OAS More rights for more people

# Verification and Compliance Manual for Port Security Officials

## Drafting Guide

Prepared and published by the Maritime and Port Security Program of the Inter-American Committee against Terrorism (CICTE).

The contents of this publication are presented exclusively for informational purposes and do not represent the official position of the Organization of American States, its General Secretariat, or its Member States.

This publication has been made possible thanks to the financial support of the Government of Canada.

We welcome your interest in this guide. Your feedback on how you have used this guide and whether it helped strengthened maritime and port security would be valuable information we can use to help design future projects.

Please contact CICTE's Maritime and Port Security Program at CICTE@oas.org to share your feedback.

OAS Cataloging-in-Publication Data

Organization of American States. Secretariat for Multidimensional Security. Inter-American Committee against Terrorism.

Verification and compliance manual for port security officials : Drafting guide / [Prepared and published by the Maritime and Port Security Program of the Inter-American Committee against Terrorism (CICTE)].

v. ; cm. (OAS. Official records ; OEA/Ser.D/XXV.29)

ISBN 978-0-8270-7378-4

1. Security, International. 2. Marine terminals--Security measures. 3. Shipping--Security measures. 4. Harbors--Security measures. 5. Terrorism--Prevention. I. Title. II. OAS/CICTE Maritime and Port Security Program. III. Series.

OEA/Ser.D/XXV.29

## CREDITS

**Luis Almagro**
Secretary General
Organization of American States (OAS)

**Arthur Weintraub**
Secretary for Multidimensional Security
Organization of American States (OAS)

**Alison August Treppel**
Executive Secretary
Inter-American Committee against Terrorism
Organization of American States (OAS)

**Violanda Botet**
Deputy Executive Secretary
Inter-American Committee against Terrorism
Organization of American States (OAS)

**Lisbeth Laurie**
Maritime and Port Security Program Manager
Inter-American Committee against Terrorism
Organization of American States (OAS)

**John Platts**
**Ivan Rice**
Co-Authors

**Jared Greenwood**
Graphic Design

# Contents

# Preface

This Drafting Guide has been developed as an aid for government agencies responsible for the security of ports. Specifically, this Guide will help them consolidate relevant national regulations, policies and procedures into a single Manual with authoritative guidance on how port security officials should perform their duties.

The potential benefits of such a document arose from the results of numerous assessments and training courses conducted by the Secretariat of Inter-American Committee against Terrorism (CICTE) under its Maritime and Port Security Program. These initiatives have revealed that government officials with port security responsibilities often use training course materials or the International Maritime Organization's (IMO) *Guide to Maritime Security and the ISPS Code, 2012 Edition* (which has been widely distributed to national authorities in the Organization of American States Member States (OAS)), as reference documents. As these are generic in nature and may not reflect current regulatory practices, it can lead to inconsistencies in how officials verify the extent to which ports and port facilities are meeting their mandatory security requirements; or how incidents of non-compliance are addressed.

In developing this Guide, it was recognized that each country's approach to port and maritime security is unique. Thus, it has been structured so that it can be easily adapted to give government officials within each country a concise yet informative context for the conduct of their port security responsibilities. Some of the text and forms in this document resemble material in the above-noted IMO Guide which, in turn, relied on the International Ship and Port Facility Security (ISPS) Code and its related guidance material.

The CICTE Secretariat would like to acknowledge the contributions of Global Affairs Canada which provided the funding for this initiative through its Anti-Crime Capacity Building Program; and Transport Canada's Maritime and Port Security Program for providing access to its verification and compliance procedures and forms which have been adapted for use in this Guide.

***Alison August Treppel***
Executive Secretary
CICTE Secretariat
December 2021

# Overview of Drafting Guide

## 1. Target Audience

The contents of the proposed Manual are for government officials within departments and agencies who are responsible for overseeing the implementation of the ISPS Code and related security measures and standards, as they pertain to port facility security. Generally, these officials are located in their country's Designated Authority (see definition in Section 5 below).

## 2. Scope

The Manual covers the following areas of responsibility:

- The conduct, review and approval of port facility security assessments (PFSAs) and updates;
- The review and approval of port facility security plans (PFSPs) and updates;
- The conduct of security verification activities at port facilities falling under the ISPS Code (or at facilities not so designated but used on an occasional basis by ships falling under the ISPS Code); and
- The undertaking of actions to address incidents of non-compliance resulting from verification activities.

Its scope also encompasses aspects of a Designated Authority's work environment in terms of organizational structure, enabling legislation, verification program objectives, code of good practice, delegation of regulatory authority, delineation of authorities and responsibilities, and training requirements. However, it ***excludes*** the following port security elements which, although important, are not mandatory under the ISPS Code. They could be added if so desired by the Designated Authority:

- Port-wide security assessments and plans;
- Security guidelines for smaller port facilities (e.g. marinas and harbors);
- Design and delivery of security awareness programs; and
- Training of port facility security officers (PFSOs) and other port personnel.

# 3. Content Adaptability

The aim of this Drafting Guide is to provide Designated Authorities in OAS Member States with a template that can easily be adapted to reflect their particular regulatory framework, governance structure and operational procedures.

It should be noted that phrases such as "Inspectors may be authorized to ..." and "Suggested Good Practices for Inspectors", as well as references to sample documents and forms, are **not** intended to replace either the existing responsibilities assigned by Designated Authorities to their Inspectors, or any documents and checklists that may have been developed.

Wherever practical, experience-based adjustments have been made to the text and forms extracted from the sources on which this Guide is based, so as to provide relevant and up-to-date contextual material for the activities potentially being performed by government officials.

# 4. Format

The proposed Manual has been formatted to provide a basis for Designated Authorities to develop a customized work instrument for their officials who have 'front-line' port facility security responsibilities, including the interface with both domestic-registered and foreign-flagged ships using port facilities under their jurisdiction. It has two Parts:

- ***Part I – General:***
  - » Summarizes a Designated Authority's governance structure, management framework and work environment for its officials.
- ***Part II – Port Facilities:***
  - » Summarizes the mandatory security requirements for port facility operators under the ISPS Code;
  - » Describes the various activities associated with the conduct, review and approval of PFSAs and PFSPs; with verifying that port facility operators keep their approved plans updated and maintain compliance with them; and with taking appropriate action to address incidents of non-compliance;
  - » Summarizes other relevant activities available to Designated Authority officials such as: participation in Port Security Committees; monitoring security measures at occasional use port facilities; and involvement with the information exchange networks of Port Facility Security Officers.

# 5. Terminology

Throughout the Guide, the following terms have been used for consistency and simplicity. However, they may not reflect the terminology used by individual Designated Authorities.

- *Applicable Legislation* denotes the legal framework enabling the implementation of the ISPS Code and related security measures.
- *Contracting Government* means a Government that has agreed to be bound by the International Convention for the Safety of Life at Sea, 1974 (referred to as the SOLAS Convention), which is the enabling document for the ISPS Code.
- *Designated Authority* refers to the organization within a Government recognized by the IMO as being responsible for ensuring the implementation of the ISPS Code and related security measures as they relate to port facility security and the ship/port interface from the point of view of the port facility.
- *Inspector* denotes an official within the Designated Authority who is responsible for undertaking verification activities. Although the IMO Guide defines the term - Duly Authorized Officer - as "*a Government official given specific authorization to undertake official duties, usually associated with inspection and enforcement activities*", Inspector is a generic term covering port security inspectors, compliance officers and other authorized officials.
- *Verification* denotes the type of activity carried out by Inspectors to ensure that the Designated Authority's obligations under the ISPS Code are met. The term covers audits, inspections, reviews and follow-on compliance actions typically associated with the issuance, maintenance and renewal of security certificates required by port facilities.

# 6. Reference Material

Since this Guide is intended to serve as a basis for providing government officials with a single document that consolidates the direction and guidance needed to carry out their verification duties under the regulatory framework linked to applying the ISPS Code and related security measures, the inclusion of reference material produced by external organizations has been limited to the IMO's Guide to Maritime Security and the ISPS Code, 2012 Edition (IMO Guide).

# Part I - General

## I-1 Purpose

This section could consist of a brief explanation of the aims of this Manual. A short statement along the following lines is suggested:

*"To provide Inspectors and other officials with a single consolidated source of the regulations, policies and procedures essential to the performance of their duties."*

## I-2 Scope

This section could outline in general terms the main work areas and activities of the Port Security Program that are covered by the Manual. Generally speaking, these are the authorities and responsibilities assigned to Inspectors and other officials in a country's Designated Authority as identified in the ISPS Code and include activities related to:

- The approval of PFSAs, PFSPs and their updates;
- Monitoring compliance with approved PFSPs; and
- Addressing incidents of non-compliance by port facility operators.

In addition, the scope could include activities that, while not mandatory under the ISPS Code, help to strengthen a country's port security framework. Examples include:

- Participation in Port Security Committees;
- Monitoring security measures at port facilities occasionally used by ships on international voyages; and
- Involvement with PFSO information exchange networks.

*NOTE: This manual does not include specific guidance regarding other port security programs beyond the ISPS Code. Many countries have additional port security-related programs in place such as cargo security programs. Additionally, this manual does not address international cargo security standards and frameworks such as the World Customs Organization's SAFE Framework or ISO 28000.*

# I-3 Abbreviations

This section could list abbreviations that are frequently used by a Designated Authority (DA), including:

- DOS – Declaration of Security
- OJT – On-the-Job Training
- PFSA – Port Facility Security Assessment
- PFSO – Port Facility Security Officer
- PFSP – Port Facility Security Plan
- RSO – Recognized Security Organization
- SOC – Statement of Compliance (for a port facility)

# I-4 The ISPS Code

This section could provide the context for the verification requirements addressed by this Manual, as well as the enabling legislation in each country. A short statement along the following lines might be considered:

> "After the tragic events of September 11, 2001, the IMO began to consider the vulnerabilities of shipping being used for terrorist activity. This led to a Diplomatic Conference on Maritime Security being held at the London headquarters of the IMO in December 2002. It was attended by this country [NOTE: insert delegation details as appropriate] as one of 109 Contracting Governments to the SOLAS Convention. The Conference adopted a number of security-related amendments to this Convention, the most far-reaching being the ISPS Code which was scheduled to take effect just 18 months later, on July 1, 2004.
>
> The ISPS Code is divided into a mandatory Part A and a Part B which recommends how to implement the requirements specified in Part A. It contains detailed security requirements for Governments and port facility operators. Those that may be directly relevant to Inspectors include:
>
> - Ensuring completion and approval of PFSAs and any subsequent amendments;
> - Approving PFSPs and any subsequent amendments; and
> - Testing approved plans."

# I-5 Enabling Legislation

This section could:

- Outline the Government's legislative framework for maritime security. Depending on the country, this may take the form of a Presidential Decree or Ministerial Directive enabling the implementation of the ISPS Code; or a broader-based Act and subordinate Regulations dealing specifically with maritime, port and/or transportation security.
- Make specific reference to the sections which authorize Inspectors and other officials to perform their port security duties. This could be in the form of an overview with the legal text placed in an appendix. Where a DA has published an approved set of Port Security Regulations as a separate document, it may be more practical to keep it separate from this Manual rather than include it as a lengthy annex.

