
	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>



**PORT FACILITY SECURITY OFFICER**

**IMO MODEL 3.21**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

## **SCOPE**

This course has been based on MCS /Circ 1188, “Guidelines on training and certification for Port Facility Security Officers”, and aims to provide knowledge to those who may be designated to perform the duties and responsibilities of a Port Facility Security Officer (PFSO), as defined in Section A/2.1.8 (and Section A/17) of the ISPS Code and, in particular the duties and responsibilities with respect to the security of a Port Facility, for ensuring the development (or for developing) of a Port Facility security assessment, for ensuring the development (or for developing), implementation, maintenance and updating of a Port Facility Security Plan and for liaising with Ship Security Officers (SSOs) and with Company Security Officers (CSOs).

## **OBJECTIVES**

Those who successfully complete this course will have the competence to:

1. Develop, maintain and supervise the implementation of a port facility security plan;
2. Assess security risk, threat, and vulnerability;
3. Undertaking regular inspections of the port facility to ensure that appropriate security measures are implemented and maintained;
4. Ensure that security equipment and any system, if any, are properly operated, tested and calibrated; and
5. Encourage security awareness and vigilance

## **ENTRY STANDARD**

Those attending this course will be persons employed (or to be employed) by a port facility operator and that they are likely to be designated as Port Facility Security Officer. However, no specific entry requirements are required.

## **COURSE CERTIFICATION, DIPLOMA OR DOCUMENT**

Documentary evidence should be issued to those who have successfully completed this course indicating that the holder has completed training as “Port Facility Security Officer” based on this course.


## **COURSE INTAKE LIMITATION**

The maximum number of trainees will be 25 persons.

## **STAFF REQUIREMENTS**

The instructors in charges of the course should have completed a port facility security officer.

A 6.09 methodological course.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### TEACHING FACILITY AND EQUIPMENT

Ordinary classroom or similar meeting room with a blackboard.

### TEACHING AIDS

Instructor Manual.

Audiovisual Aids: video compact disc player, TV, LCD Projector, overhead projector, etc.

Photographs, models, or other representations of various type of vessels and vessel parts to illustrate operational elements and security vulnerabilities

Video cassette(s)

Distance learning package (s)

Computer Based Training.

### BIBLIOGRAPHY

Fernandez, L., & Merzer, M. (2003). *Jane's Crisis Communications Handbook*, (1st ed.). Alexandria: Jane's Information Group.

FIA International Research, Ltd. (2001). *Contraband, Organized Crime and the threat to the Transportation and Supply Chain Function*. FIA International.

Hawkes, K.G. (1989). *Maritime Security*. Centreville: Cornell Maritime Press.

Interagency Commission on Crime and Security in U.S. Seaports. (2002). *Report of the Interagency Commission on Crime and Security in U.S. Seaports*. Washington, D.C.

Sidell, F.R., et al. (2002). *Jane's Chem-Bio Handbook*. (2nd ed.). Alexandria: Jane's Information Group.

Sullivan, J.P., et al. (2002). *Jane's Unconventional Weapons Response Handbook*. (1st ed.). Alexandria: Jane's Information Group.

Unit States Department of Transportation. Volpe National Transportation Systems Center. (1999). *Intermodal Cargo Transportation: Industry Best Security Practices*. Cambridge: Volpe Center.

United State Department of Transportation. (1997). *Port Security: A National planning Guide*. Washington, D.C.: U.S. DOT.

Units States Department of transportation. (1998). *Port Security: Security Force Management*. Washington, D.C.: U.S. DOT.

Viollis, P., et al. (2002). *Jane's Workplace Security Handbook*. (1st ed.). Alexandria: Jane's Information Group.



<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

**TIMETABLE**

**COURSE OUTLINE**

SUBJECT AREA	HOURS	
	L	D
<b>1. INTRODUCTION (1.0 HOURS)</b> 1.1 OVERVIEW 1.2 COMPETENCE TO BE ACHIEVED 1.3 HISTORICAL PERSPECTIVE 1.4 CURRENT SECURITY THREATS AND PATTERNS	1.0	
<b>2. MARITIME SECURITY (1.0 HOURS)</b> 2.1 RELEVANT INTERNATIONAL CONVENTIONS, CODES, CIRCULARS AND RECOMMENDATIONS INCLUDING THOSE THAT MAY RELATE TO PIRACY 2.2 RELEVANT GOVERNMENT LEGISLATION AND REGULATIONS 2.3 DEFINITIONS 2.4 HANDLING SENSITIVE SECURITY-RELATED INFORMATION AND COMMUNICATIONS	1.0	
<b>3. SECURITY RESPONSIBILITIES (1.5 HOURS)</b> 3.1 CONTRACTING GOVERNMENTS 3.2 RECOGNIZED SECURITY ORGANIZATIONS 3.3 THE COMPANY 3.4 THE SHIP 3.5 THE PORT FACILITY 3.6 SHIP SECURITY OFFICER 3.7 COMPANY SECURITY OFFICER 3.8 PORT FACILITY SECURITY OFFICER 3.9 SHIPBOARD PERSONNEL WITH DESIGNATED SECURITY DUTIES 3.10 PORT FACILITY PERSONNEL WITH DESIGNATED SECURITY 3.11 OTHER PERSONNEL	1.5	
<b>4. PORT FACILITY SECURITY ASSESSMENT AND ON-SCENE INSPECTIONS (2.5 HOURS)</b> 4.1 RISK ASSESSMENT METHODOLOGY 4.2 ASSESSMENT TOOLS 4.3 ON-SCENE SECURITY INSPECTION 4.4 SECURITY ASSESSMENT DOCUMENTATION	2.0	0.5



