GUIDANCE FOR OIL TERMINAL OPERATORS ON THE INTERNATIONAL MARITIME ORGANIZATION (IMO) INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

FIRST EDITION ~ DECEMBER 2003

The OCIMF mission is to be recognised internationally as the foremost authority on the safe and environmentally responsible operation of oil tankers and terminals.

Issued by the
Oil Companies International Marine Forum
(OCIMF)
First Edition ~ December 2003

The Oil Companies International Marine Forum (OCIMF) is a voluntary association of oil companies having an interest in the shipment and terminalling of crude oil and oil products. OCIMF is organised to represent its membership before, and consult with, the International Maritime Organization (IMO) and other government bodies on matters relating to the shipment and terminalling of crude oil and oil products, including marine pollution and safety.

Guidance for Oil Terminal Operators on the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code

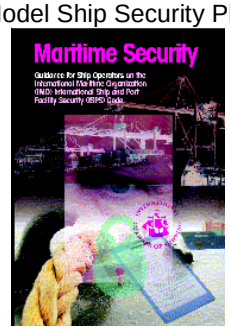
Contents

Preface

Introduction:

During internal reviews at OCIMF Committees and Forums of the SOLAS Amendments and ISPS Code measures to enhance maritime security, it was self evident that practical guidance to aid implementation was necessary especially with the intended fast-track entry into force schedule.

Various guides and recommendations have been produced by a number of authoritative sources to assist those impacted by the scope of the regime, in particular with respect to shipping and shipboard operations. A good example of this is two publications produced by, and obtainable from, the International Chamber of Shipping (ICS) entitled “Guidance for Ship Operators on the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code” and the “Model Ship Security Plan”.



Unfortunately, however, it was also apparent from the OCIMF membership that there is a shortage of similar information focussing upon the port facility and marine terminal operations, and this was compounded by a lack of familiarity of the IMO regulatory processes by those facilities now falling into the scope of SOLAS.

The primary purpose of this guide is to provide marine terminal operators with information, which it is anticipated will aid interpretation and implementation of the requirements for port facilities. These are contained in two parts;

- A consolidated copy of the requirements of the ISPS Code (Parts ‘A’ & ‘B’) relating specifically to the port facility, reorganised into a topical format.
- Secondly, an example model of a port facility security plan.

It is envisaged that these two elements will further assist the port facility operator in understanding the current requirements. It should be noted however that this guidance has been released as quickly as possible to provide port facilities with early advice. It is fully anticipated that we will benefit further from the experience of others as we progress towards entry into force and we will endeavour to provide updates to this guide as and when appropriate.

Acknowledgements:

In developing this document OCIMF has, with kind permission, reproduced text provided by the International Maritime Organization (IMO) and The National Coastal Administration of Norway for which OCIMF is extremely grateful as, without this cooperation, production of the guide would have been significantly delayed.

OCIMF also wishes to stress that this document compliments and **DOES NOT** replace the need to comply strictly with the requirements of the IMO SOLAS and ISPS Code Measures to Enhance Maritime Security and the requirements of any international or national legislation. Although much of the enclosed text derives from SOLAS and the ISPS Code, copies of the IMO publication ISPS Code 2003 Edition (Product Code: I116E) **MUST** be purchased by those required to comply with the IMO requirements and can be obtained from the IMO (or recognised stockists) at www.imo.org and following the menu to the Publications Section. The ISPS Code is available in various languages as well as “virtual” downloads.

Background Section 1

The IMO International Ship and Port Facility Security Code (ISPS Code)

At the IMO Diplomatic conference In December 2002, the International Convention for Safety of Life at Sea (SOLAS), 1974, was amended. The existing Chapter XI of SOLAS was re-identified as Chapter XI-1 and a new Chapter XI-2 was adopted to enhance maritime security. Part 'A' of this code is mandatory from 1st July 2004 with Part 'B' serving as guidance for implementation and application.

It should be noted that a significant number of sections in Part 'A' contain the statement - taking into account of the guidance given in Part 'B'. Also section 3.1 of Part 'B' states – 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.

The Objectives of the Code:

- To establish co-operation between Contacting Governments, Government Agencies, Local Authorities, Shipping and Port Industries to assess/detect security threats and take preventative measures against security incidents affecting shipping or port facilities used in international trade.
- Establish the respective roles and responsibilities of all parties concerned, at national and international level, for ensuring maritime security.
- To ensure early and efficient collation and exchange of security related information.
- To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels.
- To ensure confidence that adequate and proportionate maritime security measures are in place.

The Code Applies to Oil Facilities

- Port facilities serving cargo ships, including high-speed craft, of 500 gross tonnage and upwards; Mobile offshore drilling units; and such ships engaged on international voyages.

Note: For the purposes of SOLAS, a cargo ship is any ship which is not a passenger ship, and a tanker is a cargo ship constructed or adapted for the carriage in bulk of liquid cargoes of a flammable nature.

Contracting Governments will base their decisions on a port facility security assessment carried out in accordance with the Code. The Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

Application

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

- gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
- requiring the maintenance of communication protocols for ships and port facilities;
- preventing unauthorized access to ships, port facilities and their restricted areas;
- preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;
- providing means for raising the alarm in reaction to security threats or security incidents;
- requiring ship and port facility security plans based upon security assessments;
- requiring training, drills and exercises to ensure familiarity with security plans and procedures.

Master of a Ship

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. B4.10

Definitions Section 2

All Ships, when used in this chapter, means any ship to which this chapter applies.

Bulk Carrier means a bulk carrier as defined in Regulation IX/1.6.

Chemical Tanker means a chemical tanker as defined in Regulation VII/8.2.

Chapter means a chapter of the convention.

Company means a Company as defined in Regulation IX/1.

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

Contracting Government, when used in regulations 3,4, 7 and 10 to 13, includes a reference to the Designated Authority.

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

Declaration of Security (DoS) means an agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement.

Designated Authority means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this Chapter (XI-2) pertaining to port facility security and ship/port interface, from the point of view of the port facility.

Gas Carrier means a gas carrier as defined in Regulation VII/11.2.

High-Speed Craft means a craft as defined in Regulation X/1.2.

International Ship and Port Facility Security (ISPS) Code means the International Code for the Security of Ships and of Port Facilities consisting of Part 'A' (the provisions of which shall be treated as mandatory) and Part 'B' (the provisions of which shall be treated as recommendatory), as adopted, 12th December 2002, by the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974.

Mobile Offshore Drilling Unit (MoDU) means a mechanically propelled mobile offshore drilling unit, as defined in Regulation IX/1, not on location.

Oil Tanker means an oil tanker as defined in Regulation II-1/2.12.

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

Port Facility Security Officer or (PFSO) means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

Port Facility Security Plan or (PFSP) means a plan developed to ensure the application of measures designed to protect the port facility, ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

Recognized Security Organization or (RSO) means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by this chapter or by Part 'A' of the ISPS Code.

Regulation means a regulation of the Convention.

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

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

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

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

Security Level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Ship, when used in Regulations 3 to 13, includes mobile offshore drilling units and high-speed craft.

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

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

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

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

Security Levels Section 3

A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, the ship, ship's personnel, ship's visitors, goods and services. A14.1

The port facility security plan (PFSP) shall make provisions for the three security levels, as defined in the Part 'A' of the Code (*American Home Land Security Advisory System (HSAS) levels are indicated for comparison):* A16.1

Level 1 Normal *HSAS Green (Low), Blue (Guarded), Yellow (Elevated)*

The level for which minimum appropriate protective security measures shall be maintained at all times. A2.1.9

The following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in Part 'B' of this Code, in order to identify and take preventive measures against security incidents:

- ensuring the performance of all port facility security duties;
- controlling access to the port facility;
- monitoring of the port facility, including anchoring and berthing area(s);
- monitoring restricted areas to ensure that only authorized persons have access;
- supervising the handling of cargo;
- supervising the handling of ship's stores; and
- ensuring that security communication is readily available. A14.2

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. B16.31

Level 2 Heightened *HSAS Orange (High)*

The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident. A2.1.10

At security level 2, additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section A14.2, taking into account the guidance given in Part 'B' of the Code. A14.3

Level 3 Exceptional *HSAS Red (Incident Imminent)*

The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target. A2.1.11

Further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in Part 'B' of the Code. A14.4

At security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located. A14.4.1

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.

