PART B

Guidance regarding the provisions of chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended and part A of this Code

1 Introduction

General

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.

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.

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 paragraphs relating to port facilities. The same applies to those whose primary interest is port facilities; they should also read the paragraphs relating to ships.

1.4 The guidance provided in the following paragraphs 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 paragraphs.

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.

Responsibilities of Contracting Governments

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 (SSP) 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 (PFSO) who will be responsible for the preparation of the port facility security plan;

- ensuring completion and approval of the port facility security assessment (PFSA) and of any subsequent amendments to a previously approved assessment;

- approving the port facility security plan (PFSP) 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.

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 recognized security organizations 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 recognized security organizations. The following duties or activities cannot be 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 PFSO and to prepare a PFSP;

- approving a PFSA or any subsequent amendments to a previously approved assessment;

- approving a PFSP or any subsequent amendments to a previously approved plan;

- exercising control and compliance measures; and

- establishing the requirements for a Declaration of Security.

Setting the security level

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.

The Company and the ship

1.9 Any Company operating ships to which chapter XI-2 and part A of this Code apply has to designate a CSO for the Company and an SSO 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.

1.10 The company security officer's responsibilities include, in brief amongst others, ensuring that a ship security assessment (SSA) is properly carried out, that an SSP 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 CSO.

1.11 The SSP should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.

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, an SSP approved by, or on behalf of, the Administration. The CSO and SSO 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 into the approved plan and their implementation by the ship.

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.

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 SSP 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.

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.

The port facility

1.16 Each Contracting Government has to ensure completion of a PFSA 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 PFSA 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.

1.17 The PFSA 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 determination of the perceived threat to port installations and infrastructure;
- identification of the potential vulnerabilities; and
- calculation of the consequences of incidents.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk. The PFSA will help determine which port facilities are required to appoint a PFSO and prepare a PFSP.

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 PFSO. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.19 The PFSP 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.

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 PFSP approved by the Contracting Government or by the Designated Authority concerned. The PFSO 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 into 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 PFSA 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.

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.

Information and communication

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 security officer / ship security officers and the port facility security officers.

2 Definitions

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

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.

3 Application

General

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.

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.

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.

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.

4 Responsibility of Contracting Governments

Security of assessments and plans

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.

Designated Authorities

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.

Recognized security organizations

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.

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 an SSA or SSP or PFSA or PFSP. If an RSO has done so in respect of an SSA or SSP, that RSO should not be authorized to approve that SSP.

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 of 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 unauthorized 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 behavioural patterns of persons who are likely to threaten security;

.11 their knowledge of 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.

4.6 A recognized organization, as referred to 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.

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.

Setting the security level

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.

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.

4.10 At all times the master of a ship has the ultimate responsibility for the safety and security 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.

4.11 The CSO or the SSO should liaise at the earliest opportunity with the 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.

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.

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 the ship and to the 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.

Contact points and information on port facility security plans

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 CSOs and SSOs. 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 publicized. 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 recognized security organizations.

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.

4.16 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.

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

Identification documents

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.

Fixed and floating platforms and mobile offshore drilling units on location

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[*].

[*]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 2002 SOLAS Conference by resolution 7.

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

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 do 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.

Threats to ships and other incidents at Sea

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.

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.

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.

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.

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 PFSOs and SSOs

Alternative security agreements

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.

Equivalent arrangements for port facilities

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.

Manning level

4.28 In establishing the minimum safe manning of a ship, the Administration should take into account* that the minimum safe manning provisions established by regulation V/14** 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 SSP 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.

* Refer to Further work by the International Maritime Organisation pertaining to enhancement of maritime security, adopted by the 2002 SOLAS Conference 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.

** As was in force on the date of adoption of this Code.

Control and compliance measures*

* Refer to Further work by the International Maritime Organisation pertaining to enhancement of maritime security, adopted by the 2002 SOLAS Conference by resolution 3, inviting, amongst others, the Organisation to review Assembly resolutions A.787(19) and A.882(21) on Procedures for port State control.

General

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.

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 authorized 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*. 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 Load Line 66 as modified by the 1988 Load Line Protocol, articles 5 and 6 and regulation 8A of Annex I and 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).

