the vulnerability or security of the ship;
5 the cargo spaces and stowage arrangements;
6 the locations where the ship's stores and essential maintenance equipment is stored;
7 the locations where unaccompanied baggage is stored;
8 the emergency and stand-by equipment available to maintain essential services;
9 the number of ship's personnel, any existing security duties and any existing training requirement practices of the Company;
10 existing security and safety equipment for the protection of passengers and ship's personnel;
11 escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;
12 existing agreements with private security companies providing ship/waterside security

services; and

13 existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

B/8.6 The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

B/8.7 The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:

1 the restricted areas;
2 the response procedures to fire or other emergency conditions;
3 the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;
4 the frequency and effectiveness of security patrols;
5 the access control systems, including identification systems;
6 the security communications systems and procedures;
7 the security doors, barriers and lighting; and
8 the security and surveillance equipment and systems, if any.

B/8.8 The SSA should consider the persons, activities, services and operations that it is important to protect. This includes:

1 the ship's personnel;
2 passengers, visitors, vendors, repair technicians, port facility personnel, etc;
3 the capacity to maintain safe navigation and emergency response;
4 the cargo, particularly dangerous goods or hazardous substances;
5 the ship's stores;
6 the ship security communication equipment and systems, if any; and
7 the ship's security surveillance equipment and systems, if any.

B/8.9 The SSA should consider all possible threats, which may include the following types of security incidents:

1 damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
2 hijacking or seizure of the ship or of persons on board;
3 tampering with cargo, essential ship equipment or systems or ship's stores;
4 unauthorized access or use, including presence of stowaways;
5 smuggling weapons or equipment, including weapons of mass destruction;
6 use of the ship to carry those intending to cause a security incident and/or their equipment;
7 use of the ship itself as a weapon or as a means to cause damage or destruction**;**
8 attacks from seaward whilst at berth or at anchor; and
9 attacks whilst at sea.

B/8.10 The SSA should take into account all possible vulnerabilities, which may include:

1 conflicts between safety and security measures;
2 conflicts between shipboard duties and security assignments;

3 watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;
4 any identified security training deficiencies; and
5 any security equipment and systems, including communication systems.

B/8.11 The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

On-scene Security Survey

B/8.14 The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

1 ensuring the performance of all ship security duties;
2 monitoring restricted areas to ensure that only authorized persons have access;
3 controlling access to the ship, including any identification systems;
4 monitoring of deck areas and areas surrounding the ship;
5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
6 supervising the handling of cargo and the delivery of ship's stores; and
7 ensuring that ship security communication, information, and equipment are readily available.

There should be evidence that each individual ship has been subject to an "on site security survey

A/8.5 The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

B/8.12 Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

B/8.13 If the SSA has not been carried out by the Company the report of the SSA should be reviewed and accepted by the CSO.

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

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

A/9 SHIP SECURITY PLAN

A/9.1 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 this part of the Code.

B/9.1 The Company Security Officer (CSO) has the responsibility of ensuring that a Ship Security Plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. 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. Administrations may prepare advice on the preparation and content of a SSP.

B/9.2 All SSPs should:

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.

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.

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.

A/9.1.1 Subject to the provisions of section 9.2.1, a recognised security organisation may prepare the ship security plan for a specific ship.

If a 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.

A/9.2 The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognised security organisations.

A/9.2.1 In such cases the recognised security organisation, undertaking the review and approval of a ship security plan, 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.

B/9.4 All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognised Security Organisation (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.

A/9.3 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.

A/9.4 Such a plan shall be developed**,** taking into account the guidance given in part B of this 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. The plan shall address, 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 authorized from being taken on board the ship;

Measures may be procedural or otherwise.

.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;

.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;

The auditor should verify by interview that persons onboard are familiar with their duties and_responsibilities, as specified in the SSP.

.8 procedures for auditing the security activities;

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;

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;

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;

.13 identification of the ship security officer;

Identification of the SSO can be by name or position.

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

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;

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;[1] 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.1

[1] *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.*

B/9.5 CSOs and Ship Security Officers (SSOs) should develop procedures to:
1 assess the continuing effectiveness of the SSP; and
2 prepare amendments of the plan subsequent to its approval.

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.

Organization and Performance of Ship Security Duties

B/9.7 In addition to the guidance given in section 9.2, 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;
2 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

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;
4 the procedures and practices to protect security sensitive information held in paper or electronic format;
5 the type and maintenance requirements, of security and surveillance equipment and systems, if any;
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.

B/9.8 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:
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.

Access to the Ship

B/9.9 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.

B/9.10 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.

B/9.11 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 co-ordinated 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.

B/9.12 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.

B/9.13 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.

Security Level 1

B/9.14 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.

B/9.15 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.

Security Level 2

B/9.16 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 unauthorised 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-emphasising the procedures for reporting suspicious persons, objects, or

activities and the stressing the need for increased vigilance; and

8 carrying out a full or partial search of the ship.

Security Level 3

B/9.17 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 limiting access to a single, controlled, access point;
2 granting access only to those responding to the security incident or threat thereof;
3 directions of persons on board;
4 suspension of embarkation or disembarkation;
5 suspension of cargo handling operations, deliveries etc;
6 evacuation of the ship;
7 movement of the ship; and
8 preparing for a full or partial search of the ship.

Restricted Areas on the Ship

B/9.18 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 unauthorised 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.

B/9.19 The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas them.

B/9.20 The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security.

B/9.21 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.

Security Level 1

B/9.22 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 unauthorized access.

Security Level 2

B/9.23 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 authorized 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.