While the security levels may change from security level I, through security level 2 to security level 3, it is also possible that security levels will change directly from Security level 1 to security level 3. B4.9

Responsibilities of Contracting Governments

Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

- the degree that the threat information is credible;
- the degree that the threat information is corroborated;
- the degree that the threat information is specific or imminent; and
- the potential consequences of such a security incident. A4.1

In setting the security level, Contracting Governments should take account of general and specific threat information and set the security level applying to ships or port facilities at one of three levels. Higher security levels indicate greater likelihood of occurrence of a security incident. B4.8

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. B4.9

Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security-related information to the ships and port facilities that may be affected. A4.2

Contracting Governments should establish means of notifying PFSO's 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. A4.13

Organization and Performance of Port Facility Security Duties

Section B16.8 to B16.54 of the ISPS Code addresses specifically the security measures that could be taken at each security level covering:

- access to the port facility;
- restricted areas within the port facility;
- handling of cargo;
- delivery of ship's stores;
- handling unaccompanied baggage;
- monitoring the security of the port facility. **B16.9**

A summary of the activities for each security level under the above headings is given in attachment 'B' to this guide. Other details can be found in section 5 of this guide under - Port Facilities Security Plan.

Port Facilities Security Assessment (PFSA) Section 4

Each Contracting Government has to ensure completion of a Port Facilities Security Assessment (PFSA) for each of the port facilities, located within its territory, serving ships engaged on international voyages of 500 gross tons and upward including high speed craft. The PFSA is also an essential and integral part of the process of initially developing and updating the port facility security plan. The Contracting Government a Designated Authority within the Government or a delegated Recognized Security Organization will carry out this assessment. A15.1 A15.2 B1.16

Recognised Security Organizations (RSO)

When the port facility security assessment has been carried out by a recognised security organization, the security assessment shall be reviewed and approved for compliance of the Code by the Contracting Government within whose territory the port facility is located. A15.2.1

Persons carrying out PFSA's

The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with Part 'A' of the ISPS Code.

Those involved in a PFSA should be able to draw upon expert assistance in relation to:

- knowledge of current security threats and patterns;
- recognition and detection of weapons, dangerous substances and devices;
- recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- techniques used to circumvent security measures;
- methods used to cause a security incident;
- effects of explosives on structures and port facility services;
- port facility security;
- port business practices;
- contingency planning, emergency preparedness and response;
- physical security measures, e.g. fences;
- radio and telecommunications systems, including computer systems and networks;
- transport and civil engineering;
- ship and port operations. A15.3 B15.4

PFSA - Minimum Content

The Port Facility Security Assessment must include, at least, the following elements:

- Identification and evaluation of important assets and infrastructure it is important to protect;
- identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;
- identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability;
- identification of weaknesses, including human factors, in the infrastructure, policies and procedures. A15.5

Elements

The Port Facility Security Assessment should address the following elements within a port facility:

- physical security;
- structural integrity;
- personnel protection systems;
- procedural policies;
- radio and telecommunication systems, including computer systems and networks;
- relevant transportation infrastructure;
- utilities;
- other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility. B15.3

Risk Assessment.

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;
- calculation of the consequences of incidents calculated. B1.17

Identification and Evaluation of Assets and Infrastructure.

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 and used to prioritise their relative importance for protection. 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. B15.5 B15.6

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

- accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- cargo facilities, terminals, storage areas, and cargo handling equipment;
- systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
- port vessel traffic management systems and aids to navigation;
- power plants, cargo transfer piping, and water supplies;
- bridges, railways, roads;
- port service vessels, including pilot boats, tugs, lighters, etc.;
- security and surveillance equipment and systems;
- the waters adjacent to the port facility. B15.7

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 used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention. B15.8

Identification of the Possible Threats to the Assets and Infrastructure.

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. B15.9

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

- 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;
- 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;
- the capability and intent of those likely to mount such an attack;
- the possible type, or types, of attack, producing an overall assessment of the level of risk against which security measures have to be developed. B15.10

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

- damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the ship or of persons on board;
- tampering with cargo, essential ship equipment or systems or ship's stores;
- unauthorized access or use, including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the ship to carry those intending to cause a security incident and their equipment;
- use of the ship itself as a weapon or as a means to cause damage or destruction;
- blockage of port entrances, locks, approaches, etc.;
- nuclear, biological and chemical attack. B15.11

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. B15.12

Identification of Countermeasures

The identification and prioritisation 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. 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:

- security surveys, inspections and audits;
- consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;
- historical information on security incidents;
- operations within the port facility. B15.13 B15.14

Identification of Vulnerabilities

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. B15.15

Identification of vulnerabilities should include consideration of:

- water-side and shore-side access to the port facility and ships berthing at the facility;
- structural integrity of the piers, facilities, and associated structures;
- existing security measures and procedures, including identification systems;
- existing security measures and procedures relating to port services and utilities;
- measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;
- adjacent areas that may be exploited during, or for, an attack;
- existing agreements with private security companies providing water-side/shore-side security services;
- any conflicting policies between safety and security measures and procedures;
- any conflicting port facility and security duty assignments;
- any enforcement and personnel constraints;
- any deficiencies identified during training and drills; and
- any deficiencies identified during daily operation, following incidents or alerts,
- the report of security concerns, the exercise of control measures, audits, etc. B15.16

Completion Report

Upon completion of the PFSA, 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. A15.7

Review

The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility, and shall always be reviewed and updated when major changes to the port facility take place. A15.4

Similar Ports

The Contracting Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. A15.6

Port Facility Security Plan (PFSP) Section 5

A port facility security plan shall be developed and maintained, on the basis of a PFSA for each port facility, adequate for the ship/port interface. Such a plan shall be developed taking into account the guidance given in Part 'B' of the Code and shall be in the working language of the port facility. A16.1

The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers. The 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 Port Facility Security Officer (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 in order to minimize 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. B16.2

Preparation of the Port Facility Security Plan

Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the 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.

B16.1

Approval of Port Facility Security Plans

PFSP's have to be approved by the relevant Contracting Government, which should establish appropriate procedures to provide for:

- the submission of PFSP's to them;
- the consideration of PFSP's;
- the approval of PFSP's, with or without amendments;
- consideration of amendments submitted after approval; and
- 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 remain confidential. B16.61

Recognised Security Organisation (RSO)

A recognized security organization may prepare the PFSP of a specific port facility. However, as mentioned above, the PFSP must be approved by the Contracting Government in whose territory the port facility is located. A16.1.1 A16.2

Minimum Content

The plan shall address, at least, the following:

- measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports, and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;
- measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;
- procedures for responding to any security instructions the Contracting Government in whose territory the port facility is located may give at security level 3;
- procedures for evacuation in case of security threats or breaches of security;
- duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;
- procedures for interfacing with ship security activities;
- procedures for the periodic review of the plan and updating;
- procedures for reporting security incidents;
- identification of the port facility security officer, including 24-hour contact details;
- measures to ensure the security of the information contained in the plan;
- measures designed to ensure effective security of cargo and cargo handling equipment at the port facility;
- procedures for auditing the port facility security plan;
- procedures for responding in case the ship security alert system of a ship at the facility has been activated;
- 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 organizations. A16.3

All PFSP's, should in addition, take account of these items of Part 'B':

- detail the security organization of the port facility;
- detail the organization's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organization and its links with others, including ships in port;
- detail the basic security level 1 measures, both operational and physical, that will be in place;
- 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;
- provide for regular review, or audit, of the PFSP and for its amendment in response to experience or changing circumstances;
- detail reporting procedures to the appropriate Contracting Government's contact points.

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. B16.3

In addition to the guidance given above, the PFSP should establish the following, which relate to all security levels:

- the role and structure of the port facility security organization;
- 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;
- the port facility security organization's links with other national or local authorities with security responsibilities;
- 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;
- the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;
- the procedures and practices to protect security-sensitive information held in paper or electronic format;
- the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;
- the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;
- procedures relating to cargo handling;
- procedures covering the delivery of ship's stores;
- the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility;
- the means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches;
- the procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested;
- 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 organizations. B16.8

Access to the Port Facility

The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA. 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. B16.10 B16.11

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 practicable to do so, be co-ordinated with that applying to ships that regularly use the port facility.