# I-6 Organizational Structure

It is important for Inspectors and other officials to understand both where their positions fit within a DA, and where the DA is located within the Contracting Government's overall structure. Typically, it is either a key organization within a Government department, or a separate agency outside the department but reporting to the leadership of that department. In most cases, it should be possible to describe the organizational structure using a three (3) tiered organogram showing:

- The DA's location within the Government's overall structure;
- How the DA is structured; and
- Details of the unit(s) in which the Inspectors are based.

To provide a context for the working environment of the Inspectors, this section could also briefly describe non-legislative instruments which govern how the DA functions. These may include:

- Security roles and responsibilities of other departments and agencies with an operational presence at ports or in adjacent territorial waters (e.g. Coast Guard, Customs, Immigration, Intelligence Services and Law Enforcement);
- Security roles and responsibilities of (public) port administrations;
- Mission statement, and strategic and annual plans;
- Any statutory or regulatory overlaps between agencies, or requirements for coordination, and
- Policies and principles governing the work environment (see following sections).

# I-7 Program Objectives

The intent of this section is to provide Inspectors and other officials with a general understanding of what the Program is seeking to accomplish. If included, the content could be extracted or adapted from higher level documents governing the role of the DA (e.g. an agency or departmental strategic plan). The following five (5) Objectives are examples of high-level statements providing insight into a DA's approach to applying its verification program:

- To maintain a consistent and risk-based approach to certifying that port facilities continue to operate in compliance with the ISPS Code;
- To address incidents of non-compliance by port facilities using such facilities in a prompt and consistent manner;
- To fairly and effectively determine whether corrective action is already in progress or further action is required;
- To employ a graduated and proportionate approach to applying corrective action, with due consideration for the frequency and seriousness of the non-compliance; and
- To promote a security culture by emphasizing, through education and awareness, the benefits of a maritime transportation system that is compliant with the ISPS Code.

# I-8 Inspector Authorities and Responsibilities

This section could lay out the powers and any authorizations that are delegated to Inspectors through legislation, policy or directives. Possible examples may include the authority to:

- Enter and inspect any port facility to verify compliance with legislation governing the implementation of the ISPS Code;
- Interview or require any person to attend a verification for the purposes of ensuring compliance;
- Require the regulated port facility to produce and submit copies of any documents that may contain information relevant to compliance;
- Seize material evidence during a verification; and
- Detain any ship that, on clear grounds, is believed to be a threat to the port facility.

This section could also detail the potential responsibilities of Inspectors. If not already formalized, the following list, which has been adapted from sections 2.16.3 of the IMO Guide, could serve as a template for establishing an approved set of responsibilities:

- Advising on and Overseeing, the implementation of the ISPS Code at port facilities including those that are occasionally used by ships falling under the ISPS Code;
- Consulting port facility operators and on-port companies on security issues;
- Monitoring responsiveness to changes in the Security Level at port facilities;
- Monitoring the activities and outputs of Recognized Security Organizations (RSO) authorized by the DA to undertake tasks related to port facility security;

- Advising on security threats;
- Reviewing and Approving PFSAs, including those undertaken by RSOs;
- Monitoring compliance with Declaration of Security (DOS) procedures;
- Determining and Monitoring the requirements for port facilities to report security incidents;
- Monitoring the retention of security documents and records by port facility operators;
- Advising on the preparation and content of PFSPs;
- Reviewing and Approving PFSPs, and determining the types of amendments to an already approved plan that require submission for approval;
- Undertaking verification activities relating to the issuance and endorsement of security certificates [e.g. Statement of Compliance (SOC)] and;
- Undertaking verifications of port facilities using such facilities to assess their compliance with applicable legislation.

# I-9 Inspector Qualification Process

This section could outline the specific qualifications and training requirements for Inspectors. This might include:

## I-9.1 Credentialing

To ensure that Inspectors are adequately qualified to carry out their duties, it is suggested that a formal credentialing process be established. This would link the authorities and responsibilities delegated to an Inspector with the successful completion of specific, pre-determined elements of an approved training curriculum.

Given that Inspectors are required to present their authorizations to access a port facility to conduct their verification activities, it is important that those authorizations are clearly listed on their credentialing document or badge.

## I-9.2 Training Curriculum

A multi-phase approach to inspector training is increasingly being adopted by DAs in the OAS region and elsewhere. This approach has the benefit of gradually increasing the authorities and responsibilities delegated to a newly-hired Inspector commensurate with the level of knowledge and competencies gained. The core training elements could include the following 12 listed in section 2.16.6 of the IMO Guide:

- Knowledge of the DA's legislative framework;
- Knowledge of the international maritime security framework;
- Knowledge of the port industry over which the authority has jurisdiction;
- The responsibilities of the DA specified in the ISPS Code;
- The responsibilities delegated to Inspectors;
- Code of Good Practice;
- Description of the DA's port security verification program;
- Procedures for preparing, conducting and reporting the results of verifications;
- Procedures for handling cases of non-compliance;
- Procedures for observing or participating in exercises;
- Procedures for issuing, renewing, suspending and withdrawing certificates and other forms of authorization; and
- Procedures for conducting awareness and education activities with port industry and labour associations, port security committees and the public.

These and other training elements can be delivered through workshops organized internally or by external organizations. The means of delivery can vary, and include: formal classroom training, online training or e-learning, On-the-Job Training (OJT), and one-to-one coaching. It is suggested that a phased approach be adopted, as illustrated in the example below of a training curriculum for a newly-hired Inspector:

***Phase I*** – The new hire would be assigned to shadow an experienced Inspector who had received training in coaching. During this short orientation period, the new hire would have no delegated authority.

***Phase II*** – The orientation period would lead into a series of online training modules coupled with OJT. Once successfully completed, the individual would receive a Level I credential, authorizing access to enter a port facility for the purpose of inspection accompanied by a regular, fully credentialed Inspector.

***Phase III*** – This phase requires the completion of a formal classroom course on verification techniques coupled with 1-2 series of OJT. Successful completion would result in a Level 2 credential that authorizes the individual to access any port facility in the exercise of all authorities and responsibilities delegated to an Inspector.

***Phase IV*** – This phase would be discretionary, and could involve more advanced training on specialized topics (e.g. conducting PFSAs).

***Phase V*** – This phase would involve Refresher training and continuing professional development on a periodic basis to ensure that the Inspector maintains a high degree of competence. Ideally, such training should incorporate all new or amended verification policies and procedures.

# I-10 Information Management and Protection

This section may be used to describe the flow of information within the DA, as well as how security-related information is to be handled by Inspectors in the course of their duties. Any policies and procedures related to maintaining the confidentiality, availability, and integrity of information systems and communications technology from a cyber security standpoint could also be included.

## I-10.1 Distribution

It is a useful practice for the DA to keep its Inspectors informed of changes or clarifications on how they are to exercise their duties. This may be efficiently achieved through the regular and timely issuance of bulletins and/or amendments to this Manual, on an as-needed basis. These might focus on new or amended verification policies and procedures, or interpretations of existing policies and regulations dealing with the identification and handling of non-compliances.

Often, such information is considered to be confidential and not to be shared with regulated entities. In such cases, it may be appropriate to provide information on regulatory changes outlining new or amended policies and procedures, but omitting details of directives issued to Inspectors on how they should exercise their responsibilities.

## I-10.2 Handling

If applicable, this section could provide direction and guidance on how Inspectors should handle and protect any information that they receive which:

- Is potentially covered by legislation relating to rights to Privacy or Access to Information;
- Are security-sensitive intelligence products.

In such cases, Inspectors need to know what their responsibilities are, especially in terms of how to protect the information and disseminate it to port facility operators on a need-to-know basis.

## I-10.3 Record Keeping

This section could detail any direction to Inspectors regarding their record keeping (i.e. e-mail exchanges, completed forms, checklists, and notes of conversations). An example of such direction is shown below:

"Inspectors should ensure that:

- Records are legible, accurate, complete and properly labeled;
- Communications related to mandatory security requirements such as PFSPs are confirmed in writing and placed in the applicable record; and
- The documentation process is followed by:
    - » Indicating the dates on which each document was received and reviewed;
    - » Stamping all correspondence with the date of receipt;
    - » Identifying who conducted the review and indicating the results; and
    - » Properly storing all required documentation in the appropriate file or location."

# I-11 Liability

This section could describe any legal obligations that require Inspectors to exercise their authorities and responsibilities in a responsible manner (i.e. to perform their duties to the best of their ability within available resources). Failure to meet these obligations could result in port facility operators claiming that they have suffered damage caused by carelessness or over-zealousness in the conduct of verification activities. Such claims carry the risk of Inspectors and their DA being named as defendants in civil actions for damages before the courts. Additional topics to be covered in this section could include:

- Conditions under which Inspectors receive government protection from civil liability by any act or omission in performing their duties;
- Describing the extent of government protection; and
- Identifying verification activities deemed to be potentially careless (e.g. not following-up after observing a security guard who is not verifying the identity of an individual seeking to enter a port facility), or over-zealous (e.g. detaining a port worker after being observed in an unsecured restricted area even though there were no clear grounds to believe that the individual was posing a threat).

# I-12 Code of Conduct

This section could identify any conduct that the DA has determined to be applicable to its Inspectors. In the absence of such a Code for government officials, consideration could be given to establishing one that is based on the Code of Good Practice for Port State Control Officers Conducting Inspections within the Framework of the Memorandum of Understanding on Port State Control in the Asia-Pacific Region. It was issued in 2007 and is known as the Tokyo MOU. This 28-point Code is based on the following three principles, all of which can govern the actions of Inspectors:

- ***Integrity***, or the state of moral soundness, honesty and freedom from corrupting influences or motives;
- ***Professionalism***, including the application of accepted professional standards of conduct and technical knowledge; and
- ***Transparency***, implying openness and accountability.

Although the focus of the Tokyo MOU Code is on the actions and behavior expected of Port State Control Officers on-board ships, many of its 28 points are applicable to Inspectors. This is illustrated by the template below, which has been adapted directly from that list.

"Inspectors should:

- Use their professional judgement in carrying out their duties;
- Respect the authority of port facility operators;
- Be polite but professional and firm as required;
- Never become threatening, abrasive or dictatorial or use language that may cause offence;
- Expect to be treated with courtesy and respect;
- Comply with all health and safety requirements of the port facility (e.g. by wearing personal protective clothing), and not take any action or cause any action to be taken which could compromise their safety or that of port facility personnel;

- Comply with all security requirements of the port facility and wait to be escorted around the port facility by a responsible person;
- Present their identity cards at the start of a verification;
- Explain the reason for the verification. However, if it is triggered by a report or complaint, they must not reveal the identity of the person making the complaint;
- Apply the applicable legislation in a consistent and professional way and interpret its clauses pragmatically when necessary;
- Request port facility personnel to demonstrate the functioning of equipment or operational activities (e.g. drills);
- If unsure of a requirement or of their findings, avoid making an uninformed decision by seeking advice from colleagues;
- Where it is safe to do so, accommodate the operational needs of the port facility;
- Clearly explain the findings of the verification and the corrective action required to the PFSO;
- Issue a legible and comprehensible inspection report to the PFSO before leaving the port facility, and ensure that it is clearly understood;
- Deal with any disagreement over the conduct or findings of the verification calmly and patiently;
- Advise the PFSO of the complaints and appeals procedures if the disagreement cannot be resolved within a reasonable time;
- Be independent and not have any commercial interest in the port facilities that they inspect, or companies providing services to those port facilities.
- Be free to make decisions based on the findings of their verifications and not on any commercial considerations;
- Always follow the rules of their DA regarding the acceptance of gifts and favors;
- Firmly refuse any attempts of bribery and report any blatant cases to the DA;
- Not misuse their authority for benefit, financial or otherwise; and
- Update their technical knowledge regularly."