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.

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.

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 holding 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 a 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.

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 persons, 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.

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.

Control of ships in port

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.

Ships intending to enter the port of another Contracting Government

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 10 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.

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 or of customs, immigration or 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 PFSP. 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.

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-2/5.

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.

Additional provisions

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 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.

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.

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.

4.44 The word "delay" in regulation XI-2/9.3.5.1 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.

Non-party ships and ships below Convention size

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*, 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.

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

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.

5 Declaration of Security

General

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.

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).

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 (SSA) and should be set out in the ship security plan (SSP).

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.

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 PFSO or SSO should acknowledge the request and discuss appropriate security measures.

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.

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.

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 relevant contact details.

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

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.

5.6 A model DoS is included in appendix 1 to this part of the Code. This model is for a DoS between a ship and a port facility. If the DoS is to cover two ships this model should be appropriately adjusted.

6 Obligations of the Company

General

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

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.

6.3 This information should be in English, French or Spanish language.

6.4 With respect to ships constructed before 1 July 2004, this information should reflect the actual condition on that date.

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.

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.

6.7 Previously provided information that does not relate to the actual condition on that date need not be retained on board.

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 is not required to be left on board.

In addition other relevant guidance is provided under sections 8, 9 and 13.

7 Ship security

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

8 Ship security assessment

Security assessment

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.

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.

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; and

.6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

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 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; and

.13 ship and port operations.

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/water-side 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.

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.

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.

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.

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.

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 watchkeeping 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.

8.11 The CSO and ship security officer (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.

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 countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

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.

On-scene security survey

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.

9 Ship security plan

General

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.

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 detail reporting procedures to the appropriate Contracting Government's contact points.

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.

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

9.5 CSOs and SSOs should develop procedures to:

.1 assess the continuing effectiveness of the SSP; and

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

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

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 update an inventory of any dangerous goods or hazardous substances carried on board, including their location.

9.8 The remainder of this section 9 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

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, sidescuttles, windows and ports;

.5 mooring lines and anchor chains; and

.6 cranes and hoisting gear.

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.

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 for 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.

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 SSO, the CSO, the PFSO and to the national or local authorities with security responsibilities.

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

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 persons, 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.

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

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 unauthorized access;

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

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

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

the port facility;

.5 increasing the frequency and detail of searches of persons, 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

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

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 unauthorized access;

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

.3 protect sensitive-security areas within the ship; and

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

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

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

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

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

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

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

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.

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

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.

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.

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

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.

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

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

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.

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

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

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

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

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

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%, which may include use of x-ray screening.

Security level 2

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% x-ray screening of all unaccompanied baggage.

Security level 3

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

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 watchkeepers, security guards and deck watches, including patrols; and

.3 automatic intrusion-detection devices and surveillance equipment.

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.

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

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.

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 co-ordination with the port facility.

Security level 2

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 look-outs; and

.4 ensuring co-ordination with water-side boat patrols, and foot or vehicle patrols on the shore side, when provided.

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 co-ordinating with the port facility to provide additional shoreside lighting.

Security level 3

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.

Differing security levels

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

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*;

.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.

[*] Refer to Further work by the International Maritime Organisation pertaining to enhancement of maritime security and to Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling unit on location and fixed and floating platforms not covered by chapter XI-2 of the 1974 SOLAS Convention, adopted by the 2002 SOLAS Conference by resolution 3 and 7 respectively.

Declarations of Security

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

Audit and review

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.

10 Records

General

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.

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

11 Company security officer

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

12 Ship security officer

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

13 Training, drills and exercises on ship security

Training

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.

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 (SSP) 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 at-sea maintenance of security equipment and systems.

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 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.

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.

Drills and exercises

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.

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% 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.

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, co-ordination, 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.

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

14 Port facility security

Relevant guidance is provided under section 15, 16 and 18.

15 Port facility security assessment

General

15.1 The port facility security assessment (PFSA) may be conducted by a recognized security organization (RSO). However, approval of a completed PFSA should only be given by the relevant Contracting Government.