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. B16.12

Those Unwilling or Unable to Establish their Identity

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. B16.13

Security Procedure Areas

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, loading and unloading areas. B16.14

The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons. B16.15

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. B16.16

Restricted Areas within the Port Facility

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:

- protect ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;
- protect the port facility;
- protect ships using, and serving, the port facility;
- protect security-sensitive locations and areas within the port facility;
- protect security and surveillance equipment and systems;
- protect cargo and ship’s stores from tampering. B16.21

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

- access by individuals;
- the entry, parking, loading and unloading of vehicles;
- movement and storage of cargo and ship's stores; and
- unaccompanied baggage or personal effects. B16.22

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. B16.23

Restricted areas may include:

- shore and water-side areas immediately adjacent to the ship;
- embarkation and disembarkation areas, and ships personnel holding and processing areas, including search points;
- areas where loading, unloading or storage of cargo and stores is undertaken;
- locations where security-sensitive information, including cargo documentation, is held;
- areas where dangerous goods and hazardous substances are held;
- vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;
- areas where security and surveillance equipment are stored or located;
- essential electrical, radio and telecommunication, water and other utility installations;
- other locations in the port facility where access by vessels, vehicles and individuals should be restricted. B16.25

Structures External to the Port

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. B16.26

Handling of Cargo

The security measures relating to cargo handling should:

- prevent tampering;
- prevent cargo that is not meant for carriage from being accepted and stored within the port facility. B16.30

Delivery of Ship's Stores

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

- ensure checking of ship's stores and package integrity;
- prevent ship's stores from being accepted without inspection;
- prevent tampering;
- prevent ship's stores from being accepted unless ordered;
- ensure searching the delivery vehicle; and
- ensure escorting delivery vehicles within the port facility. B16.38

Handling Unaccompanied Baggage

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 owner 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. B16.45

Monitoring the Security of the Port Facility

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:

- lighting;
- security guards, including foot, vehicle and waterborne patrols;
- automatic intrusion-detection devices and surveillance equipment. B16.

Intrusion Devices

When used automatic intrusion-detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored which can respond to the triggering of an alarm. B16.24 B16.50

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. B16.51

Operational and Physical Security Measures

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. B1.19

In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located. A14.4.1

Use of Firearms

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. B16.7

Declarations of Security (DoS)

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. B16.57

Differing Security Levels

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. B16.55

Activities not covered by the Code

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

- it is interfacing with a ship which has been at a port of a State which is not a Contracting Government;
- it is interfacing with a ship to which this Code does not apply;
- it is interfacing with fixed or floating platforms or mobile offshore drilling units on location. **B16.56**

Security Provisions - Date of Introduction

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. B16.6

Statement of Compliance of a Port Facility

The Contracting Government within whose territory a port facility is located may issue an appropriate Statement of Compliance of a Port Facility (SoCPF) indicating that the port facility complies with the provisions of Chapter XI-2 and Part 'A' of the Code. (*See also Section 8 of this guide*) B16.62

Changes to the Plan

The Contracting Government in whose territory the port facility is located shall determine which changes to the port facility security plan shall not be implemented unless the relevant amendments to the plan are approved by them. A16.6

Retention of Records

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. B16.5

Amendment Audit and Review

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. B1.20

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. B16.58

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

- if the PFSA relating to the port facility is altered;
- 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;
- following security incidents or threats thereof involving the port facility;
- following changes in ownership or operational control of the port facility. B16.59

Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility. A16.4

Protection from Unauthorised Access Destruction or Disclosure

The plan shall be protected from unauthorized access or disclosure. The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. A16.7 A16.8

Combination Plans

The port facility security plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans. A16.5

Similar Ports

Contracting Governments may allow a port facility security plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government which allows such an alternative arrangement shall communicate to the Organization particulars thereof. A16.9

Port Facilities Security Officer (PFSO) Section 6

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 the Code. B1.18

Port Facility Security Officer (PFSO).

A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities. A17.1

Support

The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by Chapter XI-2 and this Part of the Code. A17.3

Duties

In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

- conducting an initial comprehensive security survey of the port facility, taking into account the relevant port facility security assessment;
- ensuring the development and maintenance of the port facility security plan;
- implementing and exercising the port facility security plan;
- undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
- recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;
- enhancing security awareness and vigilance of the port facility personnel;
- ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- co-ordinating with security services, as appropriate;
- ensuring that standards for personnel responsible for security of the port facility are met;
- ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
- assisting ship security officers in confirming the identity of those seeking to board the ship when requested. A17.2

The port facilities which have to comply with the requirements of Chapter XI-2 and Part 'A' of the 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 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 specific elements of an approved plan will have to be submitted for approval by the Contracting Government or by the Designated Authority concerned. B1.20

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. B16.1

The PFSO shall ensure the effective co-ordination and implementation of the PFSP by participating in exercises at appropriate intervals, taking into account the guidance given in Part 'B' of this Code. A18.4

Non Compliance

When a port facility security officer is advised that a ship encounters difficulties;

- in complying with the requirements of Chapter XI-2;
- in implementing the appropriate measures and procedures as detailed in the ship security plan;
- in the case of security level 3, following any security instructions given by the Contracting Government within whose territory the port facility is located;

the port facility security officer and the ship security officer shall liaise and co-ordinate appropriate actions. A14.5

Ship at Higher Security Level

When a port facility security officer is advised that a ship is at a security level which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary. A14.6

Amendments

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

- proposed changes, which could fundamentally alter the approach adopted to maintaining the security of the port facility;
- 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. B16.60

Port Facilities Security Training Section 7

To ensure the effective implementation of the port facility security plan, drills must be carried out at appropriate intervals, taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in Part 'B' of the Code. A18.3

The PFSO shall ensure the effective co-ordination and implementation of the PFSP by participating in exercises at appropriate intervals, taking into account the guidance given in Part 'B' of the Code. A18.4

The PFSO and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in Part 'B' of the Code. A18.1

Port Facility Security Officer (PFSO)

The PFSO should have knowledge and receive training, in some or all of the following, as appropriate:

- security administration;
- relevant international conventions, codes and recommendations;
- relevant Government legislation and regulations;
- responsibilities and functions of other security organizations;
- methodology of port facility security assessment;
- methods of ship and port facility security surveys and inspections;
- ship and port operations and conditions;
- ship and port facility security measures;
- emergency preparedness and response and contingency planning;
- instruction techniques for security training and education, including security measures and procedures;
- handling sensitive security-related information and security related communications;
- knowledge of current security threats and patterns;
- recognition and detection of weapons, dangerous substances and devices;
- recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;
- techniques used to circumvent security measures;
- security equipment and systems, and their operational limitations;
- methods of conducting audits, inspection, control and monitoring;
- methods of physical searches and non-intrusive inspections;
- security drills and exercises, including drills and exercises with ships;
- assessment of security drills and exercises. B18.1

Personnel with Specific Security Duties

Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the port facility security plan, and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part 'B' of this Code. A18.2

Port facility personnel having specific security duties should have knowledge and receive training in some or all of the following, as appropriate:

- knowledge of current security threats and patterns;
- recognition and detection of weapons, dangerous substances and devices;
- recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
- techniques used to circumvent security measures;
- crowd management and control techniques;
- security-related communications;
- operations of security equipment and systems;
- testing, calibration and maintenance of security equipment and systems;
- inspection, control, and monitoring techniques; and
- methods of physical searches of persons, personal effects, baggage, cargo and ships stores. B18.2

All Other Personnel

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:

- the meaning and the consequential requirements of the different security levels;
- recognition and detection of weapons, dangerous substances and devices;
- recognition of characteristics and behavioural patterns of persons who are likely to threaten the security;
- techniques used to circumvent security measures. B18.3

Drills and Exercises

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. B18.4

Frequency

To ensure the effective implementation of the provisions of the PFSP, 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 of the Code.

B18.5

Joint Exercises

Various types of exercises, which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, Company Security Officers (CSO), or Ship Security Officers (SSO), 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 CSO's or SSO's in joint exercises 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:

- full-scale or live;
- tabletop simulation or seminar; or
- combined with other exercises held, such as emergency response or other port state authority exercises.

B18.6

Statement of Compliance of a Port Facility (SoCPF) Section 8

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

- the port facility;
- that the port facility complies with the provisions of Chapter XI-2 and Part 'A' of the Code;
- the period of validity of the SoCPF, which should be specified by the Contracting Governments but should not exceed five years; and
- the subsequent verification arrangement established by the Contracting Government and a confirmation when these are carried out. B16.62

The Statement of Compliance of a Port Facility should be in the form set out in Part 'B' appendix 2 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. B16.63

An example of a Statement of Compliance is given in the next two pages:-

Form of Statement of Compliance of a Port Facility, Appendix 2 to Part 'B' of the ISPS Code

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 the 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 scheduled).

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.

1st VERIFICATION.

Signed……
(Signature of authorized official)

Place: ……

Date:……..

2nd VERIFICATION.

Signed……
(Signature of authorized official)

Place: ……

Date:……..

3rd VERIFICATION.

Signed……
(Signature of authorized official)

Place: ……

Date:……..

4th VERIFICATION.

Signed……
(Signature of authorized official)

Place: ……

Date:……..