Security Level 3

B/9.24 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.

Handling of Cargo

B/9.25 The security measures relating to cargo handling should:
1 prevent tampering, and
2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

B/9.26 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.

Security Level 1

B/9.27 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.

B/9.28 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.

B/9.29 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.

Security Level 2

B/9.30 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.

B/9.31 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; and
3 co-ordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

Security Level 3

B/9.32 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 suspension of the loading or unloading of cargo; and
2 verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Delivery of Ship's Stores

B/9.33 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.

B/9.34 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.

Security Level 1

B/9.35 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.

Security Level 2

B/9.36 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.

Security Level 3

B/9.37 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.

Handling Unaccompanied Baggage

B/9.38 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.

Security Level 1

B/9.39 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.

Security Level 2

B/9.40 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.

Security Level 3

B/9.41 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.

Monitoring the Security of the Ship

B/9.42 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.

B/9.43 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

B/9.44 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.

Security Level 1

B/9.45 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.

B/9.46 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.

Security Level 2

B/9.47 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.

B/9.48 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.

Security Level 3

B/9.49 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 on of 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 maximising 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.

Declarations of Security

B/9.52 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.

The contents of the SSP should be sufficiently detailed as to make clear how each of the above areas is to be addressed and procedures implemented onboard.
For example, the sentence "*Onboard measures shall prevent unauthorized access to the ship.*" is not sufficient to demonstrate compliance with the requirement of ISPS A/9.4.3.

A/9.4.1 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.

Audit and Review

B/9.53 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.

A/9.5 The Administration shall determine which changes to an approved ship security plan 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 this part of the Code.

A/9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, 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.

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.

A/9.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.

A/9.7 The plan shall be protected from unauthorized access or disclosure.

Arrangements should be in place so 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

A/9.8 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 section 9.8.1.

A/9.8.1 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 section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

Differing Security Levels

B/9.50 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.

Activities not covered by the Code

B/9.51 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[7];

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.

[7] Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution [3].

A/10 RECORDS

A/10.1 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.

A/10.2 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.

A/10.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

A/10.4 The records shall be protected from unauthorized access or disclosure.

B/10.1 Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of ship security plans are being implemented.

B/10.2 Records may be kept in any format but should be protect from unauthorized access or disclosure.

Section 10 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. Auditors should ensure that sufficient records are available so that compliance, as required by ISPS 19.1.1.1, can be verified.

A/11 COMPANY SECURITY OFFICER

A/11.1 The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

A/11.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the company security officer shall 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 recognised security organisation;

.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.

B/Relevant guidance is provided under sections 8, 9 and 13.

A/12 SHIP SECURITY OFFICER

A/12.1 A ship security officer shall be designated on each ship.

The Ship Security Officer (SSO) shall have the authority onboard to enable the stated duties and responsibilities to be carried out effectively.

A/12.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

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

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

.3 co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

.5 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;

.6 enhancing security awareness and vigilance on board;

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

.8 reporting all security incidents;

.9 co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

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

B/Relevant guidance is provided under sections 8, 9 and 13.

The Auditor should confirm by interview with the SSO, and others, that these duties and responsibilities are understood both in general terms and how they are applied to this ship.

A/13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

A/13.1 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 this Code.

B/13.1 The Company Security Officer (CSO) and appropriate shore based Company personnel**,** and the Ship Security Officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

1 security administration;
2 relevant international conventions, codes and recommendations;
3 relevant Government legislation and regulations;
4 responsibilities and functions of other security organisations;
5 methodology of ship security assessment;
6 methods of ship security surveys and inspections;
7 ship and port operations and conditions;
8 ship and port facility security measures;
9 emergency preparedness and response and contingency planning;
10 instruction techniques for security training and education, including security measures and procedures;
11 handling sensitive security related information and security related communications;
12 knowledge of current security threats and patterns;
13 recognition and detection of weapons, dangerous substances and devices;
14 recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
15 techniques used to circumvent security measures;
16 security equipment and systems and their operational limitations;
17 methods of conducting audits, inspection, control and monitoring;
18 methods of physical searches and non-intrusive inspections;

	19	security drills and exercises, including drills and exercises with port facilities; and
	20	assessment of security drills and exercises.

A/13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

B/13.2	In addition the SSO should have adequate knowledge of, and receive training, in some or all of the following, as appropriate:	
	1	the layout of the ship;
	2	the ship security plan and related procedures (including scenario-based training on how to respond);
	3	crowd management and control techniques;
	4	operations of security equipment and systems; and
	5	testing, calibration and whilst at sea maintenance of security equipment and systems.

There should be evidence onboard that the SSO has received training in the areas identified in ISPS A/12.2. The effectiveness of this training should be ascertained by means that may include interview with the SSO.

A/13.3 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 this Code.

B/13.3	Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including**,** as appropriate:	
	1	knowledge of current security threats and patterns;
	2	recognition and detection of weapons, dangerous substances and devices;
	3	recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
	4	techniques used to circumvent security measures;
	5	crowd management and control techniques;
	6	security related communications;
	7	knowledge of the emergency procedures and contingency plans;
	8	operations of security equipment and systems;
	9	testing, calibration and whilst at sea maintenance of security equipment and systems,
	10	inspection, control, and monitoring techniques; and
	11	methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.
B/13.4	All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:	
	1	the meaning and the consequential requirements of the different security levels;
	2	knowledge of the emergency procedures and contingency plans;
	3	recognition and detection of weapons, dangerous substances and devices;
	4	recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and
	5	techniques used to circumvent security measures.