15.2 If a Contracting Government uses a RSO to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.

15.3 A PFSA should address the following elements within a port facility:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks;

.6 relevant transportation infrastructure;

.7 utilities; and

.8 other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the port facility.

15.4 Those involved in a PFSA 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 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 structures and port facility services;

.7 port facility security;

.8 port business practices;

.9 contingency planning, emergency preparedness and response;

.10 physical security measures, e.g., fences;

.11 radio and telecommunications systems, including computer systems and networks;

.12 transport and civil engineering; and

.13 ship and port operations.

Identification and evaluation of important assets and infrastructure it is important to protect

15.5 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port

facility can be established. This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident. This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

15.6 Identification and evaluation of assets and infrastructure should be used to prioritise their relative importance for protection. The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid re-establishment of normal functioning is possible.

15.7 Assets and infrastructure that should be considered important to protect may include:

.1 accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;

.2 cargo facilities, terminals, storage areas, and cargo handling equipment;

.3 systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;

.4 port vessel traffic management systems and aids to navigation;

.5 power plants, cargo transfer piping, and water supplies;

.6 bridges, railways, roads;

.7 port service vessels, including pilot boats, tugs, lighters etc;

.8 security and surveillance equipment and systems; and

.9 the waters adjacent to the port facility.

15.8 The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritisation of protective measures, and decisions concerning the allocation of resources to better protect the port facility. The process may involve consultation with the

relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures

15.9 Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security requirements to enable planning and resource allocations. Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies. By identifying and assessing threats, those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.

15.10 The PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:

.1 any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack;

.2 the likely consequences in terms of loss of life, damage to property and economic disruption, including disruption to transport systems, of an attack on, or at, the port facility;

.3 the capability and intent of those likely to mount such an attack; and

.4 the possible type, or types, of attack.

producing an overall assessment of the level of risk against which security measures have to be developed.

15.11 The PFSA should consider all possible threats, which may include the following types of security incidents:

.1 damage to, or destruction of, the port facility or of the ship, 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 their equipment;

.7 use of the ship itself as a weapon or as a means to cause damage or destruction;

.8 blockage of port entrances, locks, approaches, etc.; and

.9 nuclear, biological and chemical attack.

15.12 The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification, selection, and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability

15.13 The identification and prioritization of countermeasures is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship/port interface to the possible threats.

15.14 Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

.1 security surveys, inspections and audits;

.2 consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;

.3 historical information on security incidents; and

.4 operations within the port facility.

Identification of vulnerabilities

15.15 Identification of vulnerabilities in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges, etc. that could be resolved through physical measures, e.g., permanent barriers, alarms, surveillance equipment etc.

15.16 Identification of vulnerabilities should include consideration of:

.1 water-side and shore-side access to the port facility and ships berthing at the facility;

.2 structural integrity of the piers, facilities, and associated structures;

.3 existing security measures and procedures, including identification systems;

.4 existing security measures and procedures relating to port services and utilities;

.5 measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;

.6 adjacent areas that may be exploited during, or for, an attack;

.7 existing agreements with private security companies providing water-side/shore- side security services;

.8 any conflicting policies between safety and security measures and procedures;

.9 any conflicting port facility and security duty assignments;

.10 any enforcement and personnel constraints;

.11 any deficiencies identified during training and drills; and

.12 any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

16 Port facility security plan

General

16.1 Preparation of the port facility security plan (PFSP) is the responsibility of the port facility security officer (PFSO). While the PFSO 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 PFSO.

16.2 The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers. The port facility security assessment (PFSA) will have identified the particular features of the port facility, and of the potential security risks, that have led to the need to appoint a PFSO and to prepare a PFSP. The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in the PFSP and for appropriate security measures to be established so as to minimise the likelihood of a breach of security and the consequences of potential risks. Contracting Governments may prepare advice on the preparation and content of a PFSP.

16.3 All PFSPs should:

.1 detail the security organisation of the port facility,

.2 detail the organization's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port;

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

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

.5 provide for regular review, or audit, of the PFSP and for its amendments in response to experience or changing circumstances; and

.6 detail reporting procedures to the appropriate Contracting Government's contact points.