## I-13 Occupational Health and Safety

As Occupational Health and Safety (OHS) is an important aspect of all work environments, this section could describe the OHS requirements in the workplace for Inspectors. For the sake of clarity, it could be broken into the following two sub-sections:

- ***Safety Rules for Inspectors***, which describe the rules and identify the safety equipment (e.g. high visibility clothing, personal floatation device, gloves, safety boots, eye and hearing protection, head gear, breathing apparatus) that must be worn by Inspectors in the conduct of their duties. Further, these rules should include required training and certifications that may be required by government organizations.
- ***Marine Environmental Hazards***, which are commonly found in port facilities (e.g. the tracks for large cranes at container terminals). It could also describe how to mitigate these hazards when entering port facilities (e.g. avoid parking their vehicle on guide tracks used by cranes).

# Part II – Port Facilities

## II-1 Mandatory Security Requirements for Port Facilities

This section could be included as a basis for providing Inspectors with background information on the link between their various verification activities and the obligations of port facility operators under the ISPS Code. Each operator is required to:

- Appoint a PFSO;
- Provide the PFSO with adequate training and support;
- Contribute to the conduct of PFSAs;
- Prepare a PFSP and any subsequent updates, and submit to the DA for approval;
- Ensure that the PFSP is protected from unauthorized access or disclosure;
- Ensure that the PFSP is effectively implemented by carrying out internal audits, drills and exercises at appropriate intervals;
- Comply with Government-initiated changes in Security Level;
- Initiate or respond to a DOS; and
- Report security incidents to the DA.

In addition, the port facility operator should:

- Advise the DA of any seafarer access and shore leave issues; and
- Participate in Port Security Committees.

# II-2 Port Facility Security Assessment (PFSA) Activities

## II-2.1 Scope and Complexity of PFSAs

If included, this section could provide Inspectors with useful background information on the importance of PFSAs in establishing effective security regimes at port facilities under their jurisdiction as well as a context for their various activities in conducting, updating and reviewing assessments of security at those facilities.

The ISPS Code specifies that the DA is responsible for carrying out PFSAs or else authorizing RSOs to do so on its behalf. The PFSA may be considered to be a risk analysis of all aspects of a port facility's operations in order to determine which parts of it are more susceptible, and/or more likely, to be vulnerable. It is required to include the four elements in the chart below, each of which plays a critical role in the assessment process.

| Element | Provides a basis for: |
|---|---|
| Identifying critical assets & infrastructure | Prioritizing their importance |
| Identifying possible threats to each one & estimating their likelihood of occurrence | Evaluating vulnerabilities to each threat and prioritizing security requirements |
| Identifying weaknesses in the infrastructure, policies and procedures | Establishing options to eliminate or mitigate identified vulnerabilities |
| Selecting, prioritizing and assessing the effectiveness of mitigation measures | Implementing the most cost-effective measures |

In order to address these elements within a risk management framework, a complex, multi-phase technique must be applied. As its successful application requires specialized training, neither the conduct nor the review of PFSAs (whether prepared by the DA or RSO) are generally responsibilities assigned to Inspectors. However, as shown in the following two sections, Inspectors can play important roles on teams established by the DA to perform these functions.

### II-2.2 Conducting and Updating PFSAs

This section addresses the activities that could be undertaken by Inspectors in preparing for a PFSA or PFSA Update, and conducting on-site assessments.

In practice, the undertaking of PFSAs requires the involvement of PFSOs, given their in-depth knowledge of the port facility's assets, infrastructure, vulnerabilities and past security incidents. Thus, an Inspector assigned to a port facility for verification activities is well-placed to serve as an intermediary between the assessment team and the PFSO during the early phases of a PFSA, as indicated below:

### II-2.2 (a) Preparation

This initial step involves extensive planning and coordination between the assessment team manager and the PFSO. A standard questionnaire may be developed by the DA and sent to the PFSO to assist the team in understanding the facility, its operations and its critical assets. It could also include a review of any threat assessment information that might be available. Inspectors could usefully serve in this coordination role by advising the PFSO on how the assessment is to be conducted, as well as dealing with any queries regarding the completion of the questionnaire.

### II-2.2 (b) Conducting the On-site Assessment

This phase typically consists of the following components:

- Identifying what areas, assets, information and processes need to be protected including the waters adjacent to the port facility;
- Identifying threats that could reasonably impact the critical assets and operations of the facility, or whose potential existence presents a vulnerability to the facility;
- Reviewing for potential vulnerabilities:
  - » Changes in the port facility's operations since the last PFSA;
  - » Responses to any security incidents that may have occurred since the last PFSA; and
  - » The port facility's existing security program.
- Prioritizing the impact of the above in terms of the facility's exposure to risk; and
- Identifying opportunities to reduce vulnerabilities through improved security practices.

Inspectors could usefully assist the team by leveraging their in-depth knowledge of security operations gained through their various verification activities. Further, Inspectors may be optimally positioned to coordinate meetings between the assessment team and other government agencies that may provide important information, such as intelligence agencies or law enforcement.

### II-2.3 Reviewing RSO-Prepared PFSAs and Updates

This section addresses the activities that could be undertaken by Inspectors in the process of reviewing PFSAs and PFSA Updates prepared by RSOs.

Many DAs continue to appoint RSOs to conduct PFSAs on their behalf. In such cases, it is important for a DA to establish a rigorous review and approval process to ensure that the PFSA has been performed to a satisfactory standard, and that its findings and recommendations provide a sound basis for the develop-

ment of the PFSP by the port facility operator. Inspectors can play an important role in the review process by verifying that the submitted PFSA:

- Addressed all key elements (e.g. physical security and telecommunication systems);
- Identified and evaluated important assets and infrastructure on both the landside and waterside of the facility;
- Involved consultation with relevant authorities relating to structures adjacent to the port facility which could:
  - » Cause (or be used to cause) damage within the facility; or
  - » Be used for illicit observation of the facility or for diverting attention.
  - » Identified possible threats to the assets and infrastructure, and the likelihood of their occurrence;
- Involved 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 of an attack in terms of loss of life, damage to property and economic disruption including to transport systems;
  - » The capability and intent of those likely to mount such an attack; and
  - » The possible types of attack.
- Considered all possible threats including a wide range of security incidents on the shoreside (e.g. damage to, or destruction of, the port facility or a visiting ship by explosive devices, arson, sabotage or vandalism) or waterside (e.g. blockage of port entrances, locks, approaches);
- Identified a wide range of vulnerabilities such as deficiencies in:
  - » Access controls in place for the facility, restricted areas on the facility, and on to ships berthed at the facility;
  - » Perimeter security on both the shoreside and waterside of the facility;
  - » Training programs of security personnel; and
  - » Monitoring security equipment.
- Prioritized countermeasures and procedural changes and their level of effectiveness in reducing vulnerabilities.

Given the level of complexity in conducting PFSAs, unless Inspectors have received specialty training, they should not be expected to review the application of the risk management technique for accuracy and completeness. Rather, their important contribution could be to verify whether or not the RSO has carried out the component steps of the assessment. In support of this role, it is suggested that the DA could prepare a checklist covering the points identified above. A sample PFSA Review Checklist is shown in Annex II-1. It may be adapted by the DA, as deemed appropriate.

# II-3 Port Facility Security Plan (PFSP) Approval and Verification Activities

## II-3.1 Reviewing and Approving PFSPs and Updates

This section addresses the activities that could be undertaken by Inspectors in the process of reviewing and approving Initial PFSPs and their subsequent updates.

### II-3.1 (a) Review and Approval of Initial PFSPs

Once a port facility has received its approved PFSA report, the PFSO is then responsible for writing a PFSP and submitting it for approval. The DA is responsible for ensuring that the PFSP is based on the findings of the PFSA and compliant with the applicable legislation enabling the ISPS Code. Inspectors can play an important role in this review process by using a PFSP Approval form. Annex II-2 provides a sample form which can be easily adapted by a DA to suit its approval process.

In undertaking a review, factors to be considered by Inspectors could include verification that:

- The vulnerabilities identified in the PFSA have been mitigated;
- Appropriate security measures to mitigate potential security risks have been established; and
- Any advice, direction or guidance materials issued by the DA have been heeded.

On completion of their review, Inspectors could be authorized to:

- Return the plan to the PFSO with a letter identifying areas that require improvement, if the Inspector determines that it is not strong enough or does not conform to the applicable legislation;
- Approve the plan on behalf of the DA or recommend it for approval by a higher authority within the DA, if the Inspector considers the PFSP to be compliant;
- When re-submitted by the PFSO, check the whole plan against the previous review to ensure that previously-approved items were not changed; and
- Retain a controlled copy (which must be protected against unauthorized access), as this helps to maintain the integrity of the PFSP and prevent any unauthorized amendments or modifications.

If the DA has developed a standard approval form/letter (which may take the form of an Interim SOC), it could usefully be included as an annex to the Manual.

### II-3.1 (b) Review and Approval of PFSP Updates

During the validity period of an approved PFSP, events may occur that invalidate or weaken its security measures and procedures. In such cases, an amendment could be initiated by the PFSO or DA. Examples of when a PFSP should be reviewed to see if it needs updating include when:

- The PFSA relating to the port facility has been amended;
- An independent audit or verification activities by the DA have identified deficiencies in the security framework, or questioned the continuing relevance of significant elements in the plan;
- Security incidents or threats have involved the port facility; and

- There have been substantial changes to operations, ownership or operational control.

If any of the above events result in the PFSP being amended by the PFSO and, as specified in the ISPS Code, submitted for approval before they are implemented, Inspectors could be authorized to conduct:

- A partial review if the amendments are minor (to ensure that the amended items comply with the applicable legislation); or
- A thorough review utilizing the PFSP Approval form adopted by the DA, if the amendments are complex or cover multiple areas of the PFSP.

The post-review activities of Inspectors would be the same as for an Initial PFSP (refer to section II-3.1 (a) above).

## II-3.2 Types of Verification Activity

Many countries have established their port facility security verification activities after those required by ships (which provides consistency for DAs in their regulatory oversight of each entity). This section could provide background information for Inspectors on the types of verifications that they may be authorized to undertake, and their inter-relationships.