Port/Ship Interface Section 9

Ships General

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 prior to the ship's entry into port regarding:

- the ship;
- the cargo;
- ship's personnel

There may be circumstances in which entry into port could be denied. B1.21

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;
- additional provisions applicable to both situations. B4.29

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. B4.30

Contact Points

Where a port facility has a PFSP, that fact has to be made available to Shipping Company Security Officers CSO's and Ship Security Officers SSO's. No further details of the PFSP have to be published other than that it is in place. B4.14

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 PFSP's are in place, together with contact details for the relevant PFSO. The existence of such contact points should be publicised. B4.14

Declaration of Security (DoS) Section 10

Declaration of Security Requirements

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. B5.4

The DoS shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each. A5.5

Contracting Governments shall determine when a DoS is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment. A5.1

Contracting Governments shall specify, bearing in mind the provisions of Regulation XI-2/9.2.3, the minimum period for which DoS shall be kept by the port facilities located within their territory. A5.6

Authorised Personnel

The Declaration of Security shall be completed by:

- the master or the ship security officer on behalf of the ship; and, if appropriate,
- the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility. A5.4

Situations where a DoS is indicated

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. B5.1

The need for a DoS may be indicated by the results of the PFSA and the reasons and circumstances in which a DoS is required should be set out in the port facility security plan (PFSP). B5.1.1

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). B5.1.2

Differing Levels of Security

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 DoS. B4.12

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 relevant contact details. B5.4.1

Requests for the completion of a DoS, under this section, shall be acknowledged by the applicable port facility or ship. A5.3

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. B5.2.1

An example of a Declaration of Security is given in the next two pages.

Form of Declaration of Security
Between a ship and a port facility

(As found in Appendix 1 to Part 'B' of the ISPS Code)

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.

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.

	The affixing of the initials of the FSO or SSO under these columns indicates that the activity will be done, in accordance with the relevant approved plan, by:	
Activity	**The port facility:**	**The ship**
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorised 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 the 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 the 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.

Dated …… 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
PFSO	SSO
	Company
	CSO

Port State Control Inspections

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. B1.21

Information from Ships intending to enter the Port

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:

- 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;
- any Declarations of Security that were entered into with port facilities or other ships. B4.37

Fixed and Floating Platforms and Mobile Offshore Drilling Units on Location

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. B4.19

Floating, Production, Storage and Offloading (FPSO) and Floating Storage Unit (FSU) vessels on Location

Although not originally referenced in the ISPS Code, during MSC 77 (May/June 2003) it was agreed that neither Floating Production, Storage and Offloading units (FPSOs) nor Floating Storage Units (FSUs), were ships subject to the provisions of the ISPS Code, but that they should have some security procedures in place.

Single Buoy Moorings (SBMs)

Single buoy moorings (SBMs), attached to an offshore facility would be covered by that facility's security regime and if it was connected to a port facility it would be covered by the port facility security plan (PFSP).

In all above cases the intention should be to provide sufficient security to maintain the integrity and not to otherwise "contaminate" ships and port facilities to which the SOLAS and the ISPS Code applies by virtue of a call to the FPSO/FSU or SBM

Equivalent and Alternative Security Arrangements Section 13

Summary

Port facilities attached to industries with limited or specialized port operations may wish to ensure compliance by adopting agreed equivalent security measures.

Equivalent Measures

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 the ISPS Code. This can, in particular, be the case for terminals such as those attached to factories, or quaysides with no frequent operations. B4.27

Alternative Security Agreements

Contracting Governments may conclude one or more agreements with one or more Contracting Governments. The scope of such an agreement is limited to short international voyages on fixed routes between port facilities in the territory of the parties to the agreement. B4.26

Designated Authorities and Recognised Security Organisations (RSO) — Section 14

Contracting Governments may identify a Designated Authority, or an approved Recognised Security Organisation to undertake their security duties relating to port facilities.

Recognised Security Organisation (RSO)

Contracting Governments may authorize a recognized security organization (RSO) to complete port facility security assessments and prepare port facility security plans for specific facilities; A port or harbour authority or port facility operator may be appointed as an RSO provided it has the appropriate security-related expertise. B4.5 B4.7

- An RSO may assist companies or port facilities on security matters, including development and completion of port facility security assessments and security plans. B4.4
- Where a Contracting Government uses an RSO to review or verify compliance of the PFSA, that RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment. B15.2

Port Facility Security Assessments and Port Facility Security Plans are required to be approved by the Contracting Government in whose territory the port facility is located. A15.2 A15.2.1 A16.1.1 A16.2

When authorizing a Recognised Security Organisation, Contracting Governments are required to give consideration to the competency of such organization. A15.3 B4.5

Duties that an RSO may not undertake.

Contracting Governments may not delegate to a recognized security organization certain of their security related duties:

- setting of the applicable security level;
- approving a port facility security assessment and subsequent amendments to an approved assessment;
- determining the port facilities which will be required to designate a port facility security officer;
- approving a port facility security plan and subsequent amendments to an approved plan;
- exercising control and compliance measures pursuant to Regulation XI-2/9;
- establishing the requirements for a Declaration of Security. A4.3

Security Level Communication

Contracting Governments should establish means of notifying PFSO's 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 means by which it is conveyed PFSO's. B4.13

Contracting Governments should also provide the contact details of Government officers to whom a PFSO can report security concerns. B4.16

Extended Measures

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. B16.26

Identification Documents

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. B4.18

Communication of Information to IMO

Chapter XI-2 and Part 'A' of this Code require Contracting Governments to provide certain information to the International Maritime Organization (IMO) and for information to be made available to allow effective communication between Contracting Governments and between company security officers/ship security officers and the port facility security officers B1.22

Notification of Security Levels

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 means by which it is conveyed to PFSOs. B4.13

Existence of PFSP

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 publicised. They could also provide information on the recognized security organizations appointed to act on behalf of the Contracting Government, together with details of the specific responsibility and conditions of authority delegated to such recognized security organizations. B4.14

Suitably Qualified Person

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 ships visit. B4.15

Government Officers

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 IMO. B4.16

Recognized Security Organisation (RSO)

Contracting Governments may authorize a recognized security organization (RSO) to undertake certain security-related activities, including:

- approval of ship security plans, or amendments thereto, on behalf of the Administration;
- 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;
- conducting port facility security assessments required by the Contracting Government. B4.3

RSO Authorization

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

- expertise in relevant aspects of security;
- 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;
- 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 minimize such risks;
- their ability to maintain and improve the expertise of their personnel;
- their ability to monitor the continuing trustworthiness of their personnel;
- their ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security-sensitive material;
- their knowledge of the requirements of Chapter XI-2 and Part 'A' of this Code and relevant national and international legislation and security requirements;
- their knowledge of current security threats and patterns;
- their knowledge of recognition and detection of weapons, dangerous substances and devices;
- their knowledge of recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- their knowledge of techniques used to circumvent security measures; and
- 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. B4.5

Recognized Organisation (RO)

A recognized organization as referred to in SOLAS Regulation I/6 and fulfilling the requirements of SOLAS Regulation XI-1/1, may be appointed as an RSO provided it has the appropriate security-related expertise listed in paragraph B4.5. B4.6

Harbour or Port Authority

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 B4.5. B4.7

Delegation of Duties to an RSO

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

- setting of the applicable security level;
- approving a port facility security assessment and subsequent amendments to an approved assessment;
- determining the port facilities which will be required to designate a port facility security officer;
- approving a port facility security plan and subsequent amendments to an approved plan;
- exercising control and compliance measures pursuant to Regulation XI-2/9; and
- establishing the requirements for a Declaration of Security. A4.3

PORT FACILITY SECURITY PLAN (PFSP)

NOTE:

This is an unofficial translation from Norwegian of a document issued by The National Coastal Administration (Kystdirektoratet) of Norway. The document was prepared in cooperation with Det Norske Veritas (DNV) as a part of a manual with guidance for how to implement the amendments to SOLAS (Safety of Life at Sea) Chapter XI-2 and the ISPS (International Ship & Port Facility Security) Code at Norwegian port facilities.

Where the Norwegian original has made a reference summary of the paragraphs in the ISPS Code, the unofficial translation has included the full text of each paragraph.

OCIMF appreciates the courtesy of The National Coastal Administration of Norway in allowing us to make this unofficial translation.