All crew onboard should have received security familiarization training appropriate to their

assigned security duties. The training should be documented to allow the auditor to verify that it has been carried out in a timely manner. Effectiveness of this training may be verified by interview.

A/13.4 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 this Code.

B/13.5 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.

B/13.6 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.

Drills and exercises should be conducted at the frequencies stated in Part B of the Code.

A/13.5 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.

B/13.7 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.

B/13.8 Company participation in an exercise with another Contracting Government should be recognised by the Administration.

Records should be available for all drills carried out on board the ship, including those which involved the company in compliance with ISPS A/13.5

14 PORT FACILITY SECURITY TO 18 "TRAINING FOR PORT FACILITIES"

There should be a process by which the ship can receive basic port security information prior to arrival.

A/19 VERIFICATION AND CERTIFICATION FOR SHIPS

A/19.1 Verifications

A/19.1.1 Each ship to which this part of the Code applies shall be subject to the verifications specified below:

.1 an initial verification before the ship is put in service or before the certificate required under section 19.2 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of chapter XI-2, this part of the Code and the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and this part of the Code, is in satisfactory condition and fit for the service for which the ship is intended;

.2 a renewal verification at intervals specified by the Administration, but not exceeding five years, except where section 19.3.1 or 19.3.4 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2, this part of the Code and the approved Ship Security Plan, is in satisfactory condition and fit for the service for which the ship is intended;

The use of the term "fully complies" in Section 19.1.1.1 and 19.1.1.2 means that a certificate cannot be issued unless ALL the requirements of the approved SSP are fully implemented and any associated security equipment and systems are present and fit for purpose. If the auditor identifies through objective evidence non-compliance in the approved SSP, this shall be communicated to the company, the Administration and the organisation that approved the plan. In such cases an ISSC shall not be issued until it can be shown that the security system, and any associated security equipment of the ship, is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A and B of the ISPS Code.

.3 at least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second and third anniversary date of the certificate as defined in regulation I/2(n). The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;

.4 any additional verifications as determined by the Administration.

A/19.1.2 The verifications of ships shall be carried out by officers of the Administration. The Administration may, however, entrust the verifications to a recognized security organization referred to in regulation XI-2/1.

A/19.1.3 In every case, the Administration concerned shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

A/19.1.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, this part of the Code and the approved ship security plan. After any verification under section 19.1.1 has been completed, no changes shall be made in security system and in any associated security equipment or the approved ship security plan without the sanction of the Administration.

At the Initial, Intermediate, Renewal and any additional verification, the auditor shall verify through a representative sample that at all security equipment and systems has been maintained and calibrated in accordance with the provisions of the SSP and the manufacturers' instructions.

A/19.2 Issue or endorsement of certificate

A/19.2.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

A/19.2.2 Such certificate shall be issued or endorsed either by the Administration or by the a recognized security organization acting on behalf of the Administration.

A/19.2.3 Another Contracting Government may, at the request of the Administration, cause the ship to be verified and, if satisfied that the provisions of section 19.1.1 are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship and, where appropriate, endorse or authorize the endorsement of that certificate on the ship, in accordance with this Code.

A/19.2.3.1 A copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Administration.

A/19.2.3.2 A certificate so issued shall contain a statement to the effect that it has been issued at the request of the Administration and it shall have the same force and receive the same recognition as the certificate issued under section 19.2.2.

A/19.2.4 The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix to this Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

No additional guidance.

A/19.3 Duration and validity of certificate

A/19.3.1 An International Ship Security Certificate shall be issued for a period specified by the Administration which shall not exceed five years.

On completion of an audit, and to facilitate the review process by the audit organisation, a certificate with validity not exceeding five (5) months may be issued by the auditor.

A/19.3.2 When the renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

A/19.3.2.1 When the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

A/19.3.2.2 When the renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the

renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

A/19.3.3 If a certificate is issued for a period of less than five years, the Administration may extend the validity of the certificate beyond the expiry date to the maximum period specified in section 19.3.1, provided that the verifications referred to in section 19.1.1 applicable when a certificate is issued for a period of five years are carried out as appropriate.

A/19.3.4 If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the Administration or recognized security organization acting on behalf of the Administration may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

A/19.3.5 If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Administration may extend the period of validity of the certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is verified, and then only in cases where it appears proper and reasonable to do so. No certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the expiry date of the existing certificate before the extension was granted.

A/19.3.6 A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the date of expiry of the existing certificate before the extension was granted.

A/19.3.7 If an intermediate verification is completed before the period specified in section 19.1.1, then:

.1 the expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;

.2 the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by section 19.1.1 are not exceeded.

A/19.3.8 A certificate issued under section 19.2 shall cease to be valid in any of the following cases:

.1 if the relevant verifications are not completed within the periods specified under section 19.1.1;

.2 if the certificate is not endorsed in accordance with section 19.1.1.3 and 19.3.7.2 if applicable;

.3 when a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and

.4 upon transfer of the ship to the flag of another State.

A/19.3.9 In the case of:

.1 a transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports, or

.2 a Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in section 19.4.2.

A/19.4 Interim certification

A/19.4.1 The certificates specified in section 19.2 shall be issued only when the Administration issuing the certificate is fully satisfied that the ship complies with the requirements of section 19.1. However, after [1 July 2004], for the purposes of:

.1 a ship without a certificate, on delivery or prior to its entry or re-entry into service;

.2 transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government;

.3 transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government; or

.4 when a Company assumes the responsibility for the operation of a ship not previously operated by that Company;

If the ship re-enters the management of a company after a "reasonable" period of time under the management of others, conformation should be sought from the Administration as to whether it is appropriate to issue interim certification.

until the certificate referred to in section 19.2 is issued, the Administration may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the Appendix to this part of the Code.