Over the life cycle of a SOC (or equivalent certificate), there are four (4) types of verification that DAs could conduct to ensure that the port facility continues to operate in accordance with applicable legislation and its approved PFSP. They are:

- Initial (Pre-Certification) Verifications, which are conducted after the PFSP has been approved but before the SOC is issued. Its purpose is to verify that the PFSP has been fully implemented and that the port facility is operating in accordance with the measures and procedures specified in the PFSP;
- Intermediate Verifications, which are typically conducted mid-way through the SOC's validity period (i.e. Year 3 if it has a 5-year validity period which many DAs have adopted as a standard). Its purpose is to verify continued compliance with applicable legislation and the approved PFSP;
- Renewal Verifications, which begin a new cycle. To provide sufficient time for the verification process to be completed before the SOC's validity period expires (to avoid the need for extending its validity period), many DAs require the submission of an updated PFSP for approval well in advance of the expiry date (e.g. at least 60 days). Advance notice also provides time for the PFSA to be reviewed and updated (refer to section 3.4). Following approval, a Renewal Verification is performed to verify continued compliance with the applicable legislation and the full implementation of the approved PFSP; and
- Additional Verifications, which may be performed at any time during the SOC's validity period for several reasons including:
    - » Cause (e.g. in response to a poor compliance history or a complaint);
    - » Verification of Opportunity (e.g. the facility may have had breaches of security or, during a verification of a ship berthed at the facility, an Inspector may have noted a lack of access control at the port facility); or
    - » Follow-up to an unsatisfactory Intermediate Verification.

## II-3.3 Initial (Pre-Certification) Verifications

This section addresses the activities that could be undertaken by Inspectors at each stage of an Initial Verification – Preparation, Conduct, Follow-up Action; and Response to Results.

## II-3.3 (a) Preparation

Inspectors may be authorized to perform the following activities when preparing for a security verification:

- Review the approved PFSP, including any amendments and relevant legislation;
- Review any information contained in any relevant file or database;
- Identify personnel to be interviewed during the verification. In addition to the PFSO, others to consider are selected port facility management; operations and administrative staff; and the SSO of a visiting ship, if available, (to seek information on how the port facility interacts with vessels);
- Prepare a few questions for the interviews. They should be oriented towards the purpose of the verification and specific to the personnel being interviewed (i.e. relevant to their position or responsibilities). It is important to be cognizant of why each person is being interviewed and what information should be gleaned. A sample of potential questions is shown in Annex II-4;
- Make arrangements with the PFSO for the verification;
- Make travel arrangements if required;
- Prepare required documentation and any equipment that may be needed during the verification including:
    - » Copies of any research that you may have conducted on the facility;
    - » Any relevant verification tools and forms;
    - » The ISPS Code and/or any relevant extracts of applicable legislation;
    - » Official Inspector credentials; and
    - » Safety equipment required for the facility and for boarding vessels - it may be advisable to interview the SSO on-board to confirm that required coordination and communications procedures have been conducted.
- If possible, schedule the verification when there is a ship alongside;
- Take a copy of the PFSP to the verification and compare it with the PFSP at the port facility for consistency.
- Document any known tombstone data, including PFSP references, on the Verification Report form used by the DA (see below).

## II-3.3. (b) Conduct

The Port Facility Security Verification Report form in Annex II-3 provides a sample form which can be easily adapted by a DA to suit its verification process. Inspectors may be authorized to perform the following activities when conducting a thorough and systematic verification:

- Before entering the port facility, find a suitable location to observe security procedures with respect

to access control at the main entrance. Confirm that personnel visiting the facility are challenged, identification is being checked and that this process is taking place in accordance with the PFSP;

- Upon meeting the PFSO, introduce yourself and:
  - » Explain the verification process in terms of scope, purpose, objectives, authority, legislative context, agenda and safety requirements. Advise that a debrief will be conducted with the PFSO at the end of the verification;
  - » Identify personnel that you wish to interview;
  - » Verify accuracy of the tombstone data on the partially completed report form;
  - » Use a combination of verification techniques as appropriate - observation, interviews, general on-site survey and examination of documentation and required records;
  - » Use the Port Facility Security Verification Report form to ensure that all applicable legislative requirements are fulfilled and that the approved PFSP has been implemented;
  - » During movements around the port facility, make observations of procedures for restricted areas and access control. As well, take note of the security barriers that protect the facility and restricted areas, and verify that they are in a good state of repair and effective;
  - » If deficiencies are detected, collect the appropriate evidence (e.g. copies of documentation and photographs); and
  - » Record all observations, comments and actions on the Port Facility Security Verification Report form.

### II-3.3 (c) Follow-up Action

Following completion of the verification, Inspectors may be authorized to perform the following activities:

- Debrief the PFSO and any other facility management, as applicable. Discuss any significant observations, conclusions and recommendations; and
- Advise the PFSO and applicable management of any deficiencies that require immediate attention as well as potential corrective actions that are permitted under the applicable legislation and DA procedures.
- Leave a form with the port facility which summarizes details of the verification (e.g. in terms of the areas covered); any deficiencies that were identified; and any further corrective actions that are to be taken. The Cover Sheet to the Port Facility Security Verification Report form in Annex II-3 could be used to indicate if any deficiencies were found and corrective actions required.

### II-3.3 (d) Responding to Results

Inspectors may be authorized to take the following actions:

- If no apparent security deficiencies are discovered, issue or renew the SOC;
- If minor, unintentional deficiencies are found, issue or renew the SOC only if the facility operator agrees to correct them immediately;
- If major deficiencies are discovered, delay issuing or renewing the SOC until such time as the

deficiencies are corrected;

- File the Port Facility Security Verification Report form and all related correspondence and documentation for future reference (in accordance with established filing procedures); and
- If applicable, send a letter outlining the results of the verification and any recommendations to the port facility operator.

### II-3.4 Renewal Verifications

This section could provide Inspectors with an overview of the Renewal Verification process and their role within that process.

Over the course of the validity period, the port facility's operating environment may have changed in response to international shipping trends; new technologies and techniques and emerging; and advanced ways of circumventing security procedures. Consequently, security procedures may have to be reassessed to mitigate new vulnerabilities. Thus, a key pre-verification step is for the existing PFSA to be updated either by an assessment team within the DA or by an authorized RSO.

Following its completion and approval, an updated PFSP is submitted by the PFSO for approval. This exercise may not be very onerous for the port facility as, in most cases, it may entail an audit of its current plan, and making appropriate changes based on any vulnerabilities identified in the updated PFSA.

The role of Inspectors in the Conduct, Follow-up Action and Response to Results would be the same as that described in sections II-3.3 (b)-(d).

### II-3.5 Other Post-Certification Verifications

This section could provide Inspectors with an overview of two other types of Post-Certification Verification that may be conducted - Intermediate Verifications and Additional Verifications (refer to Section II-3.2).

They would follow a similar process to a Renewal Verification. Inspectors may be authorized to handle their results as follows:

- If no apparent security deficiencies are found, endorse the SOC with signature, date and official stamp at the appropriate location on the certificate;
- If minor deficiencies are found, stamp, date and sign the SOC in the appropriate space provided that the minor deficiency is corrected immediately;
- If major deficiencies are found, instead of endorsing the SOC, take the steps identified in section I-3.3 (c) above;
- File the Port Facility Security Verification Report form, and all related correspondence and documentation for future reference; and
- If applicable, send a letter outlining the results of the verification and any recommendations to the port facility operator.

# II-4 Actions to Address Port Facility Security Verification Results

## II-4.1 Types of Action to Address Incidents of Non-Compliance

This section could provide Inspectors with useful background information on the scope and importance of a compliance program in establishing effective security regimes at port facilities under their jurisdiction as well as a context for the various compliance actions that they may be authorized to take.

Governments through their DA are ultimately responsible for ensuring that their port facilities which have been identified as falling under the ISPS Code fully comply with the security requirements specified in their relevant legislation. However, there is wide variation in the degree to which such legislation covers how incidents of non-compliance may be addressed.

Whatever the ultimate sanctions available to a DA are, before they are applied, it should consider a stepped approach which, typically, may consist of the following five (5) steps:

- Advice to a port facility operator on correcting the non-compliance;
- Further persuasion on the need to correct the non-compliance;
- Formal notification of the requirement to correct the non-compliance;
- Commencement of proceedings to impose sanctions for the failure to correct the non-compliance; and
- The imposition of sanctions for failing to correct the non-compliance.

An example of the types of action and the conditions under which they could be applied is shown below:

| Type of Action | Seriousness of Non-Compliance | Impact on Operator | Legal basis for Action |
|---|---|---|---|
| Counselling | Minor | Low | None required |
| Notice of Corrective Action or Non-Compliance | Minor | Low | None required |
| Compliance Agreement (in lieu of Monetary Penalty) | Moderate | Low to Medium | Required |
| Monetary Penalty | Moderate | Medium | Required |
| Suspension or Restriction of Port Facility Activities | Significant | Medium to High | Required |
| Withdrawal of Security Certificate | Significant | Medium to High | Required |
| Prosecution | Significant | High | Required |

However, there may be instances (e.g. a major non-compliance) where the stepped approach is required to start with formal notification. The procedures followed at each step should be taken in the knowledge that ultimately sanctions may have to be imposed if permitted by legislation. The maintenance of evidence of the deficiency and of records of the actions taken at each stage could be essential if proceedings are taken to impose sanctions and if they are to be upheld in any subsequent appeal proceedings.

### II-4.2 Role of Inspectors in Undertaking Actions

This section could provide details of how Inspectors may undertake each type of compliance action including follow-up. Any proposed compliance actions must be in accordance with applicable laws. The following are possible actions.

### II-4.2 (a) Counselling

Counselling is appropriate where the non-compliance is:

- Minor and unintentional, and does not threaten the security of the port facility or any ship using it; and
- Acknowledged by the port facility's PFSO who agrees to take corrective action in a timely manner.

Once an Inspector identifies a non-compliance, details should be recorded and any evidence collected and protected. The non-compliance should immediately be discussed with the PFSO to establish what corrective action is needed. Advice may be offered on the appropriate actions to take, including any temporary measures which could be applied until the original deficiency is corrected. A period should be agreed in which the non-compliance should be corrected and a further inspection undertaken.

Although the counselling may be verbal, keep a written record of all discussions with the PFSO.

If the follow-up establishes that the non-compliance has not been corrected within the agreed time, efforts could be made to persuade the PFSO of the need to correct the deficiency and to maintain any temporary measures. At this stage, the DA may seek to involve the port facility operator to explain that continued non-compliance may lead to a formal Notice of Corrective Action or Non-Compliance for Port Facilities being issued (see below).

### II-4.2 (b) Notice of Corrective Action or Non-Compliance

The PFSO should receive a formal notification in writing describing the non-compliance and the action needed to correct it if:

- Informal advice and persuasion have not secured correction of the minor non-compliance; or
- It is recurring; or
- The non-compliance is more serious.

Emphasis could be placed on the possible security and safety implication of the continued deficiency for those using the facility. A sample of such a notice for port facilities is shown in Annex II-5. The formal notification should:

- Set a period of time within which the non-compliance should be corrected;
- Advise that failure to correct the discrepancy within that period could lead to the commencement of

formal proceedings to achieve compliance which, in turn, could lead to sanctions being imposed on the port facility; and

- Be issued to the port facility operator rather than the PFSO.

It is important for the Inspector to record all contacts, and to retain and protect correspondence and evidence relating to the deficiency.

### II-4.2 (c) Compliance Agreement

A Compliance Agreement could be appropriate if the non-compliance:

- Is the latest in a series of minor non-compliances;
- Is moderately serious but cannot be corrected immediately; or
- Has been acknowledged as being moderately serious by the port facility operator/PFSO who agrees to take corrective action in a timely manner.