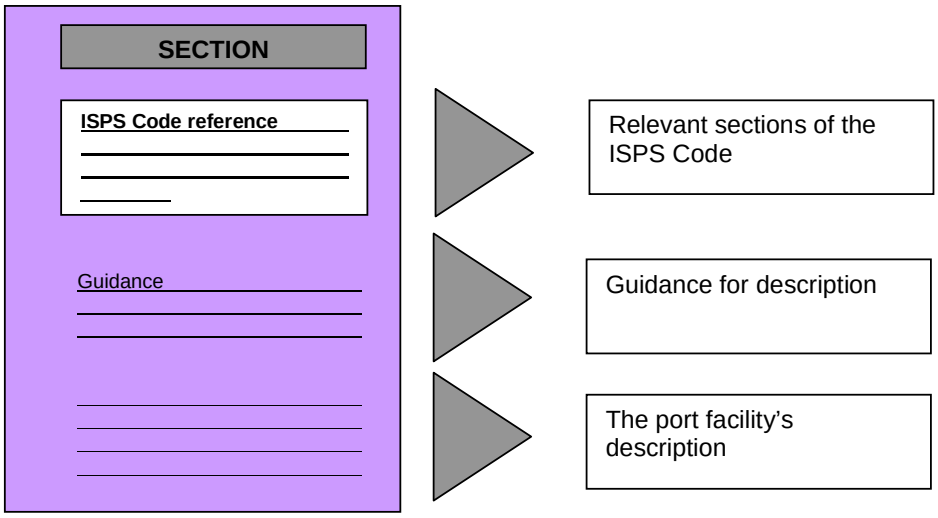
Introduction

Reference is made to the ISPS Code Part 'A' 16.1 saying;

"A port facility security plan shall be developed and maintained, on the basis of a port facility security assessment for each port facility, adequate for the ship/port interface. The plan shall make provisions for the three security levels, as defined in this Part of the Code."

Use the results from the security assessment to describe the security measures and procedures that the port facility will implement for each of the security levels. The security assessment identifies measures for security level 1, while the PFSP also must include measures and procedures that shall be implemented upon security level 2 and 3. Additionally the ISPS Code gives requirements to information, routines and log keeping that should be described in the security plan.

To ensure that the port facility include all relevant sections described in the ISPS Code, a model plan – this document – is prepared as a guidance for the port facility in preparation of its security plan. The model plan is structured as follows:



Model plan structure

Below each section there will be a reference to the relevant items in the ISPS code, with a short summary of the text in the Code. This is written in **bold inside the frame.** Furthermore, there will be guidance to what should be described in the section.

The port facility may use the model plan directly by using the ISPS Code reference and the guidance and thus be in a position to prepare their port facility security plan (PFSP). Upon completion of the plan, the **ISPS code reference** and guidance text should be deleted. Where the port facility, based on their operation, nature and/or location, chooses not to include a part described in the model plan, the reason for this should be described.

The security plan (PFSP) is subject to approval by the Contracting Government.

PORT FACILITY SECURITY PLAN
(PFSP)

The content of this plan is strictly confidential

_____

Port Facility

Doc. No./Rev.:	Description:	Prepared by:	Approved by:	This version is based on PFSA:

Table of Contents:

Document Status and Revision Control

Guidance:
Use the table on the front page of the PFSP to record document status and revision control.

Purpose and Background

Guidance:
This security plan is written in accordance with the requirements of the amendments to SOLAS, Chapter XI-2 and Part 'A' and 'B' of the international security code for ships and port facilities (International Ship & Port Facility Security Code, ISPS code). As of July 1st 2004 it is required that all port facilities serving passenger ships, cargo ships above 500 gross tonnes and mobile offshore drilling units in international traffic shall comply with the ISPS Code and have an approved security plan.

The main purpose of the ISPS Code is to enhance maritime "safety and security". The Code establishes an international framework that encourages cooperation between Contracting Governments, Designated Authorities, organisations, shipping and port facility industries, and others for the establishment of preventive measures in order to oppose security threats to port facilities and ships in international traffic.

The plan contains all information, operational procedures and measures required by SOLAS and the Code, Part 'A' and 'B'.

The security plan is based on an approved security assessment (referenced on the front page of this security plan). The plan will be updated and revised regularly and changed upon alterations to the port facility's objects, operations, infrastructure or nearby areas.

Security measures are based on a plan of actions from the security assessment and in cooperation with local authorities, suppliers and ship owners. The plan further describes measures to be implemented at security levels 1, 2 and 3.

The purpose of this plan is to:

- Document and describe responsibility, measures and procedures for security at the port facility.
- Establish routines for sharing of responsibility for security tasks between the ship and the port facility.
- Act as guidance for the PFSO (Port Facility Security Officer), with regards to security, in order to improve awareness, prevention and form of action.
- Give contact information to the PFSO and other security organisations.
- Through implementation and follow up of the plan, enhance the port facility security in order to reveal, delay or possibly avoid security incidents.
- Ensure that records of security activities are kept for traceability and handling of non-conformities.

Appendix:
Copy of the Statement of Compliance issued by the Contracting Government.

Definitions and Expressions

Guidance:
Include definitions and expressions used in the security plan and as shown in the table below (not complete; add your own abbreviations):

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

DoS (Declaration of Security): Agreement between ship and port facility that describes the share of responsibilities for implementing security measures.

IMO: International Maritime Organization.

ISPS Code (International Ship & Port Facility Security Code): IMO's international code for ship and port security.

Port Facility Security Assessment (PFSA): Process for assessment of a port facility's vulnerability with regards to a security incident. A security assessment shall include a number of activities described in the ISPS Code, Part 'A' and 'B'.

Port Facility Security Officer (PFSO): The person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

Port Facility Security Plan (PFSP): A plan developed to ensure the application of measures designed to protect the port facility and ships, persons**,** cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

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

Security level 1: The level for which minimum appropriate protective security measures shall be maintained at all times. Also known as "near normalcy".

Security level 2: The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

Security level 3: The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target. It is envisaged that at level 3 outside assistance, such as provided by national security or military services, will step in and take control of the ongoing situation.

1 Protection of Security Related Information

ISPS Code (A/16.3.11, A/16.7&8, B/16.8.6):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.11 measures to ensure the security of the information contained in the plan

A.16.7 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

A.16.8 The plan shall be protected from unauthorized access or disclosure.

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

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

1.1 Classification and Protection of the Security Plan

Guidance:
Describe how the plan will be filed.

The PFSA and PFSP are classified documents and the distribution should be limited. Procedures should control handling of sensitive information that, if known, can harm the national security. The plan shall be protected against unauthorized access.

The procedure that is established to protect against unauthorized access shall include both electronic and hard copy versions. The number of copies should be defined.

1.2 Access to the Security Plan

Guidance:
Only authorized personnel shall have access to the security plan. All personnel having access to the plan shall be identified. This can be done by a table including:

- Name and date of birth.
- Position or function.

1.3 Safeguarding of Security Related Information

Guidance:
Describe procedures for how the port facility will safeguard the security related information. This can be, but are not limited to:

- Secrecy declaration related to all security systems at the port facility.
- Procedures related to who should receive information about arrival and departure of ships and different type of cargo to be shipped through the terminal.

Describe the terminals procedures for training of personnel that will handle security related information (ref. Also section 6.1. Training.)

2 Audit, Periodical Review and Updating of the PFSP

ISPS Code (A/16.3.8, B/16.3.5):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.8 procedures for the periodic review of the plan and updating

B.16.3 All PFSPs should:

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

2.1 Internal Audit

ISPS Code (A/16.4):

A.16.4 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility

Guidance:

The port facilities internal audit process shall be described. The audit shall verify that security measures described are implemented, function satisfactorily and that personnel with security responsibility are familiar with their duties and relevant procedures described in the PFSP. The description of the audit should include:

- The internal audit intervals
- Who is responsible for the audit
- Audit scope, what should be checked and how
- Follow up, information and handling of non-conformities

It is recommended to establish a checklist to be used when performing the audit.

2.2 Review and Updating of the PFSP

Guidance:

A review and updating of the PFSP should be performed based on recommendations or comments from an audit, following a security incident or at least once every year. The PFSO is responsible for review and updating of the PFSP.

The review shall consider the following:

- Changes to the port facility's operation and/or infrastructure
- Results of an audit
- Report from a security incident

The audit process and periodical review shall be documented, e.g. as follows:

Activity/responsibility	Requirement	Performed:
Internal audit and review of the security activities	Example: Annually	Example: 1 July 2003
Periodical review of the PFSA	Every 2 ½ year	1 March 2003
Periodical review of the PFSP	Every 2 ½ year	1 April 2003
Date		dd.mm.yyyy
Signature/confirmation		……..

2.3 Approval of Updates

ISPS Code (A/16.6):

A.16.6 The Contracting Government in whose territory the port facility is located shall determine which changes to the port facility security plan shall not be implemented unless the relevant amendments to the plan are approved by them.

Guidance:
The PFSO can implement all necessary changes and updates to the PFSP. The Contracting Governments (CG) at their periodical review of the PFSP will review the updating and changes. Minor changes to the PFSP shall be reviewed and included at annual updating of the plan. It should not be required to reissue the PFSP for approval when minor changes are implemented. Upon major changes, the PFSP shall immediately be sent in for new approval by CG.

The port facility shall keep track records of all changes and updates to the PFSP.

2.4 Reporting of Security Incidents or Breaches of Security

ISPS Code (A/16.3.9, B/16.8.8):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:
.9 procedures for reporting security incidents.