<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>


SUBJECT AREA	HOURS	
	L	D
<b>5. INTRODUCTION (1.0 HOURS)</b> 5.1 SECURITY EQUIPMENT AND SYSTEMS 5.2 OPERATIONAL LIMITATIONS OF SECURITY EQUIPMENT AND SYSTEM 5.3 TESTING, CALIBRATION AND MAINTENANCE OF SECURITY EQUIPMENT AND SYSTEMS	0.5	0.5
<b>6. PORT FACILITY SECURITY PLAN (2.5HOURS)</b> 6.1 PURPOSE OF THE PORT FACILITY SECURITY PLAN 6.2 CONTENTS OF THE PORT FACILITY SECURITY PLAN 6.3 CONFIDENTIALITY ISSUES 6.4 DEVELOPMENT OF THE PORT FACILITY SECURITY PLAN 6.5 APPROVAL OF THE PORT FACILITY SECURITY PLAN 6.6 IMPLEMENTATION OF THE PORT FACILITY SECURITY PLAN 6.7 MAINTENANCE AND MODIFICATION OF THE PORT FACILITY SECURITY PLAN	2.5	
<b>7. THREAT IDENTIFICATION (1.5 HOURS)</b> 7.1 RECOGNITION, ON A NON-DISCRIMINATORY BASIS, OF PERSON POSING POTENCIAL SECURITY RISK 7.2 RECOGNITION AND DETECTION OF WEAPONS, DANGEROUS SUBSTANCES AND DEVICES 7.3 IMPLEMENTING AND CO-ORDINATING SEARCHES 7.4 METHODS OF PHYSICAL SEARCHES AND NON-INSTRUCTIVES INSPECTIONS 7.5 TECHNIQUES USED TO CIRCUMVENT SECURITY MEASURES INCLUDING THOSE USED BY PIRATES 7.6 CROWD MANAGEMENT AND CONTROL TECHNIQUES	1.0	0.5
<b>8. PORT FACILITY SECURITY ACTION (1.0 HOURS)</b> 8.1 ACTION REQUIRED BY DIFFERENT SECURITY LEVELS 8.2 MAINTAINING SECURITY OF THE SHIP/PORT INTERFACE 8.3 USAGE OF THE DECLARATION OF SECURITY 8.4 IMPLEMENTATION OF SECURITY PROCEDURES	1.0	



<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>


SUBJECT AREA	HOURS	
	L	D
<b>9. EMERGENCY PREPAREDNESS, DRILLS, AND EXERCISES (1.5 hours)</b> 9.1 CONTINGENCY PLANNING 9.2 SECURITY DRILLS AND EXERCISE 9.3 ASSESSMENT OF SECURITY DRILLS EXERCISES	0.5	1.0
<b>10. SECURITY ADMINISTRATION (1.5 HOURS)</b> 10.1 DOCUMENTATION AND RECORDS 10.2 REPORTING SECURITY INCIDENTS 10.3 MONITORING AND CONTROL 10.4 SECURITY AUDITS AND INSPECTIONS 10.5 REPORTING NONCONFORMITIES	1.5	
<b>11. SECURITY TRAINING (3.0 HOURS)</b> 11.1 TRAINING REQUIREMENTS 11.2 INSTRUCTIONAL TECHNIQUES	2.0	1.0
<b>TOTAL : 18.0 HOURS</b>	15.5	2.5

L – Lecture, D – Demonstration/Exercise

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPPS (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>


**COURSE TIMETABLE**

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
<b>Day 1</b>	<p><b>1. INTRODUCTION</b></p> <p>1.1. COURSE OVERVIEW</p> <p>1.2. COMPETENCES TO BE ACHIEVED</p> <p>1.3. HISTORICAL PERSPECTIVE</p> <p>1.4. CURRENT SECURITY THREATS AND PATTERNS</p> <p><b>2. MARITIME SECURITY POLICY</b></p> <p>2.1. RELEVANT INTERNATIONAL CONVENTIONS, CODES, CIRCULARS AND RECOMMENDATIONS INCLUDING THOSE THAT MAY RELATE TO PIRACY</p> <p>2.2. RELEVANT GOVERNMENT LEGISLATION AND REGULATIONS</p>	<p>2.3. DEFINITIONS</p> <p>2.4. HANDLING SENSITIVE SECURITY-RELATED INFORMATION AND COMMUNICATIONS</p> <p><b>3. SECURITY RESPONSIBILITIES</b></p> <p>3.1. CONTRACTING GOVERNMENTS</p> <p>3.2. RECOGNIZED SECURITY ORGANIZATIONS</p> <p>3.3. THE COMPANY</p> <p>3.4. THE SHIP</p> <p>3.5. THE PORT FACILITY</p> <p>3.6. SHIP SECURITY OFFICER</p> <p>3.7. COMPANY SECURITY OFFICER</p>	<p>3.8. PORT FACILITY SECURITY OFFICER</p> <p>3.9. SHIPBOARD PERSONNEL WITH DESIGNATED SECURITY DUTIES</p> <p>3.10. PORT FACILITY PERSONNEL WITH DESIGNATED SECURITY DUTIES</p> <p>3.11. OTHER PERSONNEL</p> <p><b>4. PORT FACILITY SECURITY ASSESSMENT AND ON-SCENE INSPECTIONS</b></p> <p>4.1. RISK ASSESSMENT METHODOLOGY</p> <p>4.2. ASSESSMENT TOOLS</p>	<p>4.3. ON-SCENE SECURITY INSPECTION</p> <p>4.4. SECURITY ASSESSMENT DOCUMENTATION</p>