In each case, the Agreement should document:

- The nature of each non-compliance and, where appropriate, the potential monetary penalty to be applied;
- The timeframe for the corrective action and any subsequent follow-up action;
- Any non-compliances which must be corrected before a particular operation can resume;
- Acceptance by the port facility operator that failure to meet with the above conditions will result in the application of the specified monetary penalty; and
- The signatures of both the Inspector and the port facility operator.

If the agreed follow-up action confirms that the conditions of the Compliance Agreement have been fully met, then the Inspector should provide the PFSO with a written note to that effect. If the conditions have not been fully met, then the Inspector may be authorized to:

- Consider granting an extension to the timeframe if the reason for the delay is outside the control of the PFSO or can be otherwise justified; or
- Apply the monetary penalty.

### II-4.2 (d) Monetary Penalty

If provided for in a country's maritime security legislation, monetary penalties are typically applied to moderately serious non-compliances or ones that may be of a minor nature but are committed deliberately or on a repetitive basis. If the legislation provides flexibility in the amount of the monetary penalty to be applied, then the following criteria could be used to assess the appropriate level:

- What is the compliance history of the port facility?
- How deliberate was the non-compliance?
- What were the consequences or potential consequences of the non-compliance?
- Does the PFSO acknowledge or plan to take corrective action?

Inspectors may be limited in their role to recommending a particular amount, with the decision and notification being handled at a more senior level within the DA.

### II-4.2 (e) Port Facility Activities Restricted or Suspended

In instances where the non-compliance has potentially serious consequences, then the Inspector's role will likely be one of comprehensively documenting the issue. If permitted by the legislation, the DA may decide that the non-compliance requires a sanction beyond a monetary penalty. Typically, this could lead to a restriction or suspension being imposed on the aspect of port operations directly affected by the non-compliance until such time as the required corrective action has been taken.

### II-4.2 (f) Withdrawal of Security Certificate

If the required corrective action is not taken by the port facility operator, then the next sanction could be the withdrawal of their security certificate until such time as corrective action acceptable to the DA is completed.

### II-4.2 (g) Prosecution

Prosecution may be considered when none of the preceding steps has resulted in correction of the non-compliance; or the non-compliance is of a very serious nature and may have resulted in a security incident.

In such cases and subject to enabling legislation, the DA may commence proceedings to seek sanctions against the port facility operator. The procedures should be clearly stated in the legislation which is likely to include the right to appeal against the imposition of sanctions. They could involve hearings before an administrative or judicial tribunal where the DA is required to explain and, if necessary, defend the actions that it has taken to seek corrective action. For this reason, the documentary evidence of the actions taken by the Inspector and of the non-compliance are likely to be essential to the success of the DA's case.

# II-5. Other Port Facility Security Activities of Inspectors

## II-5.1 Participation in Port Security Committees

Most port operators or regulators have established Port Security Committees as a mechanism for exchanging information with private or public sector entities located on or adjacent to the port. It is customary for the Inspector assigned to that port to be a member of that committee. In that role, the assigned Inspector can serve as an effective conduit between the DA and the port operator by:

- Communicating emerging regional/national security threats and possible implications of security incidents at other ports to committee members (conditional on confidentiality considerations);
- Relaying information on perceived changes in the local threat picture and recent security incidents back to the DA;
- Suggesting opportunities for increased co-ordination in the application of security procedures and measures;
- Participating in the planning and evaluation of security drills and exercises;
- Providing progress reports on the conduct of port-wide security assessments;
- Providing advice on the development of port-wide security plans;
- Addressing shore leave issues for seafarers; and
- Contributing to the design and delivery of security awareness programs for port personnel and the public.

## II-5.2 Monitoring Security at Occasional Use Port Facilities

The ISPS Code provides for DAs to determine the extent to which the ISPS Code should apply to port facilities which are occasionally used by ships on international voyages. Although such facilities are not required to appoint a PFSO, in such cases, some DAs require the operator of an Occasional Use Port Facility to:

- Designate an individual to be responsible for security operations when a ship falling under the ISPS Code is at the facility; and
- Submit the security measures and procedures to be in place at such times.

In such cases, the role of an Inspector could be to monitor the effectiveness of security operations by verifying that:

- Each DOS is properly completed;
- Security sweeps are performed in accordance with the security procedures; and
- Temporary security measures are in place throughout the port facility/ship interface.

### II-5.3 Involvement with PFSO Information Exchange Networks

Increasingly, DA are establishing information exchange networks which provide an opportunity for PFSOs to periodically interact as a group with Inspectors and their managers. In such cases, the involvement of Inspectors could include:

- Sharing best practices with respect to implementing PFSPs;
- Conducting refresher training on aspects of the ISPS Code; and
- Providing feedback on generic issues arising from verification activities.

# Annex II-1

## Sample of a PFSA Review Checklist:

| Port Facility Security Assessment Review Checklist | | |
|---|---|---|
| File Number: | | |
| Name of Port Facility: | | |
| Type of Port Facility: | | |
| Location: | | |
| Port ID Number: | | |
| SOC Date of issue (yyyy-mm-dd): | | SOC Date of expiry (yyyy-mm-dd): |
| Name of Operator: | | |
| Address of Operator: | | |
| Telephone: | Fax: | E-mail: |
| Name of PFSO: | | 24 hrs Contact Number: |
| Telephone: | Fax: | E-mail: |
| DA Office: | Address: | |
| Telephone: | Fax: | E-Mail: |
| Approval Date: | Review Date: | |
| Follow-up action required: | | |
| Reviewed by (print name): | | |
| Signature: | | |

| ISPS Ref. | Does the PFSA address the following elements: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.3.1 | Physical security of the port facility? | | | |
| B15.3.2 | Structural integrity of the facility? | | | |
| B15.3.3 | Personnel protection systems? | | | |
| B15.3.4 | Procedures and policies? | | | |
| B15.3.5 | Radio and telecommunication systems, including computer systems and networks? | | | |
| B15.3.6 | Relevant transportation infrastructure? | | | |
| B15.3.7 | Utilities? | | | |
| B15.3.8 | Other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility? | | | |
| Comments: | | | | |

| ISPS Ref. | Does the PFSA address the following assets and infrastructure that are important to protect: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.7.1 | Access, entrances, approaches, and anchorages, maneuvering and berthing areas? | | | |
| B15.7.2 | Cargo facilities, terminals, storage areas, and cargo handling equipment? | | | |
| B15.7.3 | Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks? | | | |
| B15.7.4 | Port vessel traffic management systems and aids to navigation? | | | |
| B15.7.5 | Power plants, cargo transfer piping, and water supplies? | | | |
| B15.7.6 | Bridges, railways, roads? | | | |
| B15.7.7 | Port service vessels, including pilot boats, tugs, lighters, etc? | | | |
| B15.7.8 | Security and surveillance equipment and systems? | | | |
| B15.7.9 | The waters adjacent to the port facility? | | | |
| Comments | | | | |

| ISPS Ref. | Has there been consultation with the relevant national security organizations to identify: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.10.1 | Any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack? | | | |
| B15.10.2 | The likely consequences in terms of loss of life, damage to property and economic disruption, including disruption to transport systems, of an attack on, or at, the port facility? | | | |
| B15.10.3 | The capability and intent of those likely to mount such an attack? | | | |
| B15.10.4 | The possible type, or types, of attack? | | | |
| Comments: | | | | |

| ISPS Ref. | Have all possible threats, including the following types of security incidents, been considered: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.11.1 | Damage to or destruction of, the port facility or of the ship (e.g. by explosive devices, arson, sabotage or vandalism? | | | |
| B15.11.2 | Hijacking or seizure of the ship or of persons on board? | | | |
| B15.11.3 | Tampering with cargo, essential ship equipment or systems or ship's stores? | | | |

| | | | | |
|---|---|---|---|---|
| B15.11.4 | Unauthorized access or use, including presence of stowaways? | | | |
| B15.11.5 | Smuggling weapons or equipment, including weapons of mass destruction? | | | |
| B15.11.6 | Use of the ship to carry those intending to cause a security incident and their equipment? | | | |
| B15.11.7 | Use of the ship itself as a weapon or as a means to cause damage or destruction? | | | |
| B15.11.8 | Blockage of port entrances, locks, approaches, etc? | | | |
| B15.11.9 | Nuclear, biological and chemical attack? | | | |
| Comments: | | | | |

| ISPS Ref. | Has the selection of security measures been evaluated based on information that includes: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.14.1 | Security surveys, inspections and audits? | | | |
| B15.14.2 | Consultation with port facility owners and operators, and owners/operators of adjacent structures, if appropriate? | | | |
| B15.14.3 | Historical information on security incidents? | | | |
| B15.14.4 | Operations within the port facility? | | | |
| Comments: | | | | |

| ISPS Ref. | Has the identification of vulnerabilities included consideration of: | PFSA Ref. | Yes | No |
|---|---|---|---|---|
| B15.16.1 | Waterside and shoreside access to the port facility and ships berthing at the facility? | | | |
| B15.16.2 | Structural integrity of the piers, facilities, and associated structures? | | | |
| B15.16.3 | Existing security measures and procedures, including identification systems | | | |
| B15.16.4 | Existing security measures and procedures relating to port services and utilities? | | | |
| B15.16.5 | Measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks? | | | |
| B15.16.6 | Adjacent areas that may be exploited during, or for, an attack? | | | |
| B15.16.7 | Existing agreements with private security companies providing water-side/ shore-side security services? | | | |
| B15.16.8 | Any conflicting policies between safety and security measures and procedures? | | | |
| B15.16.9 | Any conflicting port facility and security duty assignments? | | | |
| B15.16.10 | Any enforcement and personnel constraints? | | | |
| B15.16.11 | Any deficiencies identified during training and drills? | | | |
| B15.16.12 | Any deficiencies identified during daily operations, following incidents or alerts, the report of security concerns, the exercise of control measures, audits, etc? | | | |
| Comments: | | | | |

# Annex II-2

## Sample of a PFSP Approval Form :

| Port Facility Security Plan Approval Form | | |
|---|---|---|
| File Number: | | |
| Name of Port Facility: | | |
| Type of Port Facility: | | |
| Location: | | |
| Port ID Number: | | |
| SOC Date of issue (yyyy-mm-dd): | | SOC Date of expiry (yyyy-mm-dd): |
| Name of Operator: | | |
| Address of Operator: | | |
| Telephone: | Fax: | E-mail: |
| Name of PFSO: | | 24 hrs Contact Number: |
| Telephone: | Fax: | E-mail: |
| DA Office: | Address: | |
| Telephone: | Fax: | E-Mail: |
| Approval Date: | Review Date: | |
| Follow-up action required: | | |
| Reviewed by (print name): | | |
| Signature: | | |

## APPROVAL DOCUMENT SECTIONS

(Check the box when section completed)

Section 1 – Organizational Structure of the Port Facility

Section 2 – Security and Communication Equipment

Section 3 – Drills and Exercises

Section 4 – Records and Documentation

Section 6 – Security Procedures during Interfacing

Section 7 – Declarations of Security

Section 8 – Response to a Change in the Security Level

Section 9 – Security Procedures for Access Control

Section 10 – Security Procedures for Restricted Areas

Section 11 – Security Procedures for Handling Cargo

Section 12 – Security Procedures for Delivery of Ships' Stores and Bunkers

Section 13 – Security Procedures for Monitoring

Section 14 – Response to Security Threats, Breaches of Security & Security Incidents