16.4 Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.

16.5 Contracting Government should approve the PFSPs of the port facilities under their jurisdiction. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The PFSP should make provision for the retention of records of

security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

16.6 The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each measure will be in place. If there is likely to be any delay in their provision, this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

16.7 The use of firearms on or near ships and in port facilities may pose particular and significant safety risks, in particular in connection with certain dangerous or hazardous substances, and should be considered very carefully. In the event that a Contracting Government decides that it is necessary to use armed personnel in these areas, that Contracting Government should ensure that these personnel are duly authorized and trained in the use of their weapons and that they are aware of the specific risks to safety that are present in these areas. If a Contracting Government authorizes the use of firearms they should issue specific safety guidelines on their use. The PFSP should contain specific guidance on this matter, in particular with regard to its application to ships carrying dangerous goods or hazardous substances.

Organization and performance of port facility security duties

16.8 In addition to the guidance given under paragraph 16.3, the PFSP should establish the following, which relate to all security levels:

.1 the role and structure of the port facility security organisation;

.2 the duties, responsibilities and training requirements of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;

.3 the port facility security organization's links with other national or local authorities with security responsibilities;

.4 the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;

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

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

.7 the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;

.8 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;

.9 procedures relating to cargo handling;

.10 procedures covering the delivery of ship's stores;

.11 the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility;

.12 the means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches;

.13 the procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested; and

.14 the procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organisations.

16.9 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:

.1 Access to the port facility;

.2 restricted areas within the port facility;

.3 handling of cargo;

.4 delivery of ship's stores;

.5 handling unaccompanied baggage; and

.6 monitoring the security of the port facility.

Access to the port facility

16.10 The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA.

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

16.12 The PFSP should establish for each security level the means of identification required to allow access to the port facility and for individuals to remain within the port facility without challenge. This may involve developing an appropriate identification system, allowing for permanent and temporary identifications for port facility personnel and for visitors respectively. Any port facility identification system should, when it is practicable to do so, be co-ordinated with that applying to ships that regularly use 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 PFSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

16.13 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 port facility and their attempt to obtain access should be reported to the PFSO and to the national or local authorities with security responsibilities.

16.14 The PFSP should identify the locations where persons, personal effects, and vehicle searches are to be undertaken. Such locations should be covered to facilitate continuous operation, regardless of prevailing weather conditions, in accordance with the frequency laid down in the PFSP. Once

subjected to search, persons, personal effects and vehicles should proceed directly to the restricted holding, embarkation or car loading areas.

16.15 The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking passengers, ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons.

16.16 The PFSP 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

16.17 At security level 1, the PFSP should establish the control points where the following security measures may be applied:

.1 restricted areas, which should be bounded by fencing or other barriers to a standard which should be approved by the Contracting Government;

.2 checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors, and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc;

.3 checking vehicles used by those seeking entry to the port facility in connection with a ship;

.4 verification of the identity of port facility personnel and those employed within the port facility and their vehicles;

.5 restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity;

.6 undertaking searches of persons, personal effects, vehicles and their contents; and

.7 identification of any access points not in regular use, which should be permanently closed and locked.

16.18 At security level 1, all those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the approved PFSP and should be specifically approved by the Contracting Government. 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

16.19 At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

.1 assigning additional personnel to guard access points and patrol perimeter barriers;

.2 limiting the number of access points to the port facility, and identify those to be closed and the means of adequately securing them;

.3 providing for means of impeding movement through the remaining access points, e.g., security barriers;

.4 increasing the frequency of searches of persons, personal effects, and vehicle;

.5 denying access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and

.6 using patrol vessels to enhance water-side security.

Security level 3

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

.1 suspension of access to all, or part of, the port facility;

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

.3 suspension of pedestrian or vehicular movement within all, or part, of the port facility;

.4 increased security patrols within the port facility, if appropriate;

.5 suspension of port operations within all, or part, of the port facility;

.6 direction of vessel movements relating to all, or part, of the port facility; and

.7 evacuation of all, or part of, the port facility.