A/19.4.2 An Interim International Ship Security Certificate shall only be issued when the Administration or recognized security organization, on behalf of the Administration, has verified that:

.1 the ship security assessment required by this part of the Code has been completed,

.2 a copy of the ship security plan meeting the requirements of chapter XI-2 and part A of this Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;

.3 the ship is provided with a ship security alert system meeting the requirements of regulation XI-2/6, if required,

.4 the Company Security Officer:

.1 has ensured:

.1 the review of the ship security plan for compliance with this part of the Code,

.2 that the plan has been submitted for approval, and

.3 that the plan is being implemented on the ship, and

.2 has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the Company Security Officer is satisfied that the ship will successfully complete the required verification in accordance with section 19.1.1.1, within 6 months;

.5 arrangements have been made for carrying out the required verifications under section 19.1.1.1;

There should be evidence onboard that the company intends to conduct an internal security audit on the ship within three months and that the ship is planned to be offered for full term certification within the validity of the Interim ISSC.

.6 the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this part of the Code; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them; and

.7 the ship security officer meets the requirements of this part of the Code.

A/19.4.3 An Interim International Ship Security Certificate may be issued by the Administration or by a recognized security organization authorized to act on its behalf.

A/19.4.4 An Interim International Ship Security Certificate shall be valid for 6 months, or until the certificate required by section 19.2 is issued, whichever comes first, and may not be extended.

A/19.4.5 No Contracting Government shall cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgment of the Administration or the recognized security organization, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and this part of the Code beyond the period of the initial interim certificate as specified in section 19.4.4.

A/19.4.6 For the purposes of regulation XI-2/9, Contracting Governments may, prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the requirements of sections 19.4.2.4 to 19.4.2.6 have been met.

APPENDIX TO PART A
APPENDIX 1

Form of the International Ship Security Certificate
INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

Certificate No.

Issued under the provisions of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

Under the authority of the Government of _____
(name of State)

by _____
(persons or organization authorized)

Name of ship :……..……
Distinctive number or letters:…….……..…...
Port of registry :…….……
Type of ship :…….……
Gross tonnage :…….
IMO Number :……..……..
Name and address of the Company :……..……...

THIS IS TO CERTIFY:

1 that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2 that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3 that the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based ……..……..

This Certificate is valid until …….
subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at ……..
(place of issue of the Certificate)

Date of issue ……..
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate verification

Signed ……
(Signature of authorized official)
Place ……..

Date ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS*

Additional verification

Signed ……
(Signature of authorized official)
Place …….

Date ……

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed ……..…
(Signature of authorized official)
Place ……..

Date ……

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed ……
(Signature of authorized official)
Place …….

Date ……

(Seal or stamp of the authority, as appropriate)

* This part of the certificate shall be adapted by the Administration to indicate whether it has established additional verifications as provided for in section 19.1.1.4.

ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF THE ISPS CODE

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Signed ……
(Signature of authorized official)
Place …….

Date ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until …….

Signed ……
(Signature of authorized official)
Place ……

Date ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/*19.3.4* OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until …….

Signed ……
(Signature of authorized official)
Place ……

Date ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS CODE APPLIES

This Certificate shall, in accordance with section 19.3.5 / 19.3.6* of part A of the ISPS Code, be accepted as valid until …….

Signed ……
(Signature of authorized official)
Place …….

Date ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date** is ……..…

Signed ……
(Signature of authorized official)
Place …….

Date ……

(Seal or stamp of the authority, as appropriate)

***

Appendix 2

* Delete as appropriate.
** In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal)

(State)

Certificate No.

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the Government of _____
(name of State)

by _____
(persons or organization authorized)

Name of ship : ….....….….....
Distinctive number or letters : ….....
Port of registry : ….....….
Type of ship : ……….....
Gross tonnage : ….....
IMO Number : ….....….
Name and address of company : ….....…
Is this a subsequent, consecutive interim certificate? Yes/ No*
If Yes, date of issue of initial interim certificate….....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4* of the ISPS Code.

This Certificate is valid until ….....

Issued at ….....
(*place of issue of the certificate)*

Date of issue …..... …..... ….....
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

* Delete as appropriate.

Requirements of			*Questionnaire*
Part A	***Part B***		
Section 5/DECLARATION OF SECURITY			
	B/5.2		Is the need for a DoS set out in the ship security plan?
Section 6/ OBLIGATIONS OF THE COMPANY			
A/6.1			Has the Company ensured that the ship security plan contains a clear statement emphasizing the master's authority?
A/6.1			Has the Company established in the ship security plan that the master has the 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
A/6.2			Has the Company ensured that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this part of the Code?
	B/6.1		Has following information included?
		.1	parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries, for example, retail sales outlets, casinos etc
		.2	parties responsible for deciding the employment of the ship including, time or bareboat charterer(s) or any other entity acting in such capacity
		.3	in cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers
Section 8/ SHIP SECURITY ASSESSMENT			
A/8.2			Has the Ship Security Assessment carried out for the ship by the person with appropriate skills to evaluate the ship's security?
A/8.4			Has the SSA included the followings?
A/8.4			on-scene security survey
A/8.4.1			identification of existing security measures, procedures and operations
A/8.4.2			identification and evaluation of key ship board operations that it is important to protect
A/8.4.3			identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures;
A/8.4.4			identification of weaknesses, including human factors in the infrastructure, policies and procedures
	B/8.2		Prior to commencing the SSA, has the CSO ensured that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures?
	B/8.2		Has the CSO studied previous reports on similar security needs?
	B/8.2		Has the CSO met with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment, where feasible?
	B/8.2		Has the CSO should follow any specific guidance offered by the Contracting Governments?
	B/8.3		Has the SSA addressed the following elements on board or within the ship?
		.1	physical security
		.2	structural integrity
		.3	personnel protection systems
		.4	procedural policies
		.5	radio and telecommunication systems, including computer systems and networks;
		.6	other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations on board the ship or within a port facility
	B/8.4		Have those involved in a SSA been able to draw upon expert assistance in relation to the followings?