Section 15 – Audits and Amendments

| Section 1 - Organizational Structure of the Port Facility | | | |
|---|---|---|---|
| ISPS Ref. | Requirement – Does the Plan identify the: | Plan Ref. | Yes/No |
| B16.8.1 | Role and structure of the security organization? | | |
| | Name of the operator? | | |
| A16.3.10 | Name and position of PFSO & 24-hour contact information? | | |
| A16.8.2 | Duties and responsibilities of the PFSO? | | |
| B16.8.2 | Duties and responsibilities of port facility personnel with security responsibilities? | | |
| B16.8.2 | Training requirements of the PFSO and port facility personnel with designated security responsibilities? | | |
| B16.8.3 | The security organization's links with other national or local authorities with security responsibilities? | | |
| Comments: | | | |

| Section 2 – Security and Communication Equipment | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan include:** | **Plan Ref.** | **Yes/No** |
| B16.8.7 | Procedures for maintaining security and communication systems and equipment? | | |
| B16.8.7 | Procedures for identifying and correcting security equipment or systems failures or malfunctions? | | |
| B16.8.4 | A description of security equipment for access control? | | |
| B16.8.4 | A description of security equipment for monitoring the port facility and surrounding area? | | |
| B16.50 | If an automatic intrusion-detection device is used, it activates an audible or visual alarm, or both, at a location that is continuously attended or monitored? | | |
| B16.51 | Monitoring is able to function continuously, including during periods of adverse weather or power disruption? | | |
| B16.52 | Monitoring equipment covers access and movements adjacent to ships interfacing with the port facility? | | |
| Comments: | | | |

| Section 3 - Drills and Exercises | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement - Does the Plan include provision for:** | **Plan Ref.** | **Yes/No** |
| B18.5 | Security drills to be conducted every three months? | | |
| B16.8.7<br>B18.4<br>B18.5 | Security drills to test individual elements of the PFSP, including the response to security threats, breaches of security and security incidents, taking into account the types of operations, personnel changes, the types of ships interfacing with the facility and other relevant circumstances? | | |
| B16.8.7<br>B18.6 | Security exercises to fully test the PFSP, including the active participation of facility personnel who have security responsibilities, relevant government officials, the CSO and any available SSOs? | | |
| B18.6 | Security exercises to check communication and notification procedures, elements of coordination, resource availability and response? | | |
| B18.6 | Security exercises to be conducted at least once every calendar year with no more than 18 months between them? | | |
| Comments: | | | |

| Section 4 - Records and Documentation | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan include provision for the PFSO to keep the following records:** | **Plan Ref.** | **Yes/No** |
| | Inspections by PFSO at rate specified in the Plan? | | |
| | Security training, including dates, duration, description and names of participants? | | |
| | Security drills & exercises, including dates, description, names of participants and any best practices or lessons learned? | | |
| | Security threats, breaches of security and security incidents, including date, time, location, the response to them and the person to whom they were reported? | | |
| | Changes in the security level, including the date, time that notification was received and the time of compliance with the requirement of the new level? | | |
| | Maintenance, calibration and testing of equipment used for security including the date and time of the activity and the equipment involved? | | |
| | DOS in respect of the port facility? | | |
| | Internal audits and reviews of security activities? | | |
| | Security assessment information, including the PFSA, each periodic review, the dates conducted and their findings? | | |
| | The Plan, including each periodic review date conducted, their findings and any recommended amendments? | | |
| | Amendments to the Plan, including the date of its approval and implementation? | | |
| | Records of inspections and patrols at the rate specified in the plan? | | |
| | A list, by name or position, of the persons who have security responsibilities? | | |
| | An up-to-date list containing the names of screening officers (if applicable)? | | |
| | For at least 2 years and to be available to authorized officials on request; and, in the case of the Plan and its PFSA, for at least 2 years after the Plan's expiry date? | | |
| B4.1<br>B16.8.6 | Protected from unauthorized access or disclosure, including the Plan? | | |
| B16.8.6 | If in electronic format, protected from deletion, destruction and revision? | | |
| Comments: | | | |

| Section 5 - Communications | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan address:** | **Plan Ref.** | **Yes/No** |
| B16.8.4 | Procedures that allow for effective communications between personnel with security responsibilities with respect to the ships interfacing with the facility and with port operators? If applicable, the DA and local law enforcement agencies? | | |
| B16.8.12 | The means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches? | | |
| B16.8.5 | Back-up communications to ensure internal and external communications? | | |
| B16.8.4 | Procedures that allow for effective communications between personnel with security responsibilities with respect to the ships interfacing with the facility and with port operators, if applicable, the DA and local law enforcement agencies? | | |
| **Comments:** | | | |

| Section 6 - Security Procedures during Interfacing | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan include procedures for:** | **Plan Ref.** | **Yes/No** |
| A16.3.7 | Coordinating with ships interfacing with the port facility and the port operator, if applicable? | | |
| B16.8.13 | Assisting SSOs in confirming the identity of those seeking to board the ship when requested? | | |
| B16.8.14 | 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 labor organizations? | | |
| **Comments:** | | | |

| Section 7 - Declarations of Security | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan make provision for:** | **Plan Ref.** | **Yes/No** |
| A5.1<br>B5.1 | The requirements and procedures for completing a DOS? | | |
| A5.2<br>B5.2 | A DOS to be completed before an interface starts between a port facility and a ship if they are operating at different Security Levels? | | |
| | A DOS to be completed before an interface starts between a port facility and a ship if one of them does not have an approved security plan? | | |
| B5.3 | A DOS to be completed before an interface starts between a port facility and a ship if the interface involves a cruise ship, a ship carrying dangerous goods or the loading or transfer of dangerous goods? | | |
| B5.2 | A DOS to be completed before an interface starts between a port facility and a ship if the security officer of either of them identifies security concerns about the interface? | | |
| Comments: | | | |

| Section 8 - Response to a Change in the Security Level | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan contain procedures for ensuring that, when the operator of the port facility is notified of an increase in the Security level:** | **Plan Ref.** | **Yes/No** |
| A4.2<br>A16.3.4 | The port facility complies with the required additional security procedures within the specified time period after the notification? | | |
| | The DA receives a report indicating compliance or noncompliance with the Security Level? | | |
| A4.2<br>A16.3.4 | If the increase is to Security Level 3, the port facility evaluates the need for additional security procedures? | | |
| Comments: | | | |

| Section 9 - Security Procedures for Access Control | | | |
|---|---|---|---|
| **ISPS Ref.** A16.3.1 | **Requirement – Does the Plan, at all Security Levels, include procedures for preventing unauthorized access to the port facility by persons, weapons, incendiaries, explosives, dangerous substances and devices:** | **Plan Ref.** | **Yes/No** |
| **At Security Level 1:** | | | |
| B16.17.1 | Establishing control points for restricted access that should be bounded by fencing or other barriers? | | |
| B16.17.2 | Verifying the identity of every person seeking to enter a controlled access area and the reasons for which they seek entry? | | |
| B16.17.3 | Checking vehicles used by those seeking entry to the port facility? | | |
| B16.17.4 | Verifying the identity of port facility personnel and those employed within the port facility, and their vehicles? | | |
| B16.17.5 | Restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity? | | |
| B16.17.6 | Searches of persons, personal effects, vehicles and their contents at the rate specified in the Plan? | | |
| B16.13 | Denying or revoking of a person's authorization to enter or remain on a port facility if they are not authorized or fail to identify themselves? | | |
| B16.12 | Determining the appropriate access controls for deterring unauthorized access to the port facility including its restricted areas? | | |
| 16.17.7 | Identifying access points that must be secured or attended to deter unauthorized access? | | |
| B16.46 | Screening or searching unaccompanied baggage at the rate(s) specified in the Plan? | | |
| **At Security Level 2:** | | | |
| B16.47 | Increasing the frequency of screening persons and goods? | | |
| B16.47 | Authorized screening of all unaccompanied baggage by means of X-ray equipment? | | |
| B16.19.1 | Additional personnel to guard access points and for perimeter patrols? | | |
| B16.19.2 | Limiting the number of access points to the port facility? | | |
| B16.19.3 | Impeding movement through the remaining access points, e.g. security barriers? | | |
| B16.19.4 | Increasing the frequency of searches of persons, personal effects and vehicles? | | |
| B16.19.5 | Denying or revoking access to persons who are unable to provide a verifiable justification for seeking access? | | |
| B16.19.6 | Coordinating with the DA, appropriate law enforcement agencies, port operator, if applicable, to deter waterside access to the facility? | | |
| **At Security Level 3**: | | | |
| B16.48 | Additional screening of unaccompanied baggage (e.g. X-raying it from at least two different angles)? | | |
| B16.20.2 | Coordinating with emergency response personnel and other port facilities? | | |
| B16.20.2 | Granting access to those responding to the security incident or security threat? | | |
| B16.20.1 | Suspending all other access to the port facility? | | |
| B16.20.5 | Suspending port operations within all, or part, of the port facility? | | |
| B16.20.7 | Evacuating the port facility or part thereof? | | |
| B16.20.3 | Restricting pedestrian and vehicular movements? | | |
| B16.20.4 | Increasing security patrols within the port facility, if appropriate? | | |
| B16.20.6 | Directing vessel movements relating to all, or part, of the port facility? | | |
| Comments: | | | |

| Section 10 - Security Procedures for Restricted Areas | | | |
|---|---|---|---|
| **ISPS Ref.**<br><br>B16.21 | **Requirement – Does the Plan make provision for designating restricted areas, including those listed below, and specifying measures and procedures, as appropriate to the facility's operations at each Security Level:** | **Plan Ref.** | **Yes/No** |
| B16.25.1 | Land areas adjacent to ships interfacing with the port facility? | | |
| B16.25.2 | Embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas, including search points? | | |
| B16.25.3 | Areas designated for loading, unloading or storage of cargo and ships' stores? | | |
| B16.25.4 | Areas in which security-sensitive information is kept, including cargo documentation? | | |
| B16.25.5 | Areas where dangerous goods and hazardous substances are held? | | |
| B16.25.6 | Vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms? | | |
| B16.25.7 | Areas where security and surveillance equipment is stored or located? | | |
| B16.25.8 | Essential electrical, radio and telecommunication, water and other utility installations? | | |
| B16.25.9 | Locations in the port facility where it is reasonable to restrict access by vehicles and persons? | | |
| **At Security Level 1**: | | | |
| B16.27.1 | Providing permanent or temporary barriers to surround the restricted area? | | |
| B16.27.2 | Procedures for securing all access points not actively used and providing physical barriers or security guards to impede movement through the remaining access points? | | |
| B16.27.3 | Procedures for controlling access to restricted areas, such as a pass system that identifies an individual's entitlement to be within the restricted area? | | |
| B16.27.4 | Procedures for examining the identification and authorization of persons and vehicles seeking entry, and clearly marking vehicles allowed access to restricted areas? | | |
| B16.27.5 | Procedures for patrolling or monitor the perimeter of restricted areas? | | |
| B16.27.6 | Procedures for using security personnel, automatic intrusion detection devices or surveillance equipment/systems to detect unauthorized entry or movement in the restricted areas? | | |
| B16.27.7 | Procedures for controlling the movement of vessels in the vicinity of ships using the port facility? | | |
| B16.21 | Procedures for designating temporary restricted areas, if applicable, to accommodate port facility operations? including restricted areas for segregating unaccompanied baggage that has undergone authorized screening by a ship operator? | | |
| B16.21 | Procedures for conducting a security sweep (both before and after) if a temporary restricted area is designated? | | |
| **At Security Level 2:** | | | |
| B16.28.1 | Procedures for enhancing physical barriers, including the use of patrols or intrusion detection devices? | | |
| B16.28.2 | Procedures for reducing the number of access points and enhancing controls applied at the remaining access points? | | |
| B16.28.3 | Procedures for restricting parking of vehicles adjacent to ships? | | |
| B16.28.4 | Procedures for reducing access to restricted areas and movements and storage in them? | | |
| B16.28.5 | Procedures for using surveillance equipment that records and monitors continuously? | | |
| B16.28.6 | Procedures for increasing the number and frequency of patrols, including the use of waterside patrols? | | |
| B16.28.7 | Procedures for establishing and restricting access to areas adjacent to restricted areas? | | |
| B16.28.8 | Enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility? | | |
| **At Security Level 3:** | | | |
| B16.29.1 | Procedures for designating additional restricted areas adjacent to the security incident or threat to which access is denied? | | |
| B16.29.2 | Procedures for searching restricted areas as part of a security sweep of all or part of the port facility? | | |