B.16.8 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:
.8 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns.

Guidance:
It is recommended to establish a checklist for reporting of security incidents. This should include when and how the incident report shall be sent to the authorities for approval. Example:

Incident:	Description:	Date of incident	Handling of non-conformity:

3 Security Organization at the Port Facility

ISPS Code (B/16.3.1, B/16.8.1):

B.16.3 All PFSPs should:
.1 detail the security organization of the port facility,

B.16.8 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:
.1 the role and structure of the port facility security organization

3.1 Organization Chart

Guidance:
The security organisation should be visualised in an organisation chart. The port facility security organisation should be in line with organisation of other activities at the terminal.

3.2 Contact Information to Relevant Security Authorities

ISPS Code (A/16.3.10, B/16.8.3):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:
.10 identification of the port facility security officer including 24-hour contact details

B.16.8 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:
.3 the port facility security organisation links with other national or local authorities with security responsibilities

Guidance:
Develop an organisation chart with lines of communication to relevant local and national security authorities. This should include points of contact to central security, local police department, contracting government, harbour authorities in the region, etc.

It is recommended to make a table containing the following information:

Name	Organisation/ Company	Address	Office phone	Mobile/ Home phone	Other contact info

The 24-hour contact information for the PFSO to be described.

3.3 Responsibility for Port Facility Security

ISPS Code (A/16.3.6, A/17.1-3, B/16.8.2):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects

A.17.1 A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

A.17.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.1 conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
.2 ensuring the development and maintenance of the port facility security plan;
.3 implementing and exercising the port facility security plan;
.4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
.5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
.6 enhancing security awareness and vigilance of the port facility personnel;
.7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;
.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
.9 co-ordinating implementation of the port facility security plan with the appropriate Company and Ship security officer(s);
.10 co-ordinating with security services, as appropriate;
.11 ensuring that standards for personnel responsible for security of the port facility are met;
.12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
.13 assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

A.17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by Chapter XI-2 and this Part of the Code.

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

.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.

Guidance:

Here the duties and area of responsibility for the port facilities security personnel should be described.

For the port facilities at _____, the overall security is the responsibility of the harbour master and PFSO. They will, individually or together, make decisions that, in accordance with his/their professional judgement, are required for maintaining the security of the port facility. This includes initiation of any measure required or necessary to maintain the security.

It is recommended to describe the area of responsibility for PFSO, other security personnel and additional personnel as relevant.

Duties and areas of responsibility of the PFSO shall include, but are not limited to *(this is included as guidance, delete what is not relevant and add other relevant task/s)*:

- Performance of a comprehensive initial security survey of the port facility where the results from the PFSA are taken into account.
- Ensure development and maintenance of the PFSP.
- Conduct periodical security inspections at the port facility in order to ensure implementation of proper security measures.
- Recommend and include modifications in the PFSP in order to improve weaknesses and update the plan so that changes to the port facility are implemented.
- Strengthen the consciousness and alertness with regards to security among the employees at the port facility.
- Ensure that adequate training is offered to personnel responsible for the port facility security.
- Report to the authorities and keep records of port facility security threats.
- Coordinate the implementation of the PFSP with interfacing companies and SSO's.
- Ensure that employees responsible for security at the port facility adhere to the relevant standards.
- Ensure that security equipment is correctly used, tested, calibrated and maintained.
- Assist the SSO, as required, by confirming the identity of persons that seek access to the ship.

Similar list of duties and area of responsibility should be prepared for:

- Port facility security personnel.
- Other port facility personnel.

4 Interface with Ship Security Activities

ISPS Code (A/16.3.7):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.7 procedures for interfacing with ship security activities

4.1 Exchange of Information

ISPS Code (B/4.11):

B.4.11 The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liaise at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility.

Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility's security level and should provide the ship with any relevant security information.

Guidance:

Develop a procedure that describes how the exchange of information between a ship and port facility, with regards to ISPS requirements, shall be conducted. e.g. at a change of security level the following need to be described:

- Who (at the port facility) will inform the ship and coordinate actions together with the SSO.
- Who will decide if a new DoS shall be issued if the existing DoS does not cover the new security level? Further, describe the criteria that will require a new DoS to be established. Reference is also made to section 4.2 (DoS).

The PFSO shall, as soon as possible, establish contact with the SSO and provide information about the security level at the port facility. Further, he shall inform the SSO of any changes in security level and provide other relevant security information. Procedures should be developed.

4.2 Declaration of Security (DoS)

ISPS Code (A/5, B/5):

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

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

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

.2 there is an agreement on a DoS between Contracting Governments covering certain international voyages or specific ships on those voyages;

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

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

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

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

(continued over page)

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

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

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

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

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

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

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

B.5.1.1 The need for a DoS may be indicated by the results of the PFSA and the reasons and circumstances in which a DoS is required should be set out in the PFSP.

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

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

B.5.2.1 In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the PFSO or SSO should acknowledge the request and discuss appropriate security measures.

B.5.3 A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking of 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.

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

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

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

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

B.5.6 A model DoS is included in Appendix 1 to this part of the Code ***(see page 29 of this document)*****. 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.**

Guidance:
The purpose of the DoS is to ensure agreement between the ship and port facility of the respective security measures and that the ship-shore activities will perform in accordance with their respective security plans. This will ensure that the security is taken care of in a satisfactory and efficient manner.

A DoS would normally only be needed in extraordinary situations and is not generally required. Further, a ship can **request** a DoS but the port facility can **demand** a DoS is issued prior to ship call.

A DoS shall be issued upon request of the security authorities.

4.3 Different Level of Security

ISPS Code (A/14.6, B/4.12):

A.14.6 When a port facility security officer is advised that a ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liase with the ship security officer and co-ordinate appropriate actions, if necessary.

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

Guidance:
The PFSO should undertake an assessment of the situation in consultation with the CSO or SSO. The result can be completion of a DoS. Procedures to cover this should be established.

4.4 Ships that Encounter Difficulties in Complying with Requirements

ISPS Code (A/14.5):

A.14.5 When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of Chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security officer and ship security officer shall liase and co-ordinate appropriate actions.

Guidance:
The PFSO and SSO shall liase and coordinate appropriate actions. A procedure should be established describing how this is done.

4.5 Suspicion of Irregularities Onboard a Ship

Guidance:
Describe actions to be implemented by the port facility if such suspicion arises. The PFSO shall liase with security authorities to decide if a ship shall be denied access to the port facility. If a ship will not accept to be denied access, this should be reported to the security authorities and the local police department.

4.6 Activated Ship Security Alert System at the Port Facilities

ISPS Code (A/16.3.14):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.14 procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

Guidance:

Prepare a procedure describing the port facility's action upon such security alert – who acts, how, etc.

Information about an activated ship security alarm shall as soon as possible be reported to the PFSO, who shall establish contact with the SSO and obtain a verification of the situation.

PFSO duties (examples only):

- Evaluate the situation and try to get an overview of the threats to the ship and the port facility (who, number of persons, type of threat, etc.)
- Initiate actions
- Inform the authorities and the police department

4.7 Cooperation and Coordination of Security Measures

ISPS Code (A/17.2.9 & .13)

A.7.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.9 co-ordinating implementation of the port facility security plan with the appropriate Company and Ship security officer(s);

.13 assisting Ship security officers in confirming the identity of those seeking to board the ship when requested.

Guidance:

The terminal shall, upon request, assist the SSO by confirming the identity of persons seeking access to the ship. Prepare a procedure describing how this identification shall be performed:

- Verification of the identity documents
- Contact with employer
- Contact with the police

The ship may, in liaison with the port facility, establish a dedicated area where identification, inspection and checking of persons, luggage and goods can be performed. Further, ensure that all vehicles can be subject to control and checking in accordance with the requirements of the SSP. Even if the responsibility rests with the ship, there will still be a need for coordination of the control of persons, luggage and vehicles at the port facility to ensure conformity between the PFSP and SSP.

The PFSO should describe how the port facility will take into account the requirements of the SSP, and how this will be coordinated between PFSO and SSO.

5 Security Measures

ISPS Code (A/16.3.1 & .2):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

- **.1 measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;**
- **.2 measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;**

5.1 Description of Security Levels 1-2-3

ISPS Code (A/2.1.9-.11):

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

- **.9 Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.**
- **.10 Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.**
- **.11 Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.**

Guidance:

The relevant security authority will determine the security level that applies to the port facility. However, following incidents or security deficiency, the local police department or PFSO can change the level of security as deemed necessary. Security level 1 is the modus of normal operation.

5.2 Records of Dangerous Goods

ISPS Code (B/16.8.11):

B.16.8 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:
.11 the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility.