	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
<b>Day 2</b>	<p><b>5. SECURITY EQUIPMENT</b></p> <p>5.1. SECURITY EQUIPMENT AND SYSTEMS</p> <p>5.2. OPERATIONAL LIMITATIONS OF SECURITY EQUIPMENT AND SYSTEMS</p> <p>5.3. TESTING, CALIBRATION AND MAINTENANCE OF SECURITY EQUIPMENT AND SYSTEMS</p> <p><b>6. PORT FACILITY SECURITY PLAN</b></p> <p>6.1. PURPOSE OF THE PORT FACILITY SECURITY PLAN</p>	<p>6.2. CONTENTS OF THE PORT FACILITY SECURITY PLAN</p> <p>6.3. CONFIDENTIALITY ISSUES</p> <p>6.4. DEVELOPMENT OF THE PORT FACILITY SECURITY PLAN</p> <p>6.5. APPROVAL OF THE PORT FACILITY SECURITY PLAN</p> <p>6.6. IMPLEMENTATION OF THE PORT FACILITY SECURITY PLAN</p>	<p>6.7. MAINTENANCE AND MODIFICATION OF THE PORT FACILITY PLAN</p> <p><b>7. THREAT IDENTIFICATION</b></p> <p>7.1. RECOGNITION, ON A NON-DISCRIMINATORY BASIS, OF PERSONS POSING POTENTIAL SECURITY RISK</p> <p>7.2. RECOGNITION AND DETECTION OF WEAPONS, DANGEROUS SUBSTANCES AND DEVICES</p> <p>7.3. IMPLEMENTING AND CO-ORDINATING SEARCHES</p> <p>7.4. METHODS OF PHYSICAL SEARCHES AND NON-INSTRUSIVE INSPECTIONS</p> <p>7.5. TECHNIQUES USED TO CIRCUMVENT SECURITY MEASURES INCLUDING THOSE USED BY PIRATES</p>	<p>7.6. CROWD MANAGEMENT AND CONTROL TECHNIQUES</p> <p><b>8. PORT FACILITY SECURITY ACTIONS</b></p> <p>8.1. ACTIONS REQUIRED BY DIFFERENT SECURITY LEVELS</p> <p>8.2. MAINTAINING SECURITY OF THE SHIP/PORT INTERFACE</p> <p>8.3. USAGE OF DECLARATION OF SECURITY</p> <p>8.4. IMPLEMENTATION OF SECURITY PROCEDURES</p>



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
<b>Day 3</b>	<b>9. EMERGENCY PREPAREDNESS, DRILLS, AND EXERCISES</b> 9.1. CONTINGENCY PLANNING 9.2. SECURITY DRILLS AND EXERCISES 9.3. ASSESSMENT OF SECURITY DRILLS AND EXERCISES	<b>10. SECURITY ADMINISTRATION</b> 10.1. DOCUMENTATION AND RECORDS 10.2. REPORTING SECURITY INCIDENTS 10.3. MONITORING AND CONTROL 10.4. SECURITY AUDITS AND INSPECTIONS 10.5. REPORTING NONCONFORMITIES	<b>11. SECURITY TRAINING</b> 11.1. TRAINING REQUIREMENTS 11.2. INSTRUCTIONAL TECHNIQUES	11.2. INSTRUCTIONAL TECHNIQUES (contd)

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

## **MANUAL**

### **1. Introduction**

#### **1.1. Course overview**

As with other IMO Model Courses the starting point should be a brief statement of the purpose of the course, a short review of the timeline, an introduction of participants, determination of knowledge and experience levels, and a brief description of the teaching facility.

#### **1.2. Competencies to be achieved**

Instructors should emphasize that no one is being trained to fight or similarly respond to security threats but rather that trainees should be able to identify, deter, or mitigate such actions through proper planning, preparation, and coordination with various entities.


#### **1.3. Historical perspective**

Trainees are most likely to appreciate the seriousness and proportions of the problem of security in general and maritime security in particular, if they have a sense of the relevant history. Notable examples of security incidents should be relayed to this end. These might include the ACHILLE LAURO in 1985, Pan Am Flight 103 in 1988, the Mumbai bomb blasts of 1993, the World Trade Center bombing in 1993, the hijackings of the M.T. PETRO RANGER in 1998 and the M.V. ALONDRA RAINBOW in 1999, the bomb attack on the USS COLE in 2000, the hijacking of the M.V. INABUKWA in 2001, the terrorist attacks of September 11, 2001 on the World Trade Center and the Pentagon, the hijacking of the MT HAN WEI in 2002 and the explosion of the Limburg in 2002. Examples of piracy and hijacking incidents should also be included and a special mention should be made to the incidents in the Gulf of Aden where numerous ships, along with their crew, have been held for ransom for as long as eight months.

#### **1.4. Current security threats and patterns**

Current threats to maritime security should be summarized in order to provide a basis for understanding of the recent conventions and legislation in this area and to fully grasp the importance of the training provided by this course. The prospective security officers receiving this training must clearly sense the reality of today's security issues, which include Some may have adopted a mindset that places the problem of security in the past or in such a remote corner that it appears distant or irrelevant. Before continuing on with the course this mindset should be identified and addressed.

Piracy and armed attacks continue to occur on an all too frequent basis. Attacks occur mostly in port areas whereas piracy by definition usually occurs on ships at sea. In fact, the United Nations Convention on the Law of the Sea, Article 101, defines piracy as any of the following acts: illegal acts of violence or detention or any act of depredation committed for private ends

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

by the crew or the passengers of a private ship or private aircraft and directed on the high seas against another ship or aircraft or against persons or property on board such ship or aircraft. It also includes such acts against a ship, aircraft, person or property in a place outside of the jurisdiction of any State.