Requirements of			*Questionnaire*
Part A	***Part B***		
		.1	knowledge of current security threats and patterns
		.2	recognition and detection of weapons, dangerous substances and devices
		.3	recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security
		.4	techniques used to circumvent security measures
		.5	methods used to cause a security incident
		.6	effects of explosives on ship's structures and equipment
		.7	ship security
		.8	ship/port interface business practices
		.9	contingency planning, emergency preparedness and response
		.10	physical security
		.11	radio and telecommunications systems, including computer systems and networks
		.12	marine engineering
		.13	ship and port operations
	B/8.5	Has the CSO obtained and recorded the information required to conduct an assessment for followings?	
		.1	the general layout of the ship
		.2	the location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.
		.3	the location and function of each actual or potential access point to the ship
		.4	changes in the tide which may have an impact on the vulnerability or security of the ship
		.5	the cargo spaces and stowage arrangements
		.6	the locations where the ship's stores and essential maintenance equipment is stored
		.7	the locations where unaccompanied baggage is stored
		.8	the emergency and stand-by equipment available to maintain essential services
		.9	the number of ship's personnel, any existing security duties and any existing training requirement practices of the Company;
		.10	existing security and safety equipment for the protection of passengers and ship's personnel;
		.11	escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship
		.12	existing agreements with private security companies providing ship/waterside security services
		.13	existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.
	B/8.6	Has the SSA examineed each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security? This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.	
	B/8.7	Has the SSA considered the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance for Followings?	
		.1	the restricted areas
		.2	the response procedures to fire or other emergency conditions
		.3	the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.

Requirements of			*Questionnaire*
Part A	*Part B*		
		.4	the frequency and effectiveness of security patrols
		.5	the access control systems, including identification systems
		.6	the security communications systems and procedures
		.7	the security doors, barriers and lighting
		.8	the security and surveillance equipment and systems, if any
	B/8.8	Has the SSA considered the following persons, activities, services and operations that it is important to protect?	
		.1	the ship's personnel
		.2	passengers, visitors, vendors, repair technicians, port facility personnel, etc;
		.3	the capacity to maintain safe navigation and emergency response
		.4	the cargo, particularly dangerous goods or hazardous substances
		.5	the ship's stores
		.6	the ship security communication equipment and systems, if any
		.7	the ship's security surveillance equipment and systems, if any
	B/8.9	Has the SSA considered all possible threats, which may include the following types of security incidents?	
		.1	damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism
		.2	hijacking or seizure of the ship or of persons on board
		.3	tampering with cargo, essential ship equipment or systems or ship's stores
		.4	unauthorized access or use, including presence of stowaways
		.5	smuggling weapons or equipment, including weapons of mass destruction
		.6	use of the ship to carry those intending to cause a security incident and/or their equipment
		.7	use of the ship itself as a weapon or as a means to cause damage or destruction
		.8	attacks from seaward whilst at berth or at anchor
		.9	attacks whilst at sea
	B/8.10	Has the SSA taken into account all possible vulnerabilities for followings?	
		.1	conflicts between safety and security measures
		.2	conflicts between shipboard duties and security assignments;
		.3	watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance
		.4	any identified security training deficiencies
		.5	any security equipment and systems, including communication systems
	B/8.11	Has the particular consideration been given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods?	
	B/8.12	Upon completion of the SSA, has the report been prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability?	
	B/8.13	If the SSA has not been carried out by the Company, has the report of the SSA been reviewed and accepted by the CSO?	
	B/8.14	Has the on-scene security survey been examined and evaluated existing shipboard protective measures, procedures and operations for followings?	
		.1	ensuring the performance of all ship security duties
		.2	monitoring restricted areas to ensure that only authorized persons have access;

Requirements of			*Questionnaire*
Part A	*Part B*		
		.3	controlling access to the ship, including any identification systems
		.4	monitoring of deck areas and areas surrounding the ship
		.5	controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
		.6	supervising the handling of cargo and the delivery of ship's stores;
		.7	ensuring that ship security communication, information, and equipment are readily available
Section 9/ SHIP SECURITY PLAN			
A/9.3	Does the result of Ship Security Assessment attach to the Ship Security Plan?		
A/9.4	Does the Plan address 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 authorized from being taken on board the ship
		.2	identification of the restricted areas and measures for the prevention of unauthorized access
		.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
		.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
		.9	procedures for training, drills and exercises associated with the plan
		.10	procedures for interfacing with port facility security activities
		.11	procedures for the periodic review of the plan and for updating
		.12	procedures for reporting security incidents
		.13	identification of the ship security officer
		.14	identification of the company security officer including with 24-hour contact details
		.15	procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any
		.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
		.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
A/9.4.1	Is the personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship?		
A/9.6	In the case that the Plan is to be kept in an electronic format, is it to be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment?		
	B/9.2	Does the SSP contain following contents?	
		.1	detail of the organizational structure of security for the ship