| Comments: | | | |
|---|---|---|---|
| Section 11 - Security Procedures for Handling Cargo | | | |
| **ISPS Ref.** | **Requirement – Does the Plan include procedures for:** | **Plan Ref.** | **Yes/No** |
| B16.31 | Identifying cargo that is accepted for loading onto ships interfacing with the port facility? | | |
| B16.31 | Identifying cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up? | | |
| **At Security Level 1**: | | | |
| B16.32.1 | Verifying that cargo, containers and cargo transport units entering the port facility match the invoice or other cargo documentation? | | |
| B16.32.1 | Routine inspection of cargo, containers, transport units and cargo storage areas before and during handling operations to detect evidence of tampering, unless unsafe to do so? | | |
| B16.32.2 | Verifying that the cargo entering the facility matches the delivery documentation? | | |
| B16.32.3 | Searching vehicles entering the port facility? | | |
| B16.32.4 | Examining seals and other methods used to detect evidence of tampering when cargo, containers or cargo transport units enter the port facility or are stored there? | | |
| **At Security Level 2:** | | | |
| B16.35.1 | Detailed checking of cargo, containers, and cargo transport units in or about to enter the port facility or cargo storage areas, for weapons, explosives and incendiaries? | | |
| B16.35.2 | Intensified inspections to ensure that only documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship? | | |
| B16.35.3 | Detailed search of vehicles for weapons, explosives and incendiaries? | | |
| B16.35.4 | Increasing the frequency and detail of examinations of seals and other methods used to prevent tampering? | | |
| B16.36.1 | Increasing the frequency and intensity of visual and physical inspections? | | |
| B16.36.2 | Increasing the frequency of the use of scanning/detection equipment, mechanical devises or dogs? | | |
| B16.36.3 | Coordinating enhanced security measures with shippers or those acting on their behalf in accordance with an established agreement and procedures? | | |
| **At Security Level 3:** | | | |
| B16.37.1 | Restricting or suspending cargo movements or operations in all or part of the port facility? | | |
| B16.37.2 | Confirming the inventory and location of certain dangerous cargoes in the port facility? | | |
| Comments: | | | |

| Section 12 - Security Procedures for Delivery of Ships' Stores and Bunkers | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan include procedures for:** | **Plan Ref.** | **Yes/No** |
| **At Security Level 1:** | | | |
| B16.40.1 | Checking ship stores? | | |
| B16.40.2 | Requiring advanced notification of the delivery of ships' stores or bunkers, including a list of stores, and driver and vehicle registration information in respect of delivery vehicles? | | |
| B16.40.3 | Inspecting delivery vehicles at the rate specified in the Plan? | | |
| At Security Level 2: | | | |
| B16.42.1 | Detailed checking of ship's stores? | | |
| B16.42.2 | Detailed searches of delivery vehicles? | | |
| B16.42.3 | Coordinating with ship personnel to check the order against the delivery note prior to entry to the port facility? | | |
| B16.42.4 | Escorting delivery vehicles in the port facility? | | |

| | | | |
|---|---|---|---|
| **At Security Level 3:** | | | |
| B16.44 | Restricting or suspending the delivery of ships' stores and bunkers? | | |
| B16.44 | Refusing to accept ships' stores in the port facility? | | |
| **Comments:** | | | |

| Section 13 - Security Procedures for Monitoring | | | |
|---|---|---|---|
| **ISPS Ref.** B16.51 | **Requirement – Does the Plan 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, including:** | **Plan Ref.** | **Yes/No** |
| **At Security Level 1:** | | | |
| B16.52.1 | Observe the general port facility area, including shore- and water-side accesses to it? | | |
| B16.52.2 | Observe access points, barriers and restricted areas? | | |
| B16.52.3 | Allow port facility security personnel to monitor areas and movements adjacent to ships, including augmentation of lighting provided by the ship itself? | | |
| **At Security Level 2:** | | | |
| B16.53.1 | Additional procedures to increase the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance? | | |
| B16.53.2 | Procedures for increasing the frequency of foot, vehicle or waterborne patrols? | | |
| B16.53.3 | Procedures for assigning additional security personnel to monitor and patrol? | | |
| **At Security Level 3:** | | | |
| B16.54.1 | Procedures for switching on all lighting in, or illuminating the vicinity of, the port facility? | | |
| B16.54.2 | Procedures for switching on all surveillance equipment capable of recording activities in or adjacent to the port facility? | | |
| B16.54.3 | Procedures to maximize the length of time that surveillance equipment can continue to record? | | |
| **Comments:** | | | |

| Section 14 - Response to Security Threats, Breaches of Security and Security Incidents | | | |
|---|---|---|---|
| ISPS Ref. | **Requirement – Does the Plan address procedures at all Security Levels for:** | **Plan Ref.** | **Yes/No** |
| A16.3.3 | Responding to security threats, breaches of security and security incidents, including provisions to maintain critical port facility and interface operations? | | |
| A16.3.5 | Evacuating the port facility in case of security threats and security incidents? | | |
| | Briefing port facility personnel on potential threats to security and the need for vigilance? | | |
| | Securing non-critical operations in order to focus response on critical operations? | | |
| A16.3.9 | Reporting security threats, breaches of security and security incidents to the appropriate law enforcement agencies, the DA and, if applicable, the port operator? | | |
| **Comments:** | | | |

| Section 15 - Audits and Amendments | | | |
|---|---|---|---|
| **ISPS Ref.** | **Requirement – Does the Plan address when an audit is required and the timing for submitting audit-based amendments, as follows:** | **Plan Ref.** | **Yes/No** |
| B16.59.1 | The PFSA relating to the facility is altered? | | |
| B16.59.2 | An independent audit or the DA's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant elements of the approved Plan? | | |
| B16.59.3 | Security incidents or threats involving the port facility have occurred? | | |
| B16.59.4 | There is a new operator of the port facility, a change in operations or location, or modifications to the port facility that could affect its security? | | |
| B16.60 | If the audit results require an amendment to be made to the PFSA or Plan, the PFSO submits an amendment to the Designated Authority for approval within 30 days after completion of the audit? | | |
| | If the operator of a port facility submits other amendments to the approved Plan, they are to be submitted at least 30 days before they take effect? | | |
| **Comments:** | | | |

| **PFSP REVIEW:** |
|---|
| APPROVED: |
| DISAPPROVED: |
| **Comments:** |

# Annex II-3

## Sample of a Port Facility Security Verification Report Form

| PORT FACILITY SECURITY VERIFICATION REPORT FORM | | | | | |
|---|---|---|---|---|---|
| Marine File Number: | | | | | |
| Type of Port Facility: | | | | | |
| Name of Port Facility: | | | | ID Number: | |
| Location: | | | | | |
| SOC Number: | | | Security Level: | | |
| Name of Operator: | | | | | |
| Address of Operator: | | | | | |
| Telephone: | | Fax: | | E-mail: | |
| Name of PFSO: | | | | Contact Number: | |
| Telephone: | | Fax: | | E-mail: | |
| Type of Verification: | | | | | |
| Initial | | Intermediate | | Renewal | |
| Additional (includes monitoring and follow-up) | | | | | |
| | Areas of Verification (tick the appropriate boxes below):<br>1. Documents and Records<br>2. Access Control<br>3. Restricted Area Access Control<br>4. Handling of Cargo<br>5. Delivery of Ships Stores and Bunkers<br>6. Security Procedures for Monitoring<br>7. Procedures for Threats and Security Incidents<br>8. Security Communications<br>9. Audits and Amendments<br>10. Procedures for Shore Leave and Visitors to the Ship<br>11. Procedures for Interfacing with Ship Security Activities<br>12. Evacuation Procedures<br>13. Security Procedures to Protect the Security Plan | | | | |
| Deficiencies Found | Yes | No | Supporting Documentation | Yes | No |
| Date of last Verification (yyyy-mm-dd) | | | | | |
| Have there been any changes to the port facility since the plan was approved? | | | | Yes | No |
| DA Security Office: | | | Address: | | |
| Telephone: | | Fax: | | E-Mail: | |
| Date of Verification (yyyy-mm-dd) | | | | | |
| Name of Inspector: | | | Signature: | | |

Note: Only the above Cover Sheet to the Report Form is to be given to the PFSO. It must be retained at the port facility's office for a period specified by the DA and be available for consultation by an authorized official at all times.

| 1. Documents and Records | Compliant ☐ | Action Required ☐ |
|---|---|---|
| Plan References: | | |
| PFSA | Note approval date: | |
| PFSP | Note approval date: | |
| Records of annual audits | Note date of last audit and its findings | |
| Records of DOS | Note date of last DOS | |
| Records of Training | For each course, list date, duration, description and participants | |
| Record of personnel with security responsibilities | List by name or position | |
| Records of drills | Note date of last drill. For each drill, note date, description, names of participants, and any best practices or lessons learned that might improve the plan | |
| Records of security threats, breaches and incidents | For each event, note date, time, location, description, the response and to whom it was reported | |
| Records of change in Security Level | For each change, note the date, the time that notification was received, and the time of compliance with the requirements of the new Security Level | |
| Records of maintenance, calibration and testing of security equipment | For each activity, note date, time and the equipment involved | |
| Record of PFSP amendments | For each amendment, note approval and implementation dates | |
| Records of inspections and patrols | | |

**Possible questions for Inspectors to ask the PFSO/security personnel and follow-up actions:**

- O Does the PFSO keep the records or are they kept elsewhere?
- O If so, has the PFSO documented their existence, location and the name/position of the person responsible?
- O Are they complete as required and kept for at least 1 year?
- O Are the PFSP and related PFSA kept for at least 1 year after the day on which the PFSP expires?
- O How are records protected from unauthorized access or disclosure?
- O Are records kept electronically?
- O If so, how are they protected from deletion, destruction and revision?
- O Are computer passwords protected and how often are they password changed?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

| |
|---|
| **Action required by Operator (if necessary):** |
| **Action by Inspector (if necessary):** |

| 2. Access Control | Compliant ☐ | Action Required ☐ |
|---|---|---|

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- O Gates/Barriers
  - » Are gates secured (manned/locked) and in good condition?
  - » Do gates have card accesses?
  - » Do gates have keys?
- O Fencing
  - » Are fences in good condition and clear of equipment/vehicles and debris against them.?
  - » Who patrols/checks the fences?
  - » Whom do personnel report breaches or damage to fencing to?
  - » Are logs maintained for patrols of fence line or maintenance?
- O Rail Security
  - » Are access controls established where rail lines enter the facility?
  - » Who monitors the activity at rail access points?
- O Identification
  - » What types of ID are valid to access the port facility?
  - » When would a person be denied access to the facility or a restricted area?
  - » Is a log kept?