Terrorism usually involves violence or the threat of violence by extremist groups seeking to gain political objectives by malicious means. A terrorist group may hope to make a statement by using various types of bombs, making bomb threats or hijacking a ship. Increasingly, terrorists are acting in connection with extremist religious sects that promote suicidal behavior.

Contraband smuggling, a criminal activity, may result in large financial loss to the shipowner whose ship is being used by the smugglers. Often drugs are the commodity being smuggled and they may be brought on board in a number of creative ways such as in luggage, stores, on or in a person's body, or in electronic equipment. Weapons are also a frequent item associated with smuggling. Like drugs, weapons, too, find their way on board in creative ways, such as cargo containers.

Cargo theft, an age-old problem, continues to plague the maritime industry and causes financial losses in staggering amounts. Prevention is normally the most effective method of dealing with this security threat. Although there may not be violence or political issues involved in most cargo theft cases, this matter remains high on the list of security threats and requires solutions discussed in this course. Instructors should convey that cargo theft is only one of the various threats to the security of cargo. Other such security threats should be discussed during this section of the course.


Collateral damage occurs when a nearby fire, explosion, or attack results in damage to a ship or facility. While the damage is sometimes unintended, the costs are nevertheless real.

There are measures that may minimize the consequences of this type of damage.

## **2. Maritime Security Policy**

### **2.1. Relevant international conventions, codes, circulars and recommendations including those that may relate to piracy**

The meeting of the Diplomatic Conference in December of 2002, resulted in amendments to SOLAS 74 in which Chapter XI-2 "Special Measures to Enhance Maritime Security" was added. Chapter XI-2 as well as the ISP code should be explained briefly at this stage. In addition, various IMO circulars providing guidance relating to implementation of SOLAS Chapter XI-2 and the ISPS code, as well as IMO circulars on guidance related to Piracy and Armed Robbery against ships, can be listed here. These will be studied in more depth in later sections of the course.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

It must be emphasized, at the stage, that guidance given in Part B is not optional. As stated in SOLAS XI-2, Reg 4, companies and ships are required to comply with Part A of the ISPS code, taking into account guidance given in Part B of the ISPS code. Similarly, in Reg 10, port facilities are required to comply with Part A of the code, taking into account guidance given in Part B. As advised in the preamble to the ISPS code, the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/ or cargo.

A common problem that seafarer's face in some ports is the refusal of port facilities to grant seafarers shore leave because of security concerns. Trainees should be advised that Resolution 11 of the 2002 SOLAS Conference explicitly requires that the human element needs to be taken into account when establishing an ISPS security regime.

### **2.2. Relevant government legislation and regulations**

It will be helpful for trainees to understand that some governments have acted on a national level to produce legislation and/or regulations concerned with measures to enhance maritime security. Instructors may wish to use examples developed by their own national and/or of other countries to illustrate the focus of this section of the course.

### **2.3. Definitions**


Trainees will need a working knowledge of several terms found in SOLAS Chapter XI-2 Regulation 1 and in the ISPS Code Part A section 2. These terms may well need clarification by an experienced instructor in order for trainees to reach the necessary level of understanding. For instance, it might require emphasis or other clarification by the instructor to establish that the Ship Security Officer is a person on board the ship and in that sense it may be impossible for a Company Security Officer to also act as the Ship Security Officer.

### **2.4. Handling sensitive security-related information and communications**

Trainees should understand that certain information and communications will be considered security sensitive and that the level of sensitivity may change, as do levels of security 1,2 and 3. Seemingly benign conversation, therefore, may result in disastrous consequences. All personnel will need to appreciate the risk of security leaks through communication by improper methods or to the wrong persons.

## **3. Security Responsibilities**

This section is intended to give trainees a clear picture of the proportions of the maritime security system conceived of by the IMO and to show how the various entities will work together to form an efficient and effective whole.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### **3.1. Contracting governments**

SOLAS Chapters XI-1 and XI-2 discuss the roles of the contracting Governments and their obligations in the overall scheme to enhance maritime security. A brief understanding of this will help the trainee to comprehend how and why their own governments have acted and how they may experience the port state control exercised by another Government.

Whilst describing the contracting Governments' roles in setting the security alert, it must be clarified that only Government or the designated authority set security levels for their port facilities and administrations for ships. If, however, an imminent threat poses a security risk to a ship or port facility, and an immediate response is required, the ship and port facility can take action as required at a higher security level. Trainees should also be informed that although the ship can operate at a higher security level than the port, a ship can never operate at a lower security level than that applying to the port or port facility it is in.

### **3.2. Recognized Security Organizations**


Recognized Security Organizations are defined in SOLAS Chapter XI-2 and discussed throughout Parts A and B of the ISPS Code. The trainee should understand how and when an RSO may take on the security related activities of a contracting government.

### **3.3. The company**

The company is defined by SOLAS Chapter XI-1 and is given numerous obligations under Chapter XI-2 and the ISPS Code from Continuous Synopsis Records to the maintenance of the International Ship Security Certificate. Trainees would benefit greatly from a clear understanding of the role of the company and the support that they should expect from the company.

### **3.4. The ship**

The term ship as used here means a ship to which Chapter XI of SOLAS applies. Various segments of Chapter XI and the ISPS Code discuss the persons, activities, plans, documentation and so forth that a ship will be exposed to in a security context. All trainees will need to understand these requirements, as they relate to this important cornerstone of a maritime transportation system.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### 3.5. The port facility

The Port Facility is defined in SOLAS Chapter XI-2 Regulation 1 part 1.9 and is the location where a ship/port interface takes place. As such, numerous duties and activities are assigned to the Port Facility. All trainees should understand the role of the Port Facility in maintaining the security of a maritime transportation system.