Restricted areas within the port facility

16.21 The PFSP should identify the restricted areas to be established within the port facility and 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. This should also include, in appropriate circumstances, measures to ensure that temporary restricted areas are security swept both before and after that area is established. The purpose of restricted areas is to:

.1 protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;

.2 protect the port facility;

.3 protect ships using, and serving, the port facility;

.4 protect security-sensitive locations and areas within the port facility,

.5 protect security and surveillance equipment and systems; and

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

16.22 The PFSP should ensure that all restricted areas have clearly established security measures to control:

.1 access by individuals;

.2 the entry, parking, loading and unloading of vehicles;

.3 movement and storage of cargo and ship's stores, and

.4 unaccompanied baggage or personal effects.

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

16.24 When automatic intrusion-detection devices are installed they should alert a control centre which can respond to the triggering of an alarm.

16.25 Restricted areas may include:

.1 shore- and water-side areas immediately adjacent to the ship;

.2 embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas, including search points;

.3 areas where loading, unloading or storage of cargo and stores is undertaken;

.4 locations where security-sensitive information, including cargo documentation, is held;

.5 areas where dangerous goods and hazardous substances are held;

.6 vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;

.7 areas where security and surveillance equipment are stored or located;

.8 essential electrical, radio and telecommunication, water and other utility installations; and

.9 other locations in the port facility where access by vessels, vehicles and individuals should be restricted.

16.26 The security measures may extend, with the agreement of the relevant authorities, to restrictions on unauthorized access to structures from which the port facility can be observed.

Security level 1

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

.1 provision of permanent or temporary barriers to surround the restricted area, whose standard should be accepted by the Contracting Government;

.2 provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;

.3 providing passes which must be displayed to identify individual's entitlement to be within the restricted area;

.4 clearly marking vehicles allowed access to restricted areas;

.5 providing guards and patrols;

.6 providing automatic intrusion-detection devices, or surveillance equipment or systems to detect unauthorized access into, or movement within, restricted areas; and

.7 control of the movement of vessels in the vicinity of ships using the port facility.

Security level 2

16.28 At security level 2, the PFSP should establish the enhancement of the frequency and intensity of the monitoring of, and control of access to, restricted areas. The PFSP should establish the additional security measures, which may include:

.1 enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion-detection devices;

.2 reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;

.3 restrictions on parking adjacent to berthed ships;

.4 further restricting access to the restricted areas and movements and storage within them;

.5 use of continuously monitored and recording surveillance equipment;

.6 enhancing the number and frequency of patrols, including water-side patrols, undertaken on the boundaries of the restricted areas and within the areas;

.7 establishing and restricting access to areas adjacent to the restricted areas; and

.8 enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility.

Security level 3

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

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

.2 preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.

Handling of cargo

16.30 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 within the port facility.

16.31 The security measures should include inventory control procedures at access points to the port facility. Once within the port facility, cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

Security level 1

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

.1 routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;

.2 checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;

.3 searches of vehicles; and

.4 checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

16.33 Checking of cargo may be accomplished by some or all of the following means:

.1 visual and physical examination; and

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

16.34 When there are regular or repeated cargo movements, the CSO or the 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 concern.

Security level 2

16.35 At security level 2, the PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include:

.1 detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;

.2 intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship;

.3 intensified searches of vehicles; and

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

16.36 Detailed checking of cargo may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (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 addition to an established agreement and procedures.

Security level 3

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

.1 restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and

.2 verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.

Delivery of ship's stores

16.38 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;

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

.5 ensure searching the delivery vehicle; and

.6 ensure escorting delivery vehicles within the port facility.

16.39 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

16.40 At security level 1, the PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include:

.1 checking of ship's stores;

.2 advance notification as to composition of load, driver details and vehicle registration; and

.3 searching the delivery vehicle.

16.41 Checking of ship's stores may be accomplished by some or all of the following means:

.1 visual and physical examination; and

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

Security level 2

16.42 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ship's stores, which may include:

.1 detailed checking of ship's stores;

.2 detailed searches of the delivery vehicles;

.3 co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; and

.4 escorting the delivery vehicle within the port facility.