Requirements of			*Questionnaire*
Part A	***Part B***		
		.2	detail of the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility
		.3	detail of the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
		.4	detail of the basic security measures for security level 1, both operational and physical, that will always be in place
		.5	detail of 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	details of the regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances
		.7	reporting procedures to the appropriate Contracting Governments contact points
	B/9.3		Has the preparation of an effective SSP rested 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?
	B/9.4		Has this Society not prepared, or assisted in the preparation of, the plan?
	B/9.5		Have the following procedures been developed by CSO and SSO?
		.1	assess the continuing effectiveness of the SSP
		.2	prepare amendments of the plan subsequent to its approval
	B/9.7		Has the SSP established the following which relate to all security levels?
		.1	the duties and responsibilities of all shipboard personnel with a security role
		.2	the procedures or safeguards necessary to allow such continuous communications to be maintained at all times
		.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
		.4	the procedures and practices to protect security sensitive information held in paper or electronic format
		.5	the type and maintenance requirements, of security and surveillance equipment and systems, if any
		.6	the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns
		.7	procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location
(Access to the Ship)			
	B/9.9		Has the SSP established the security measures covering all means of access to the ship identified in the SSA?
		.1	access ladders
		.2	access gangways
		.3	access ramps
		.4	access doors, side scuttles, windows and ports
		.5	mooring lines and anchor chains
		.6	cranes and hoisting gear
	B/9.10		Has the SSP identified the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels for each level?
	B/9.10		Has the SSP established the type of restriction or prohibition to be applied and the means of enforcing them for each security level?

Requirements of		*Questionnaire*	
Part A	***Part B***		
	B/9.11	Has the SSP established 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?	
	B/9.11	Has any ship identification system been co-ordinated with that applying to the port facility?	
	B/9.11	Has the SSP established provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action?	
	B/9.13	Has the SSP established the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis?	
	(Security Level 1)		
	B/9.14	Has the SSP established the following security measures to control access to the ship?	
		.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
		.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
	B/9.15	Has the SSP specified that all those seeking to board a ship should be liable to search, and has the frequency of such searches, including random searches, been specified in the SSP?	
	(Security Level 2)		
	B/9.16	Has the SSP established the following security measures?	
		.1	assigning additional personnel to patrol deck areas during silent hours to deter unauthorised 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- emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance
		.8	carrying out a full or partial search of the ship
	(Security Level 3)		
	B/9.17	Has the SSP detailed the following security measures?	

Requirements of			*Questionnaire*
Part A	***Part B***		
		.1	limiting access to a single, controlled, access point
		.2	granting access only to those responding to the security incident or threat thereof;
		.3	directions of persons on board
		.4	suspension of embarkation or disembarkation
		.5	suspension of cargo handling operations, deliveries etc
		.6	evacuation of the ship
		.7	movement of the ship
		.8	preparing for a full or partial search of the s
(Restricted Areas on the Ship)			
	B/9.18		Has the SSP identified the restricted areas to be established on the ship, specified 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?
	B/9.19		Does the SSP ensure that there are clearly established policies and practices to control access to all restricted areas them?
	B/9.20		Does the SSP provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security?
	B/9.21		Does the restricted areas include the followings?
		.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
		.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
	(Security Level 1)		
	B/9.22		Has the SSP established the following security measures to be applied to restricted areas?
		.1	locking or securing access points
		.2	using surveillance equipment to monitor the areas
		.3	using guards or patrols
		.4	using automatic intrusion detection devices to alert the ship’s personnel of unauthorized access
	(Security Level 2)		
	B/9.23		Has the frequency and intensity of the monitoring of, and control of access to restricted areas been increased to ensure that only authorized persons have access?

Requirements of			*Questionnaire*
Part A	***Part B***		
	B/9.23	Has the SSP established the following additional security measures?	
		.1	establishing restricted areas adjacent to access points
		.2	continuously monitoring surveillance equipment
		.3	dedicating additional personnel to guard and patrol restricted areas
	(Security Level 3)		
	B/9.24	Has the SSP detailed the following security measures which could be taken by the ship, in close co-operations with those responding and the port facility?	
		.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
		.2	searching of restricted areas as part of a search of the ship
(Handling of Cargo)			
	(Security Level 1)		
	B/9.27	Has the SSP established the following security measures to be applied during cargo handling?	
		.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
		.4	checking of seals or other methods used to prevent tampering
	(Security Level 2)		
	B/9.30	Has the SSP established the following additional security measures to be applied during cargo handling>	
		.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
		.4	increased frequency and detail in checking of seals or other methods used to prevent tampering
	(Security Level 3)		
	B/9.32	Has the SSP detailed the following security measures which could be taken by the ship, in close co-operation with those responding and the port facility?	
		.1	suspension of the loading or unloading of cargo
		.2	verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location
(Delivery of Ship's Store)			
	(Security Level 1)		
	B/9.35	Has the SSP established the following security measures to be applied during delivery of ship’s stores?	
		.1	checking to ensure stores match the order prior to being loaded on board
		.2	ensuring immediate secure stowage of ship’s stores
	(Security Level 2)		