### 3.6. -3.11 Ship Security Officer, Company Security Officer, Port Facility Security Officer, Shipboard personnel with specific security duties, Port facility personnel with Designated security duties, and Other personnel

Trainees should understand the role of each of these various persons and know what to expect from each in terms of authority and responsibility. The ISPS Code Parts A and B, as well as the STCW Code clearly delineate the functions, duties, and training requirements for each of these categories of personnel. In the end these are the very people that will make the security plans work and will recognize areas for improvement. They will each need to appreciate their own role as well as that played by the others.


## 4. Port Facility Security Assessment

### 4.1. Risk assessment methodology

Port facility security assessment is an essential and integral part of the process of developing and updating the Port Facility Security Plan. In this segment of the course, it should be communicated to trainees that risk-based decision-making is one of the best tools available to complete a security assessment and to determine appropriate security measures for a port facility. Risk based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions to reduce the vulnerability and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses.

Trainees should learn that the Port Facility Security Officer may delegate the assessment to a person(s) with skills to evaluate the security of a facility and carry out the Port Facility Security Assessment. They should also know that the Port Facility Security Assessment may be conducted by a Recognized Security Organization, but that approval of a completed Port Facility Security Assessment should only be given by the relevant Contracting Government.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

Prior to commencing a Port Facility Security Assessment, the Port Facility Security Officer should obtain current information on the assessed threat for the local area and should be knowledgeable about the types of vessels calling on the facility. The Port Facility Security Officer should identify and evaluate possible threats to key facility operations, assets and infrastructure, and the likelihood of their occurrence, in order to establish and prioritize security measures.

The Port Facility Security Officer should study previous reports on similar security requirements. When feasible, the Port Facility Security Officer should consult with appropriate port personnel and other Port Facility Security Officers on the methodology and aspects of the assessment. The Port Facility Security Officer should examine access points, including rail access, roads, waterside, and gates, and evaluate their potential for use by unauthorized individuals who may cause transportation security incidents. This includes individuals with legitimate access as well as those who seek to obtain unauthorized entry.

Detailed guidance concerning methodologies for risk-based security assessment is provided in the ISPS Code Part B.

#### **4.2. Assessment tools**


Trainees in the Port Facility Security Officer course must be encouraged to adopt systematic and consistent approaches to the evaluation of security conditions and vulnerabilities. The use of checklists to perform inspections of security in day-to-day operations should be discussed, noting the inclusion of categories such as the following:

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

#### **4.3. On-scene security inspection**

It should be imparted to trainees that the Port Facility Security Assessment should include an on-scene security assessment and evaluation of the facility, to include the following elements:

- The general layout of the port facility;
- The location and function of each actual or potential access point to the port facility;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

- Existing protective measures including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;
- Numerical strength, reliability, and security duties of the port facility's personnel;
- Security doors, barriers, and lighting.
- The location of areas which should have restricted access, such as control stations, communications centers, cargo storage areas, etc.;
- The emergency and stand-by equipment available to maintain essential services;
- Response procedures for fire or other emergency conditions;
- Existing security and safety equipment for protection of personnel and visitors;
- The level of supervision of the port facility's crew, vendors, repair technicians, dock workers, etc.;
- Existing agreements with private security companies providing port facility security services at all security levels, including any security forces contracted by visiting vessels;
- Procedures for control of security keys and other access prevention systems;
- Cargo and vessel stores operations; and
- Response capability to incidents.

#### **4.4. Security assessment documentation**

In addition to periodic updates and reviews, the Port Facility Security Assessment provides the opportunity for the owners to monitor compliance with the Port Facility Security Plan and make amendments as necessary.

Trainees should understand that the Port Facility Security Assessment should be documented and retained by the port facility. The Port Facility Security Assessment should be performed periodically, taking account of changing threats and/or significant changes in the port facility.

It should be noted that the report must be protected from unauthorized access or disclosure.


### **5. Security Equipment**

#### **5.1. Security equipment and systems**

Course participants should be aware of the types of security equipment and systems that are useful in enhancing maritime security, both ashore and afloat. Examples of such equipment include:

- AIS



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

- Ship Security Alert System
- Locks
- Lighting
- Handheld radios
- GMDSS equipment
- Closed Circuit Televisions
- Automatic Intrusion Detection Device (Burglar Alarm)
- Metal detectors
- Explosive detectors
- Baggage screening equipment
- Container X-ray devices
- General alarm

Participants are not expected to acquire detailed technical or scientific knowledge concerning the theoretical underpinnings of the operation of security equipment. The objective is to ensure familiarity with the capabilities and appropriate deployment of such devices and systems. The Port Facility Security Officer may well be in the position to influence the purchase and installation of security equipment and should be able to evaluate the security equipment for shipboard use. Instructors are encouraged to discuss this possibility as well as the resultant additional level of knowledge with trainees.

The instructor should also explain how passive and non-lethal measure such as netting, barbed/razor wire, electric fencing, long-range acoustic devices, etc., can be used as preventive measures to deter attackers and delay boarding in case of attack by pirates and armed robber. Even a simple act such as the application of grease on railing can delay boarding. The use of water hoses also be discussed. Safety precautions related to the use of these devices must be explained on the trainees.


### **5.2. Operational limitations of security equipment and systems**

The intent of this course segment is to communicate to trainees the functional limitations and operating constraints of security equipment that they may encounter or be called upon to use.