Guidance:

Procedures are to be established defining how the port facility keep track of dangerous goods at their premises. The port facility may already have established procedures for handling of dangerous goods (e.g. based on the International Maritime Dangerous Goods (IMDG) Code). If so, elements of this should be used as relevant.

5.3 Restricted Areas

ISPS Code (B/16.21):

B.16.21 The PFSP should identify the restricted areas to be established within the port facility, 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 sensitive security locations and areas within the port facility;
.5 to protect security and surveillance equipment and systems; and
.6 protect cargo and ship's stores from tampering.

Guidance:
The security plan shall include maps of the terminal area where restricted areas are clearly marked. Further, a table should be made including:

- Name of the restricted area, building, etc.
- When and at which occasions new restricted areas will be established.

Description of measures is given in section Security measures, item 5.6-5.8.

5.4 Security Instruction from Contraction Government at Security Level 3

ISPS Code (A/16.3.4):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.4 procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3;

Guidance:
Prepare a procedure that describe how the port facility will stay in continuous contact with the Contracting Government at security level 3, and how it will cooperate in implementing appropriate measures. This can be through cooperation with police department and the civil defence.

5.5 Use of Firearms

ISPS Code (B/16.7):

B.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 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 its application to ships carrying dangerous goods or hazardous substances.

Guidance:
The use of firearms within the port facilities is considered a particular and significant safety risk, in particular in ports that handle dangerous or hazardous substances. As it may be applicable for the police or army to carry weapons in connection with the measures described in the PFSP, there should be description for precautions and how to act to avoid that it will constitute a risk to the operation at the terminal.

5.6 Security Measures at Level 1

ISPS Code (B/16.9-54):

B.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.**

Further reference is made to sections 16.9 through to 16.54 of ISPS Code Part 'B'.

Guidance:
Based on the PFSA and the plan of actions, describe the measures that the port facility have implemented as a part of normal operations.

The PFSA shall give an answer to those security measures that are required to be implemented by the port facility. Regardless of the result of the PFSA all appropriate security measures should be addressed.

Describe those measures that are relevant for the port facility. The PFSP shall also include a description of what the measures involve and who is responsible for execution. Group the measures as follows:

Access control
Restricted areas
Cargo control, ship stores and baggage
Surveillance

5.7 Security Measures at Level 2

Guidance:
Based on the measures at security level 1, describe those additional measures that will be implemented at security level 2. These can be an enforcement of the level 1 measures as well as new measures. Structure as at level 1 should be maintained. Group the measures as follows:

Access control
Restricted areas
Cargo control, ship stores and baggage
Surveillance

5.8 Security Measures at Level 3

Guidance:
Based on the measures at security level 2, describe those additional measures that will be implemented at security level 3. These can be an enforcement of the level 1 and 2 measures as well as new measures. Structure as at level 2 should be maintained.

Additional to the measures the port facility shall at level 3 act on instructions by the Contracting Government as described in section 5.4 above.

Group the measures as follows:

Access control
Restricted areas
Cargo control, ship stores and baggage
Surveillance

6 Security Training and Drills

6.1 Training

ISPS Code (B/16.8.2):

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

.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;

Guidance:

Prepare a plan for development of skills and training requirements for security. Personnel with responsibility within port security shall have knowledge about, or receive training in, those areas described in the table below; i.e. those not already having competence within these areas of port security must receive relevant training.

The PFSP shall include an overview of

- Skill/competence requirements (related to position)
- Plan of training and drills.

The training plan shall specify the competence and training requirements for the following category of personnel:

- PFSO
- Port facility personnel with security responsibilities.
- Other port facility personnel (not having specific security responsibilities, but still required to receive training in some security topics).

Examples of competence requirements for port facility employees.
(prepare a corresponding table for the organisation):

PFSO's, port facility personnel with security responsibilities/duties and all other personnel having duties at the port facilities, should have knowledge about and receive training in all or those relevant of the following areas:			
	PFSO	**Personnel with security responsibility**	**Other port facility personnel**
Security administration	18.1.1		
Relevant international conventions, codes and recommendations	18.1.2		
Relevant Government legislation and regulations	18.1.3		
Responsibilities and functions of other security organizations	18.1.4		
Methodology of port facility security assessment	18.1.5		
Methods of ship and port facility security surveys and inspections	18.1.6		
Ship and port operations and conditions	18.1.7		
Ship and port facility security measures	18.1.8		
Emergency preparedness and response and contingency planning	18.1.9		
Instruction techniques for security training and education, including security measures and procedures	18.1.10		
Handling sensitive security related information and security related communications	18.1.11		
Knowledge of current security threats and patterns	18.1.12	18.2.1	
Recognition and detection of weapons, dangerous substances and devices	18.1.13	18.2.2	18.3.2
Recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security	18.1.14	18.2.3	18.3.3
Techniques used to circumvent security measures	18.1.15	18.2.4	18.3.4
Security equipment and systems, and their operational limitations	18.1.16		
Methods of conducting audits, inspection, control and monitoring	18.1.17		
Methods of physical searches and non-intrusive inspections	18.1.18		
Security drills and exercises, including drills and exercises with ships; and	18.1.19 18.4	18.4	18.4
Assessment of security drills and exercises	18.1.20		
Crowd management and control techniques		18.2.5	
Operations of security equipment and systems		18.2.7	
Testing, calibration and maintenance of security equipment and systems		18.2.8	
Security related communications		18.2.6	
Methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.		18.2.10	
The meaning and the consequential requirements of the different security levels			18.3.1

6.2 Drills

ISPS Code (B/18.4-6):

B.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.

B.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.

B.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 exercises should be made bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response. These exercises may be:

.1 full scale or live;
.2 tabletop simulation or seminar; or
.3 combined with other exercises held such as emergency response or other port State authority exercises.

Guidance:

Prepare a table of the different types of drills that the port facility has planned to carry out, including the following for each type of drill:

- Name of drill
- Purpose of drill (what are personnel to be tested or trained to)
- Method (seminar, table top, full scale)
- Scope (participants, schedule)
- Frequency (how often shall the drill be performed)

Further, it is recommended that minor drills be held every three months in order to check individual parts of the PFSP against typical threats. Other drills should be held annually, typically:

- Full scale or live
- Tabletop simulations or seminar
- Combined with other exercises held such as emergency response or other port State authority exercises

Find below an example for a drill and exercise plan.

Drill (name/purpose)	Method	Date	Responsible	Participants
ISPS code training for port authorities	*Tabletop*	**13.03.2003**	*Joe X*	*Peter A.* *Paul B.* *Mary C.*

The port facility shall also document all performed drills and exercises (based on the above drill and exercise plan). An example of such documentation is:

Drill (name/purpose)	Date	Elements tested at drill	Evaluation of result	Signature by PFSO
ISPS code training for port authorities	*13.03.2003*	**Access control**	*As planned, however…..*	*Sign:*

7 Emergency Preparedness at Security Incidents

7.1 Security Incident and Provisions for Maintaining Critical Operations

ISPS Code (A/16.3.3, B/16.8.4):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

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

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

.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

Guidance:

Emergency preparedness procedures to be established for the threats and cause of events identified in the PFSA. As an example this can be that the port facility upon discovery of an unidentified object at the terminal secures the area around the object, evacuate personnel and calls in experts (police or army). Procedures should identify persons to be contacted/notified at the different type of threats. Typically, notification should be given directly to the local police department and harbour authorities.

The PFSP shall also describe how critical port facility operations are maintained (including ship/port interaction, unloading/loading, etc.) and how personnel and other resources shall be used to obtain this. i.e. possible change of priority of operations so the resources are focused at critical tasks.

7.2 Evacuation and Preparation for Evacuation

ISPS Code (A/16.3.5):

A.16.3 Such a plan shall be developed taking into account the guidance given in Part 'B' of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.5 procedures for evacuation in case of security threats or breaches of security

Guidance:

Procedures for evacuation to be established. It is recommended that already existing procedures for evacuation of the terminal are used and amended as appropriate. An evacuation procedure should include:

- Evacuation signal (alarm)
- Who should evacuate at different incidents/types of alarm
- Escape routes for the different areas and identification of mustering points.
- Reporting routines (checking that personnel are at mustering point)
- Shut down procedures, closing of and similar activities that shall be performed prior to evacuation.

7.3 Searching and Contact Information to Experts

ISPS Code (B/16.8.12):

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

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

Guidance:

It is recommended that contact is established and agreements made with organisations and instances with appropriate knowledge. Contact data should be listed, and it is recommended that this form a part of the other contact information forming part of section 3. At this section only the procedure for how to make the contact should be included. This can be done in a short table, as follows:

Type of incident	Who should be contacted	Name of contact	Contact phones
Suspicion of illegal goods	*Local police department*	*Sgt. P.O.Lice*	*+44-007-911-999*

7.4 Bomb Threats

Guidance:

It is recommended to make a standard procedure for activities following a bomb threat.