Suggested Good Practices for Inspectors: Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.

**Observations:**

**Action required by Operator (if necessary):**

**Action by Inspector (if necessary):**

| 3. Restricted Area Access Control | Compliant ☐ | Action Required ☐ |
|---|---|---|

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- O What ID is valid to access or remain in a restricted area?
- O What procedures are in place to issue passes, record their issuance, and record their loss?
- O What procedures are in place for verifying the identity of authorized officials?
- O What procedures are in place for verifying the identity of emergency responders?
- O What procedures are in place for verifying visitors, truck drivers and ship's crew?
- O How are keys and passes controlled for restricted areas?
- O What is the process for reporting lost keys, passes or access cards?
- O Is a record kept of those that are lost?
- O Are persons subject to additional security measures when working in restricted areas?
- O Are persons entering the facility or restricted area recorded in a log?
- O What is the procedure for crew access?
- O What procedures are in place to ensure that only authorized crew are allowed back on the vessel?
- O What procedures are in place for visitors to access restricted areas or the vessel?
- O Are all restricted areas secured in accordance with the procedures contained in the security plan?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

| 4. Handling of Cargo | Compliant ☐ | Action Required ☐ |
|---|---|---|

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- O What procedures are followed to deter cargo tampering?
- O How is cargo identified and accepted for loading onto vessels?
- O How long is cargo stored at the facility prior to loading?
- O Are there temporary storage areas?
- O How is cargo in temporary storage areas inspected prior to loading?
- O Is there an inventory of dangerous cargos?
- O Are these cargos segregated from the remainder of the cargo at the port facility?
- O Are they subject to additional security procedures?
- O If so, are they detailed in the PFSP?
- O What procedures are applied to inspect vehicles carrying cargo?
- O If so, are they detailed in the PFSP?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations**

**Action required by Operator (if necessary):**

**Action by Inspector (if necessary):**

| 5. Delivery of Ships Stores | Compliant ☐ | Action Required ☐ |
|---|---|---|
| **Plan References:**<br>**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**<br>O How are security guards advised of ships' stores deliveries?<br>O Are all ships' stores deliveries scheduled in advance?<br>***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.* | | |
| **Observations:** | | |
| **Actions Required by Operator (if necessary):** | | |
| **Actions Taken by Inspector (if necessary):** | | |

| 6. Security Procedures for Monitoring | Compliant ☐ | Action Required ☐ |
|---|---|---|

**Plan References:**

**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

O Alarms, Motion Detectors and Lights

- » Who responds to alarm activations?
- » Is the alarm company local?
- » Do the alarms call the police?
- » Are they silent or audible?
- » Where are the motion detection devices located?
- » Who is responsible to ensure that facility lighting is in good working order?
- » What are the maintenance procedures for alarms, motion detectors and lights?

O Control/Surveillance Rooms

- » Is this area restricted?
- » Is it signed?
- » Who has access?
- » How is access controlled/secured?
- » How many persons are on duty throughout the day?
- » Do they have other security responsibilities that may take them away from monitoring camera activity?
- » Is the control room ever unattended?
- » How is the surveillance equipment maintained?
- » Are records of maintenance and occurrences kept in the control room?
- » Are images recorded when cameras are motion-activated, continuously recorded or not capable of recording?
- » What is the length of recording time?
- » How long are the recordings kept before re-recording?

O Security Rounds

- » Who conducts security rounds?
- » What do the security rounds entail?
- » As part of security rounds, are passes verified and unfamiliar persons questioned?
- » Are the times and results recorded?
- » Are security sweeps conducted before (and/or after) a vessel interfaces with the dock?
- » What is the procedure for security sweeps?
- » Are all restricted areas patrolled?
- » If so, what is the frequency?

O Waterside Security

- » Who patrols the waterside of the port facility?
- » How does the PFSO contact the police or service provider for assistance?
- » Do security rounds include a patrol of the waterside and lands adjacent to the water?
- » Who conducts patrols of the lands adjacent to the waterside? What is their frequency?
- » Are there surveillance cameras directed at the waterside of the port facility?
- » Do they record activity and, if so, how?

O Lighting

- » Is lighting effective at night?
- » Are video recording cameras?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

| **7. Procedures for Responding to Security Threats, Breaches of Security and Security Incidents** | **Compliant** ☐ | **Action Required** ☐ |
|---|---|---|

**Plan References:**
**Possible questions for PFSO/security personnel and follow-up actions:**

- O Reporting Security Incident and Threats
  - » What are the procedures for reporting suspicious activities?
- O Do facility personnel use Security Incident Reports at the facility?
  - » Are these logged and submitted to the DA?
  - » What procedures do facility personnel follow if they receive a bomb threat on their phone; or discover a suspicious package on the dock; or discover a suspicious person or activity occurring in the facility?
- O Response Procedures
  - » What is the responsibility of the PFSO when notified of an increase in Security Level?
  - » How does the PFSO respond to a specific security threat or breach?
  - » How do personnel with security responsibilities respond to a specific security threat or breach?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

| 8. Security Communications | Compliant ☐ | Action Required ☐ |
|---|---|---|

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- O Are personnel equipped with radios for security communication purposes?
- O What channel is used for security communications?
- O Does the communication system and backup system (radio, telephone, etc.) provide a reliable means for the PFSO to contact someone on the facility or on-board the vessel?.
- O Are additional communication procedures put into effect when Security Levels increase?
- O Are facility personnel aware of the signs that are used to advise them of a change in Security Level?
- O Can facility personnel identify the PFSO?
- O Ask the PFSO if the vessel (or ship's agent) advises the facility of its Security level prior to arrival?
- O How is this information communicated?
- O What are the maintenance procedures for communications equipment?
- O Under what circumstances is a DOS completed?
- O Who has the authority to complete a DoS at the facility?
- O How are communication procedures established when interfacing with a vessel?
- O Does the PFSO use a radio or cellular phone to contact SSOs on-board ships?
- O How is the delivery and inspection of ships' stores coordinated?
- O How is information concerning the contact of reciprocal security officers, SSAS activation, security threats, breaches and incidents conveyed?
- O How is crew access controlled?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

| 9. Audits and Amendments | Compliant ☐ | Action Required ☐ |
|---|---|---|
| **Plan References:**<br>**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**<br>O Are annual audits of the PFSP based on the date of the original plan's approval?<br>O Do audits take place whenever there is a new operator, a change in operations or location, or modification to the port facility that could affect its security?<br>O Is there evidence of audits being undertaken in the form of audit plans, audit reports, meeting minutes, records of follow-up or remedial actions?<br>O Does the person who conducted the audit have the relevant formal qualifications and work experience?<br>***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.* | | |
| **Observations:** | | |
| **Actions Required by Operator (if necessary):** | | |
| **Actions Taken by Inspector (if necessary):** | | |

## 10. Procedures for Shore Leave and Visitors to the Ship

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- What are the procedures in place for facilitating shore leave?
- Who is responsible for escorting or continuously monitoring seafarers transiting through restricted areas of the port?
- How is this coordinated with the ship?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

## 11. Procedures for Interfacing with Ship Security Activities

**Plan References:**

**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

**Note:** Some possible questions have been covered under Section 8 (Security Communications), including how communications take place between the facility and the ship and ship's stores (e.g. how they are received, and the coordination between the facility and the ship)..

» Is there an exchange of information between the ship and the facility? This could include contact info, emergency numbers, etc?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

## 12. Evacuation Procedures

**Plan References:**

**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- » Where is the muster point for the evacuation?
- » How does the facility coordinate an evacuation of the ship through the port facility?

***Suggested Good Practices for Inspectors:*** *Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

## 13. Security Procedures to Protect the Security Plan

**Plan References:**
**Possible questions for Inspectors to ask PFSO/security personnel and follow-up actions:**

- O Is the PFSP made available only to people who have a legitimate need to know how to fulfil their official duties or contractual obligations?
- O Is the PFSP handled with due care and only in accordance with authorized procedures?
- O Is the PFSP kept in a safe place and accessed only in accordance with authorized procedures?

***Suggested Good Practices for Inspectors**: Verify each response through a further interview, observation, referral to the PFSP, spot check or testing, as applicable.*

**Observations:**

**Actions Required by Operator (if necessary):**

**Actions Taken by Inspector (if necessary):**

| Date | Additional Comments |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# Annex II-4

## Sample of Interview Questions

### Port Facility Security Officer

What training have you received for your position?

What are your procedures for access control?

What are your restricted areas, where are they located and how are they identified?

To whom are security incidents reported and how are they reported to appropriate authorities?

Do you have security cameras and if so describe their use (e.g. how are they monitored and do they continuously record?

How is cargo checked entering the facility?

How does your facility communicate with the security force and ships alongside?

Do you conduct regular inspections of the port facility to ensure the continuation of appropriate security measures?

### Personnel with Security Responsibilities

What training have you received to perform your security duties?

What are your duties regarding security at the facility?

What is a Security Level and what does each Level mean?

How do your security duties change at each Security Level?

Explain how you conduct physical searches of persons, effects, baggage, cargo and ship stores.

Explain how your security equipment and systems are operated.

### Personnel without Security Responsibilities

What are security levels?

What is required of you at each security level?

What security orientation or training have you received?

### Ship Security Officer of Visiting Ship

How do you communicate with the PFSO or other security personnel?

Were you provided with emergency telephone numbers for the port?

What is the Security Level of the ship?

What is the Security Level of the port facility?

# Annex II-5

## Sample of a Notice of Corrective Action or Non-Compliance for Port Facilities

| NOTICE OF CORRECTIVE ACTION OR NON-COMPLIANCE FOR PORT FACILITIES | | | | |
|---|---|---|---|---|
| File Number: | | | Date: | |
| Name of Port Facility: | | | | |
| Item No. | Description of Deficiency | Legislative Reference | Action Required | Date to be Rectified |
| | | | | |
| | | | | |
| | | | | |

| Position, Name and Signature of the Authorized Representative of the Operator | | | |
|---|---|---|---|
| Address | | Date | |
| Address | | Telephone Number | |
| City | | FAX | |
| State/Postal Code | | EMAIL | |
| Country | | WEB site | |

| Designated Authority | | | |
|---|---|---|---|
| Name of Authority | | | |
| Address | | | |
| City | | State/Postal Code | |
| Country | | | |
| Name of Authorized Official | | | |
| Signature | | | |