Issues such as effective range, environmental sensitivities, and operator (human) error should be addressed as appropriate.

### **5.3. Testing, calibration and maintenance of security equipment and systems**

Trainees should be familiar with methods for ensuring the continuing accuracy, efficiency, and operational readiness of selected items of security equipment and associated systems. They

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

should understand the need for developing methods to ensure that the tasks and procedures required to support such equipment while the vessel is at sea are in place and are adhered to.

## **6. Port Facility Security Plan**

### **6.1. Purpose of the Port Facility Security Plan**

The Port Facility Security Plan is defined in the ISPS Code Part A Section 2.1 as a plan that will ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident. Therefore it is imperative that all candidates for the Port Facility Security Officer position fully understand the nature of the Port Facility Security Plan. The Port Facility Security Officer is responsible for the development, implementation, revision, and maintenance of the Port Facility Security Plan and for liaison with Ship Security Officers and Company Security Officers.

### **6.2. Contents of the Port Facility Security Plan**


The contents of the Port Facility Security Plan are most clearly established in the ISPS Code Part A section 16 with additional information provided in Section 16 of Part B of the Code. Trainees should be intimately familiar with the contents of the plan in a generic fashion thus providing a basis for easy transition to the role of Port Facility Security Officer at the port facilities to which they may be assigned. It is suggested that a completed sample plan be provided by instructors to give trainees a better opportunity to understand the document to which they must be responsive in their role as Port Facility Security Officer.

### **6.3. Confidentiality issues**

The Port Facility Security Plan is to be considered a confidential document and must be protected from unauthorized access or disclosure. Instructors should place notable emphasis on this.

### **6.4. Development of the Port Facility Security Plan**

The Port Facility Security Officer is responsible to ensure that the Port Facility Security Plan is prepared and submitted for approval. Instructors should have already addressed the process of port facility security assessment that leads up to development of the Port Facility Security Plan. Trainees should understand that all security measures in the Port Facility Security Plan must be in place within a reasonable amount of time from the date of the plan's approval.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### **6.5. Approval of the Port Facility Security Plan**

Ensuring that the Port Facility Security Plan is ultimately approved is the duty of the Port Facility Security Officer and therefore the Port Facility Security Officer trainee must have a clear understanding of the approval process in order to properly manage it. This section of the course explains the requirements and conditions for approval of the Port Facility Security Plan and that it must be accompanied by a completed Port Facility Security Assessment upon application for approval.

### **6.6. Implementation of the Port Facility Security Plan**

Implementation of the Port Facility Security Plan is the responsibility of the Port Facility Security Officer. Section 16 of the ISPS Code Part B is very helpful in determining appropriate material for use by instructors in conveying the details of the implementation of a Port Facility Security Plan.

### **6.7. Maintenance and modification of the Port Facility Security Plan**


The Port Facility Security Plan is intended to address security measures for each of the three security levels but on further inspection it can be seen that the Port Facility Security Plan is a living document and will require modification over time. Trainees must understand not only the provisions set out by the Port Facility Security Plan but also their role in maintaining its effectiveness and contributing to positive modifications of the plan over time. Instructors should consider creating an exercise or a sample scenario showing the proper method of maintenance, realization of the need for modification, the proper route to follow for suggesting modifications, and the approval necessary before a modification or amendment can be set in place as new policy.

## **7. Threat Identification, Recognition, and Response**

### **7.1. Recognition, on a non-discriminatory basis, of persons posing potential security risks**

Instructors should explain suspicious patterns of behavior, while emphasizing the importance of avoiding racial profiling and ethnic stereotyping. Example of suspicious behaviors includes:

- Unknown persons photographing vessels or facilities.
- Unknown persons attempting to gain access to vessels or facilities.
- Individuals establishing businesses or roadside food stands either adjacent or in proximity to facilities.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>


- Unknown persons loitering in the vicinity of ships or port facilities for extended periods of time.
- Unknown persons telephoning facilities to ascertain security, personnel, or standard operation procedures.
- Vehicles containing personnel loitering and perhaps taking photographs or creating diagrams of vessels or facilities.
- Small boats, with personnel on board, loitering and perhaps taking photographs or creating diagrams of vessels or facilities.
- General aviation aircrafts operating in proximity to vessels or facilities.
- Persons who may be carrying bombs or participating in suicide squad activities.
- Unknown persons attempting to gain information about vessels or facilities by walking up to personnel or their families and engaging them in conversation.
- Vendors attempting to sell merchandise.
- Workmen trying to gain access to facilities to repair, replace, service, or install equipments.
- E-mails attempting to obtain information regarding the facilities to repair, replace, service, or install standard operating procedures.
- Package drop-offs/attempted drop-offs.
- Anti-national sentiments being expressed by employees or vendors.
- Anti-national pamphlets or flyers distributed to employees or placed on windshields in parking lots.
- Out-of-the-ordinary phone calls.
- Recreational boaters or persons aboard refugee craft posing as mariners in distress to attract assistance from other vessels.

### **7.2. Recognition and detention of weapons, dangerous substances and devices**

The focus of this session is on the characteristics and potential effects of prohibited weapons, explosives; chemical, biological, and radiological devices; substances and compounds that pose a hazard to personnel, ships and facilities; and other related topics.

### **7.3. Implementing and co-ordinating searches**

Trainees should be taught that, to ensure that a thorough and efficient search is completed in the shortest possible time, search plans should be prepared in advance. The search plan should be comprehensive, and should detail the routes searchers should follow and the places on the route where weapons, devices, dangerous substances, etc. might be hidden.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

The plan should be developed in a systematic manner to cover all options and to ensure no overlap or omission. This allows those responsible to concentrate on the actual search without worrying about missing something.