8 Communication Systems

ISPS Code (B/16.3.2, B/16.8.4-5):

B.16.3 All PFSPs should:

.2 the organisation'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;

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

.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;

Guidance:

Describe communication systems for:

- Security personnel internally at the port facility. Typically phones, radio communication, alarm push buttons, alarm bells
- Communication between ship and port facility, e.g. radio, phone, fax.
- Contact with local authorities (e.g. police department), local harbour authorities and Contracting Government.

A typical example of a table is shown below:

	Internal at port facility	Terminal or ship	Police	Harbour authorities	Contracting Government
Radio					
Alarm push button					
Normal phone					
Mobile phone					
Fax					

Further it should be described how communications are solved in situations where e.g. phone lines are lost.

9 Inspection and Maintenance of Security Equipment

ISPS Code (B/16.8.7):

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

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

Guidance:

The following should be described:

- How to ensure that the effectiveness of all security equipment is in accordance with the intentions.
- Maintenance of equipment.
- Methods of identifying equipment failure or malfunction.
- Temporary measures to be initiated upon equipment failure to ensure port facility security.

It is recommended to make reference to the equipment operation and maintenance manuals. An example of temporary measures can typically be to replace a failing surveillance camera with patrolling guard/s.

ACCESS TO THE PORT FACILITY

SECURITY LEVEL 1

The PFSP should establish control points where the following security measures may be applied: B16.17

- restricted areas, which should be bounded by fencing or other barriers to a standard which should be approved by the Contracting Government; B16.17.1
- checking identity of all persons seeking entry to the port facility in connection with a ship, including ship's personnel and visitors, confirming their reasons for doing so by checking, for example, joining instructions, boarding passes, work orders, etc.; B16.17.2
- checking vehicles used by those seeking entry to the port facility in connection with a ship; B16.17.3
- verification of the identity of port facility personnel and those employed within the port facility and their vehicles; B16.17.4
- restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity; B16.17.5
- undertaking searches of persons, personal effects, vehicles and their contents; B16.17.6
- identification of any access points not in regular use, which should be permanently closed and locked. B16.17.7
- 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, ship's personnel should not be required to search their colleagues or their personal effects. Any such searches shall be undertaken in a manner, which fully takes into account the human rights of the individual and preserves their basic human dignity. B16.18

SECURITY LEVEL 2

The PFSP should establish the additional security measures to be applied, which may include: B16.19

- assigning additional personnel to guard access points and patrol perimeter barriers; B16.19.1
- limiting the number of access points to the port facility, and identifying those to be closed and the means of adequately securing them; B16.19.2
- providing for means of impeding movement through the remaining access points, e.g. security barriers; B16.19.3
- increasing the frequency of searches of persons, personal effects, and vehicles; B16.19.4
- denying access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; B16.19.5
- using patrol vessels to enhance waterside security. B16.19.6

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 that could be taken by the port facility, in close co-operation with those responding and the ships at the, port facility, which may include: B1620

- suspension of access to all, or part, of the port facility; B16.20.1
- granting access only to those responding to the security incident or threat thereof; B16.20.2
- suspension of pedestrian or vehicular movement within all, or part, of the port facility; B16.20.3
- increased security patrols within the port facility, if appropriate B16.20.4
- suspension of port operations within all, or part, of the port facility; B16.20.5
- direction of vessel movements relating to all, or part, of the port facility; B16.20.6
- evacuation of all, or part, of the port facility. B16.20.7

RESTRICTED AREAS

SECURITY LEVEL 1

The PFSP should establish the security measures to be applied to restricted areas, which may include: B16.27

- provision of permanent or temporary barriers to surround the restricted area, whose standard should be accepted by the Contracting Government; B16.27.1
- 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; B16.27.2
- providing passes which must be displayed to identify individual entitlement to be within the restricted area; B16.27.3
- clearly marking vehicles allowed access to restricted areas; B16.27.4
- providing guards and patrols; B16.27.5
- providing automatic intrusion-detection devices, or surveillance equipment or systems to detect unauthorized access into, or movement within, restricted areas; and B16.27.6
- control of the movement of vessels in the vicinity of ships using the port the port facility. B16.27.7

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: B16.28

- enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion-detection devices; B16.28.1
- reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses; B16.28.2
- restrictions on parking adjacent to buildings, storage, and berthed ships; B16.28.3
- further restricting access to the restricted areas and movements and storage within them; B16.28.4
- use of continuously monitored and recording surveillance equipment; B16.28.5
- enhancing the number and frequency of patrols, including water-side patrols, undertaken on the boundaries of the restricted areas and within the areas; B16.28.6
- establishing and restricting access to areas adjacent to the restricted areas; B16.28.7
- enforcing restrictions on access by unauthorized craft to the water adjacent to ships using the port facility. B16.28.8

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 that could be taken by the port facility, in close co-operation with those responding and the ships at the, port facility, which may include:

- 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; B16.29.1
- preparing for the searching of restricted areas as part of a search of all, or part, of the port facility. B16.29.2

HANDLING OF CARGO

SECURITY LEVEL 1

The PFSP should establish the security measures to be applied during cargo handling, which may include: B16.32

- routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations; B16.32.1
- checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation; B16.32.2
- searches of vehicles; B16.32.3
- checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility; B16.32.4
- Checking of cargo may be accomplished by some or all of the following means;
  - visual and physical examination;
  - using scanning/detection equipment, mechanical devices, or dogs; B16.33
- 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 concerned. B16.34

SECURITY LEVEL 2

The PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include: B16.35

- detailed checking of cargo, cargo transport units and cargo storage areas within the port facility; B16.35.1
- intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and is then loaded onto the ship; B16.35.2
- intensified searches of vehicles; B16.35.3
- increased frequency and detail in checking of seals and other methods used to prevent tampering. B16.35.4
- detailed checking of cargo may be accomplished by some or all of the following means: B16.36
- increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination); B16.36.1
- increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; B16.36.2
- co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures. B16.36.3

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 that could be taken by the port facility, in close co-operation with those responding and the ships at the, port facility, which may include: B16.37

- restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; B16.37.1
- verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location. B16.37.2

DELIVERY OF SHIPS STORES

SECURITY LEVEL 1

The PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include: B16.40

- checking of ship's stores and package integrity; B16.40.1
- advance notification as to composition of load, driver details and vehicle registration; B16.40.2
- searching the delivery vehicle. B16.40.3
- Checking of ship's stores may be accomplished by some or all of the following means: B16.41
- visual and physical examination; B16.41.1
- using scanning/detection equipment, mechanical devices or dogs. B16.41.2

For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship. B16.39

SECURITY LEVEL 2

At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ships stores, which may include: B16.42

- detailed checking of ship's stores; B16.42.1
- detailed searches of the delivery vehicles; B16.42.2
- co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; B16.42.3
- escorting the delivery vehicle within the port facility. B16.42.4
- Detailed checking of ship's stores may be accomplished by some or all of the following means: B16.43
- increasing the frequency and detail of searches of delivery vehicles; B16.43.1
- increasing the use of scanning-detection equipment, mechanical devices, or dogs; B16.43.2
- restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period. B16.43.3

SECURITY LEVEL 3

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 that 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; B16.44

UNACCOMPANIED BAGGAGE

SECURITY LEVEL 1

The PFSP should establish the security measures to be applied when handling unaccompanied to ensure that:

- unaccompanied baggage is screened or searched up to and including 100%, which may include use of x-ray screening. B16.46

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. B16.47

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 that could be taken by the port facility in close co-operation with those responding and the ships at the port facility, which may include:

- subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
- preparations for restriction or suspension of handling of unaccompanied baggage;
- refusal to accept unaccompanied baggage into the port facility. B16.48

SECURITY OF THE PORT FACILITY

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: B16.52

- observe the general port facility area, including shore and Waterside accesses to it; B16.52.1
- observe access points, barriers and restricted areas; B16.52.2
- 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. B16.52.3

SECURITY LEVEL 2

The PFSP should establish the additional security measures to be applied, to enhance the monitoring and surveillance capability, which may include: B16.53

- increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage; B16.53.1
- increasing the frequency of foot, vehicle or waterborne patrols; B16.53.2
- assigning additional security personnel to monitor and patrol. B16.53.3

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 that could be taken by the port facility, in close co-operation with those responding and the ships at the, port facility, which may include: B16.54

- switching on all lighting within, or illuminating the vicinity of, the port facility; B16.54.1
- switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; B16.54.2
- maximizing the length of time such surveillance equipment can continue to record. B16.54.3