Requirements of			*Questionnaire*
Part A	*Part B*		
	B/9.36		Has the SSP established 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?
	(Security Level 3)		
	B/9.37		Has the SSP detailed the following security measures which could be taken by the ship, in close co-operation with those responding and the port facility?
		.1	subjecting ship's stores to more extensive checking
		.2	preparation for restriction or suspension of handling of ship's stores
		.3	refusal to accept ship's stores on board the ship
(Handling Unaccompanied Baggage)			
	(Security Level 1)		
	B/9.39		Has the SSP established 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?
	(Security Level 2)		
	B/9.40		Has the SSP established the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage?
	(Security Level 3)		
	B/9.41		Has the SSP detailed the following security measures which could be taken by the ship, in close co-operation with those responding and the port facility?
		.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
		.3	refusal to accept unaccompanied baggage on board the ship.
(Monitoring the Security of the Ship)			
	B/9.44		Has the SSP established 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?
	(Security Level 1)		
	B/9.45		Has the SSP established 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?
	B/9.46		Has the following been 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
		.4	coverage may be provided through coordination with the port facility
	(Security Level 2)		

Requirements of			*Questionnaire*
Part A	***Part B***		
	B/9.47	Has the SSP established the following additional security measures to be applied to enhance the monitoring and surveillance capabilities?	
		.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
		.4	ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided
	(Security Level 3)		
	B/9.49	Has the SSP detailed the following security measures which could be taken by the ship, in close co-operation with those responding and the port facility?	
		.1	switching on of 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	maximising the length of time such surveillance equipment can continue to record
		.4	preparation for underwater inspection of the hull of the ship
		.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
(Differing Security Levels)			
	B/9.50	Has the SSP established 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?	
(Activities not covered by the Code)			
	B/9.51	Has the SSP established details of the procedures and security measures the ship should apply when the following cases?	
		.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
		.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
(Declaration of Security)			
	B/9.52	Has the SSP detailed how requests for DoS from a port facility will be handled and the circumstances under which the ship itself should request a DoS?	
(Audit and Review)			
	B/9.53	Has 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?	
Section 10/ RECORDS			
A/10.3	In the case that the records are to be kept in an electronic format, is it to be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment?		
Section 11/ COMPANY SECURITY OFFICER			
A/11.1	Does the Company Security Officer designated for the ship?		

Requirements of		***Questionnaire***
Part A	***Part B***	
A/11.2	Are following duties and responsibilities of the company security officer included in the Plan?	
	.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 recognised security organisation
	.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
	.13	ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained
Section 12/ SHIP SECURITY OFFICER		
A/12.1	Does the Ship Security Officer designated on the ship?	
A/12.2	Are following duties and responsibilities of the ship security officer included in the Plan?	
	.1	undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained
	.2	maintaining and supervising the implementation of the ship security plan, including any amendments to the plan
	.3	co-ordinating the security aspects of the handling of cargo and ship’s stores with other shipboard personnel and with the relevant port facility security officers;
	.4	proposing modifications to the ship security plan
	.5	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
	.6	enhancing security awareness and vigilance on board
	.7	ensuring that adequate training has been provided to shipboard personnel, as appropriate
	.8	reporting all security incidents
	.9	co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer
	.10	ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

Requirements of SOLAS XI-2		*Questionnaire*
Regulation 5/ Specific responsibility of Companies		
	Has the Company ensured that the master has available on board, at all times, the following information?	
	.1	who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship
	.2	who is responsible for deciding the employment of the ship
	.3	in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies)
Regulation 6/ Ship security alert system		
1	Has the ship been provided with a ship security alert system? (Ship's type =)(required*/not required*)	
3	.1	Has the ship security alert system been capable of being activated from the navigation bridge and in at least one other location?
	.2	Has the ship security alert system been conformed to performance standards not inferior to those adopted by the Organization?
4	Has the ship security alert system activation points been designed so as to prevent the inadvertent initiation of the ship security alert?	
Regulation 8/ Master's discretion for ship safety and security		
1	Has the master not been constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgement of the master, is necessary to maintain the safety and security of the ship?	
2	When a conflict between any safety and security requirements applicable to the ship arised during its operations, has the master given effect to those requirements necessary to maintain the safety of the ship?	
Regulation 9/ Control and compliance measures		
2.3	Does the ship shall keep records of the information referred to in paragraph 2.1 for the last 10 calls at port facilities?	

Requirements of		*Index for Questionnaire*
Part A	***Part B***	
Section 5/DECLARATION OF SECURITY		
A/5.7		Have DoSs been kept onboard the ship within the period specified by the Administration?
	B/5.4.1	Is the agreed DoS signed and dated by both the port facility and the ship?
	B/5.5	Is the agreed DoS completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships?
Section 6/OBLIGATIONS OF THE COMPANY		
A/6.1		Has the Company ensured that the ship security plan contains a clear statement emphasizing the master's authority?
A/6.1		Has the Company established in the ship security plan that the master has the 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?
A/6.2		Has the Company ensured that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this part of the Code?
	B/6.1	Has following information included?
	B/6.1.1	parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries, for example, retail sales outlets, casinos etc
	B/6.1.2	parties responsible for deciding the employment of the ship including, time or bareboat charterer(s) or any other entity acting in such capacity
	B/6.1.3	in cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers
Section 7/SHIP SECURITY		
A/7.1		Does the ship act upon the security levels set by Contracting Governments as set out in A/7.2?
A/7.2		At security level 1, have the following activities being carried out, through appropriate measures?
A/7.2.1		ensuring the performance of all ship security duties
A/7.2.2		controlling access to the ship
A/7.2.3		controlling the embarkation of persons and their effects
A/7.2.4		monitoring restricted areas to ensure that only authorized persons have access
A/7.2.5		monitoring of deck areas and areas surrounding the ship
A/7.2.6		supervising the handling of cargo and ship's stores
A/7.2.7		ensuring that security communication is readily available
A/7.3		At security level 2, have the additional protective measures, specified in the ship security plan, being implemented for each activity detailed in section 7.2?
A/7.4		At security level 3, have further specific protective measures, specified in the ship security plan, being implemented for each activity detailed in section 7.2?
Section 9/SHIP SECURITY PLAN		
A/9.1		Does the ship carry on board the approved Ship Security Plan?
A/9.7		Does the plan being protected from unauthorized access or disclosure?