16.43 Detailed checking of ship's stores may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of searches of delivery vehicles;

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

.3 restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period.

Security level 3

16.44 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include preparation for restriction, or suspension, of the delivery of ship's stores within all, or part, of the port facility.

Handling unaccompanied baggage

16.45 The PFSP 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 allowed in the port facility and, depending on the storage arrangements, before it is transferred between the port facility and the ship. It is not envisaged that such baggage will be subjected to screening by both the port facility and the ship, and in cases where

both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the ship is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security level 1

16.46 At security level 1, the PFSP 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%, which may include use of x-ray screening.

Security level 2

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

Security level 3

16.48 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility in close co-operation with those responding and the ships at 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 preparations for restriction or suspension of handling or unaccompanied baggage; and

.3 refusal to accept unaccompanied baggage into the port facility.

Monitoring the security of the port facility

16.49 The port facility security organization should have the capability to monitor the port facility and its nearby approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:

.1 lighting;

.2 security guards, including foot, vehicle and waterborne patrols, and

.3 automatic intrusion-detection devices and surveillance equipment.

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

16.51 The PFSP 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 or of power disruptions.

Security level 1

16.52 At security level 1, the PFSP should establish the security measures to be applied, which may be a combination of lighting, security guards or use of security and surveillance equipment to allow

port facility security personnel to:

.1 observe the general port facility area, including shore- and water-side accesses to it;

.2 observe access points, barriers and restricted areas, and

.3 allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself.

Security level 2

16.53 At security level 2, the PFSP should establish the additional security measures to be applied, to enhance the monitoring and surveillance capability, which may include:

.1 increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage;

.2 increasing the frequency of foot, vehicle or waterborne patrols, and

.3 assigning additional security personnel to monitor and patrol.

Security level 3

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

.1 switching on all lighting within, or illuminating the vicinity of, the port facility;

.2 switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and

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

Differing security levels

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

Activities not covered by the Code

16.56 The PFSP should establish details of the procedures and security measures the port facility should apply when:

.1 it is interfacing with a ship which has been at a port of a State which not a Contracting Government;

.2 it is interfacing with a ship to which this Code does not apply; and

.3 it is interfacing with fixed or floating platforms or mobile offshore drilling units on location.

Declarations of Security

16.57 The PFSP should establish the procedures to be followed when, on the instructions of the Contracting Government, the PFSO requests a DoS or when a DoS is requested by a ship.

Audit, review and amendment

16.58 The PFSP should establish how the PFSO intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP.

16.59 The PFSP should be reviewed at the discretion of the PFSO. In addition it should be reviewed:

.1 if the PFSA relating to the port facility is altered;

.2 if an independent audit of the PFSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant elements of the approved PFSP;

.3 following security incidents or threats thereof involving the port facility; and

.4 following changes in ownership or operational control of the port facility.

16.60 The PFSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the PFSP relating to:

.1 proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; and

.2 the removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems, etc., previously considered essential in maintaining the security of the port facility

should be submitted to the Contracting Government that approved the original PFSP for their consideration and approval. Such approval can be given by, or on behalf of, the Contracting Government with, or without, amendments to the proposed changes. On approval of the PFSP, the Contracting Government should indicate which procedural or physical alterations have to be submitted to it for approval.

Approval of port facility security plans

16.61 PFSPs have to be approved by the relevant Contracting Government, which should establish appropriate procedures to provide for:

.1 the submission of PFSPs to them;

.2 the consideration of PFSPs;

.3 the approval of PFSPs, with or without amendments;

.4 consideration of amendments submitted after approval, and

.5 procedures for inspecting or auditing the continuing relevance of the approved PFSP.

At all stages, steps should be taken to ensure that the contents of the PFSP remains confidential.

Statement of Compliance of a Port Facility

16.62 The Contracting Government within whose territory a port facility is located may issue an appropriate Statement of Compliance of a Port Facility (SoCPF) indicating:

.1 the port facility;

.2 that the port facility complies with the provisions of chapter XI-2 and part A of the Code;

.3 the period of validity of the SoCPF, which should be specified by the Contracting Governments but should not exceed five years; and

.4 the subsequent verification arrangements established by the Contracting Government and a confirmation when these are carried out.