Trainees should be acquainted with the utility of “check cards” in conducting systematic searches. For example, a “check card” is a card that can be issued to each searcher specifying the route to follow and the areas to be searched. These cards can be colour-coded for different areas of responsibility, for example blue for deck, red for engine room. On completion of individual search tasks, the cards are returned to a central control point. When all cards are returned, the search is known to be complete.

Course participants should be familiar with the basic equipment that may be employed in conducting searches. This list may include:

- flashlights and batteries;
- screwdrivers, wrenches and crowbars;
- mirrors and probes;
- gloves, hard hats, overalls and non-slip footwear;
- Plastic bags and envelopes for collection of evidence;
- forms on which to record activities and discoveries.

Trainees should learn procedures to be followed so as to ensure effective and efficient searches. Examples of these include the following:

- Crew members and facility personnel should not be allowed to search their own areas in recognition of the possibility that they may have concealed packages or devices in their own work or personal areas
- The search should be conducted according to a specific plan or schedule and must be carefully controlled.
- Special consideration should be given to search parties working in pairs with one searching “high” and one searching “low”. If a suspicious object is found, one of the pair can remain on guard while the other reports the find.
- Searchers should be able to recognize suspicious items.
- There should be a system for marking or recording “clean” areas
- Searchers should maintain contact with the search controllers, perhaps by UHF / VHF radio, bearing in mind the dangers of using non-intrinsically safe radio equipment in the vicinity of Improvised Explosive Devices (IEDs)
- Searchers should have clear guidance on what to do if a suspect package, device, or situation is found.
- Searchers should bear in mind that weapons and other dangerous devices may be intentionally placed to match its context as a means of disguise, such as a toolbox in an engine room.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

Participants in the course should be acquainted with the fact that there are many places in board a ship where weapons, dangerous substances, and devices can be concealed. Some of these are:

#### **Cabins**

- Back, sides and underneath drawers
- Between bottom drawer and deck
- Beneath bunks, e.g. taped to bunk under mattress
- Under a washbasin
- Behind removable medicine chest
- Inside radios, recorders, ect
- Inside ventilator ducts
- Inside heater units
- Above or behind light fixtures
- Above ceiling and wall panels
- Cut-outs behind bulkheads, pictures, etc.
- False bottom clothes closets – hanging clothes
- Inside wooden clothes hangers
- Inside rolled socks, spare socks
- Hollowed-out melding


#### **Companionways**

- Ducts
- Wire harnesses
- Railings
- Fire extinguishers
- Fire hoses and compartments
- Access panels in floor, walls, ceilings
- Behind or inside water coolers, igloos

#### **Toilet and showers**

- Behind and under washbasins
- Behind toilets
- In ventilation ducts and heaters
- Toilet tissue rollers, towel dispensers, supply lockers
- Taped to shower curtains, exposed piping, and light fixtures
- Access panels in floor, walls, ceiling

#### **Deck**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

- Ledge on deck housing, electrical switch rooms, winch control panels
- Lifeboat storage compartments, under coiled rope, in deck storage rooms
- Paint cans, cargo holds, battery rooms, chain lockers

#### Engine room

- Under deck plates
- Cofferdams, machinery pedestals, bilges
- Journal-bearing shrouds and sumps on propeller shaft
- Under catwalk, in bilges, in shaft alley
- Escape ladders and ascending area
- In ventilation ducts, attached to piping or in tanks with false gauges
- Equipment boxes, emergency steering rooms, storage spaces

#### Galleys and stewards' stores


- Flour bins and dry stores
- Vegetable sacks, canned foods (re-glued labels)
- Under or behind standard refrigerators
- Inside fish or sides of beef in freezers
- Bonded store lockers , slop chest, storage rooms

#### 7.4. Methods of physical searches and non-intrusive inspections

In this segment of the course, trainees will learn techniques used to conduct physical and non-instructive searches of persons, personal effects, baggage, cargo, and a ship's stores. Trainees should be informed that, unless there are clear security ground for doing so, members of the ship's crew should not be required to search their colleagues or their personal effects. It should be conveyed that any such search shall be undertaken in a manner that fully takes into account the human rights of the individual and preserves his or her basic human dignity.

#### 7.5. Techniques used to circumvent security measures including those used by pirates

Trainees should be cautioned that no security equipment or measure is infallible. They should be apprised of the known techniques that can be employed to evade security systems and controls, such as the disabling of alarm systems, picking of locks, jamming of radio signals, etc.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### **7.6. Crowd management and control techniques**

Course participants should be familiarized with the basic patterns of behavior of people in groups during time of crisis. The critical importance of clear communication with vessel personnel, port facility personnel, passengers, and others involved should be underscored.

## **8. Port Facility Security Actions**

Parts A and B of the ISPS Code are helpful in organizing material to be conveyed in this section of the course. Instructors should convey that this section of the course is where ideas, plans, and preparation turn into actions and procedures.

### **8.1. Actions required by different security levels**

The instructor should convey the different types of security measures that should be considered for the various security levels that may be set. Feedback from or discussion among the trainees will help in deciding whether or not the necessary knowledge is being conveyed. Trainees may benefit from an in-class creation of a checklist detailing the appropriate generic actions given various conditions.