Requirements of		*Index for Questionnaire*
Part A	***Part B***	
Section 10/RECORDS		
A/10.1		Does the records of the following activities addressed in the ship security plan being kept on board for at least the minimum period specified by the Administration?
A/10.1.1		training, drills and exercises
A/10.1.2		security threats and security incidents
A/10.1.3		breaches of security
A/10.1.4		changes in security level
A/10.1.5		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
A/10.1.6		internal audits and reviews of security activities
A/10.1.7		periodic review of the ship security assessment
A/10.1.8		periodic review of the ship security plan
A/10.1.9		implementation of any amendments to the plan
A/10.1.10		maintenance, calibration and testing of security equipment, if any including testing of the ship security alert system
A/10.2		Does the records being kept in the working language or languages of the ship? If the language or languages used are not English, French or Spanish, does a translation into one of these languages being included?
A/10.4		Does the records being protected from unauthorized access or disclosure?
Section 11/COMPANY SECURITY OFFICER		
A/11.1		Does the Company Security Officer designated for the ship?
Section 12/SHIP SECURITY OFFICER		
A/12.1		Does the Ship Security Officer designated on the ship?
Section 13/TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY		
A/13.2		Does the ship security officer have knowledge and have received training?
	B/13.1	Does the Ship Security Officer (SSO) have knowledge of, and receive training, in the following?
	B/13.1.1	security administration
	B/13.1.2	relevant international conventions, codes and recommendations
	B/13.1.3	relevant Government legislation and regulations
	B/13.1.4	responsibilities and functions of other security organisations
	B/13.1.5	methodology of ship security assessment
	B/13.1.6	methods of ship security surveys and inspections
	B/13.1.7	ship and port operations and conditions
	B/13.1.8	ship and port facility security measures
	B/13.1.9	emergency preparedness and response and contingency planning

Requirements of		*Index for Questionnaire*
Part A	***Part B***	
	B/13.1.10	instruction techniques for security training and education, including security measures and procedures
	B/13.1.11	handling sensitive security related information and security related communications
	B/13.1.12	knowledge of current security threats and patterns
	B/13.1.13	recognition and detection of weapons, dangerous substances and devices
	B/13.1.14	recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security
	B/13.1.15	techniques used to circumvent security measures
	B/13.1.16	security equipment and systems and their operational limitations
	B/13.1.17	methods of conducting audits, inspection, control and monitoring;
	B/13.1.18	methods of physical searches and non-intrusive inspections
	B/13.1.19	security drills and exercises, including drills and exercises with port facilities
	B/13.1.20	assessment of security drills and exercises
	B/13.2.1	the layout of the ship
	B/13.2.2	the ship security plan and related procedures (including scenario-based training on how to respond)
	B/13.2.3	crowd management and control techniques
	B/13.2.4	operations of security equipment and systems
	B/13.2.5	testing, calibration and whilst at sea maintenance of security equipment and systems
A/13.3	Does shipboard personnel having specific security duties and responsibilities understand their responsibilities for ship security as described in the ship security plan, and have sufficient knowledge and ability to perform their assigned duties?	
	B/13.3	Have shipboard personnel having specific security duties have sufficient knowledge and ability to perform their assigned duties, for following matters?
	B/13.3.1	knowledge of current security threats and patterns
	B/13.3.2	recognition and detection of weapons, dangerous substances and devices
	B/13.3.3	recognition of characteristics and behavioural patterns of persons who are likely to threaten security
	B/13.3.4	techniques used to circumvent security measures
	B/13.3.5	crowd management and control techniques
	B/13.3.6	security related communications
	B/13.3.7	knowledge of the emergency procedures and contingency plans
	B/13.3.8	operations of security equipment and systems
	B/13.3.9	testing, calibration and whilst at sea maintenance of security equipment and systems
	B/13.3.10	inspection, control, and monitoring techniques
	B/13.3.11	methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores
	B/13.4	Does All other shipboard personnel have sufficient knowledge of the following items and is familiar with relevant provisions of the SSP, if any?
	B/13.4.1	the meaning and the consequential requirements of the different security levels

Requirements of		*Index for Questionnaire*
Part A	***Part B***	
	B/13.4.2	knowledge of the emergency procedures and contingency plans
	B/13.4.3	recognition and detection of weapons, dangerous substances and devices
	B/13.4.4	recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security
	B/13.4.5	techniques used to circumvent security measures
A/13.4	Does the drills being carried out at appropriate intervals?	
	B/13.6	Does the drills being conducted at least once every three months?
	B/13.6	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, does the drill being conducted within one week of the change?
	B/13.6	Have the drills tested individual elements of the plan such as those security threats listed in paragraph 8.9?
A/13.5	Has the company security officer ensured the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals?	
	B/13.7	Have the exercises which include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as ship security officers, been carried out at least once each calendar year with no more than 18 months between the exercises?
	B/13.7	Have the exercises tested communications, coordination, resource availability, and response?
	B/13.8	Has the company participation in an exercise with another Contracting Government been recognised by the Administration?