16.63 The Statement of Compliance of a Port Facility should be in form set out in the appendix to this part of the Code. If the language used is not Spanish, French or English, the Contracting Government, if it considers it appropriate, may also include a translation into one of these languages.

17 Port facility security officer

General

17.1 In those exceptional instances where the ship security officer has questions about the validity of identification documents of those seeking to board the ship for official purposes, the port facility security officer should assist.

17.2 The port facility security officer should not be responsible for routine confirmation of the identity of those seeking to board the ship.

In addition relevant guidance is provided under sections 15, 16 and 18.

18 Training, drills and exercises on port facility security

Training

18.1 The port facility security officer should have knowledge 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 port facility security assessment;

.6 methods of ship and port facility 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 the 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 ships; and

.20 assessment of security drills and exercises.

18.2 Port facility personnel having specific security duties should have knowledge and receive training in some or all of the following, 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 operations of security equipment and systems;

.8 testing, calibration and maintenance of security equipment and systems,

.9 inspection, control, and monitoring techniques; and

.10 methods of physical searches of persons, personal effects, baggage, cargo, and ship’s stores.

18.3 All other port facility personnel should have knowledge of and be familiar with relevant provisions of the PFSP in some or all of the following, as appropriate:

.1 the meaning and the consequential requirements of the different security levels;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and

.4 techniques used to circumvent security measures.

Drills and exercises

18.4 The objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties, at all security levels, and to identify any security-related deficiencies which need to be addressed.

18.5 To ensure the effective implementation of the provisions of the port facility security plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as those security threats listed in paragraph 15.11.

18.6 Various types of exercises, which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, company security officers, or ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of company security officers or ships security officers in joint exercise should be made, bearing in mind the security and work implications for the ship. These exercises should test communication, co-ordination, 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 emergency response or other port State authority exercises.

19 Verification and certification for ships

No additional guidance.

Appendix to part B

Appendix 1
Form of a Declaration of Security between a ship and a port facility*

DECLARATION OF SECURITY

Name of Ship: ....

Port of Registry: ....

IMO Number: ....

Name of Port Facility: ....

This Declaration of Security is valid from ……..…..…..... until ……...….…..... for the following activities

....
(list the activities with relevant details)

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Date at ……..……on the…….……

Signed for and on behalf of

the port facility:	the ship:
……...……	……...……
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*

Name and title of person who signed

Name: ……...……	Name: ……...……
Title: ……...……	Title: ……...……

Contact Details

(to be completed as appropriate)
(indicate the telephone numbers or the radio channels or frequencies to be used)

for the port facility:	for the ship:
Port Facility	Master
……...……	……...……
Port Facility Security Officer	Ship Security Officer
……...……	……...……
	Company
	……...……
	Company Security Officer
	……...……

[*] This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two ships this model should be appropriately modified.

Appendix 2

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

(Official seal) *(State)*

Statement Number

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

The Government of……..……..…….
(name of the State)

Name of the Port Facility ……..……..…….
Address of the Port Facility ……..……..…….

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Port Facility Security Plan. This plan has been approved for the following <specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):

Passenger ship
Passenger high speed craft
Cargo high speed craft
Bulk carrier
Oil tanker
Chemical tanker
Gas carrier
Mobile offshore Drilling Units
Cargo ships other than those referred to above

This Statement of Compliance is valid until ....., subject to verifications (as indicated overleaf)

Issued at..... .....
(place of issue of the statement)

Date of issue..... .....
(Signature of the duly authorized official issuing the document)

(Seal or stamp of issuing authority, as appropriate)

Endorsement for verifications

The Government of <*insert name of the State*> has established that the validity of this Statement of Compliance is subject to <*insert relevant details of the verifications (e.g. mandatory annual or unscheduled)*>.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

First verification

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

(Seal or stamp of authority, as appropriate)

Second verification

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

(Seal or stamp of authority, as appropriate)

Third verification

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

(Seal or stamp of authority, as appropriate)

Fourth verification

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

(Seal or stamp of authority, as appropriate)