### **8.2. Maintaining security of the ship/port interface**

The ship/port interface is defined in SOLAS Chapter XI-2 Regulation 1. It is this interface that determines that a port facility exists and therefore determines the need for a Port Facility Security Plan and the interaction with the Ship Security Plan. The security levels of the port and the ship, with liaison services provided by the Company Security Officer, will allow the Port Facility Security Officer and the Ship Security Officer to understand their duties and constraints. Instructors should ensure that trainees are clear on the critical importance of the interaction between the shipboard security plan and that of the port facility.

### **8.3. Usage of the Declaration of Security**

The Declaration of Security (DoS) is defined in Regulation 1 of SOLAS Chapter XI-1. The ISPS Code further describes the function of the Declaration of Security, when it should be completed, who may initiate it, and who is required to sign it. There is a sample Declaration of Security in Appendix 1 of Part B of the ISPS Code, which may be helpful in explaining the nature and use of the Declaration of Security.



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

The trainees must also be advised that a DoS is not a routine document and therefore not required to be signed for each ship/port interface. The DoS is intended to be used in exceptional cases usually related to higher risk, when there is a need to reach an agreement between the port facility and the ship as to the security measures to be applied during the ship/port interface, because either the provisions of the PFSP and the SSP did not envisage the situation or have not anticipated the specific circumstances as listed in the ISPS Code. There should be a security-related reason relating to the specific ship/port interface or ship-to-ship activity for requiring or requesting completion of a DoS.

#### **8.4. Implementation of security procedures**

Building on the understanding gained from previous sections in this course, trainees should be ready to synthesize the requirements and plans into actual procedures such as security inspections, controlling access to the ship, monitoring port areas and areas surrounding the ship, and so forth.

### **9. Emergency Preparedness, Drills, and Exercises**

#### **9.1. Contingency planning**


This portion of the course is concerned with incident response planning for a variety of contingencies associated with terrorism and other criminal activities that may arise in the maritime setting. Appropriate action to be taken in the case of bomb threats, explosions, piracy, hijackings, and similar events should be discussed.

#### **9.2. Security drills and exercises**

It should be conveyed to participants in the Port Facility Security Officer course that the objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties at all security levels and in the identification of any security related deficiencies, which need to be addressed

Trainees should learn that the effective implementation of the provisions of the Port Facility Security Plan requires that drills be conducted at least once every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as:

- damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the ship or of persons on board; why double space
- tampering with cargo, essential ship equipment or systems or ship's stores;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

- unauthorized access or use including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the ship to carry those intending to cause a security incident and their equipment;
- use of the ship itself as a weapon or as a means to cause damage or destruction; blockage; of port entrances, locks, approaches etc; and
- nuclear, biological and chemical attack

It should be conveyed to trainees that various types of exercises that may include participation of Port Facility Security Officers, in conjunction with relevant authorities of Contracting Governments, Company Security Officers, or Ship Security Officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of Company Security Officers or Ship Security Officers in joint exercises should be made bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response. These exercises may be:

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


### **9.3. Assessment of security drills and exercises**

Participants should learn that at the end of each drill or exercise, the Port Facility Security Officer shall review the drill or exercise, and ensure that any mistakes made or deficiencies identified are corrected. All personnel involved shall give their comments on the effectiveness of the drill to the Port Facility Security Officer, who is responsible for ensuring that port facility personnel understand their security responsibilities.

## **10. Security Administration**

### **10.1. Documentation and records**

Drawing on Part B of the ISPS Code and Appendix B thereto the instructor will find sufficient references to, and examples of, required documents as well as requirements for record keeping. The Statement of Compliance of a Port Facility should be the main emphasis here. Records of activities addressed in the Port Facility Security Plan must be kept for certain time periods that are determined by administrations.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### **10.2. Reporting security incidents**

Trainees will appreciate that all security incidents must be reported in accordance with specific reporting requirements. It may be helpful for instructors to provide several sample security incidents and have the class or individuals explain how they would go about reporting these incidents.

### **10.3. Monitoring and control**

Here the focus of monitoring is on the Port Facility Security Plan itself. Proper administration of the plan requires that the Port Facility Security Officer review the Port Facility Security Plan and measure its effectiveness and relevance over time.

### **10.4. Security audits and inspections**

In a fashion similar to the ISM Code, IMO requires that audits and inspections be conducted to formally assess the effectiveness of the Port Facility Security Plan in all respects. The ISPS Code provides sufficient material for instruction in this area.


### **10.5. Reporting nonconformities**

The audit, inspection, and periodic review process required by the ISPS Code naturally calls for a means of identifying, communicating, and rectifying non-conformities. The Port Facility Security Officer plays a key role in the effort to keep the Port Facility Security Plan in an optimum condition.

## **11. Security Training**

### **11.1. Training requirements**

The training requirements set out under the ISPS Code can be found in Parts A and B of the Code and should be explained to the trainees. Instructors should clarify the requirements for who needs to be trained, what the training consists of, and where the responsibility lies for the training of various persons involved in maritime security. Under the ISPS Code Part A section 17 the Port Facility Security Officer is given the duty and responsibility to ensure adequate training for all personnel responsible for the security of the port facility. A thorough understanding of the requirements for such training is therefore imperative.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-ISPSP (I)-19</b>
	<b>PORT FACILITY SECURITY OFFICER</b>	<b>REV. 4 -2015</b>

### **11.2. Instructional techniques**

Given that the Port Facility Security Officer carries the burden of ensuring that proper training in the appropriate subjects is provided to all port facility personnel responsible for the security of the port facility, the Port Facility Security Officer should have a clear understanding of instructional techniques. This information may be used directly by the Port Facility Security Officer as instructor or may be employed by the Port Facility Security Officer in evaluating instructional programs being used by, or being considered for use by the port facility.

CONTROLLED COPY