
	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015



**COMPANY SECURITY
OFFICER**

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

SCOPE

This course has been based on MSC/Circ 1154, "Guidelines on training and certifications for Company Security Officers", and aims to provide knowledge to those who may be designated to perform the duties and responsibilities of a Company Security Officer (CSO), as defined in paragraph 2.1.7 (and paragraph 11) of the ISPS Code, Part A. In particular, the duties and responsibilities with respect to the security of a ship, for ensuring the development (or for developing) of a ship security assessment, for ensuring the development (or for developing) of implementation, maintenance and updating of a ship security plan, and for liaising with Ship Security Officers (SSOs) and with Port Facility Security Officers (PFSOs).

OBJECTIVE

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

1. Develop, maintain and supervise the implementation of a ship security plan;
2. Assess security risk, threat, and vulnerability;
3. Ensure appropriate security measures are implemented and maintained;
4. Ensure that security equipment and any systems, if any, are properly operated; and
5. Encourage security awareness and vigilance.

ENTRY STANDARDS


It is assumed that those attending this course will be persons employed (or to be employed) by a company and that they are likely to be designated as Company Security Officer.

COURSE CERTIFICATE, DIPLOMA OR DOCUMENT

Documentary evidence should be issued to those who have successfully completed this course indicating that the holder has completed training as "Company Security Officer".

COURSE INTAKE LIMITATIONS

The maximum number of trainees will 25 persons.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

STAFF REQUIREMENTS

The instructor in charge of the course have completed a Company Security Officer course or, alternatively, have adequate experience in maritime security matters.

The instructors should either have appropriate training in or be familiar with instructional techniques and training methods.

TEACHING FACILITIES AND EQUIPMENT

An ordinary classroom or similar meeting room with a blackboard or equivalent is sufficient for the lectures.

TEACHING AIDS

Instructor Manual.

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

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

BIBLIOGRAPHY AND WEBSITE

Violence at Sea: Piracy in the Age of Global Terrorism, Peter Lehr, Lloyds Marine Intelligence Unit.

Contemporary Piracy and Maritime Terrorism, Martin N. Murphy, Adelphi Paper.

Dangerous Waters, John Burnett

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

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

International Chamber of shipping (2003). Maritime Security: Guidance for Ship Operators on the IMO International Ship and Port Facility Security Code. London: ICS.

International Chamber of shipping (2003). Model Ship Security plan. London: ICS.

International Chamber of Shipping / International Shipping Federation (1999).

United States Coast Guard. Risk-based Decision Making.



SEAFARERS TRAINING CENTER

M-CSO (I)-18

COMPANY SECURITY OFFICER

REV. 5 -2015

**TIMETABLE
COURSE OUTLINE**

SUBJECT AREA	HOURS	
	L	D
1. INTRODUCTION (1.0 HOURS) 1.1 COURSE OVERVIEW 1.2 COMPETENCE TO BE ACHIEVED 1.3 HISTORICAL PERSPECTIVE 1.4 CURRENT SECURITY THREATS AND PATTERNS	1.0	
2. MARITIME SECURITY (1.0 HOURS) 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	
3. SECURITY RESPONSIBILITIES (1.5 HOURS) 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	
4. PORT FACILITY SECURITY ASSESSMENT AND ON-SCENE INSPECTIONS (2.5 HOURS) 4.1 RISK ASSESSMENT METHODOLOGY 4.2 ASSESSMENT TOOLS 4.3 ON-SCENE SECURITY INSPECTION 4.4 SECURITY ASSESSMENT DOCUMENTATION	2.0	0.5
5. SECURITY EQUIPMENT (1.0 HOURS) 5.1 SECURITY EQUIPMENT AND SYSTEMS 5.2 OPERATIONAL LIMITATIONS OF SECURITY EQUIPMENT AND SYSTEMS 5.3 TESTING, CALIBRATION AND MAINTENANCE OF SECURITY EQUIPMENT AND SYSTEMS	0.5	0.5
6. SHIP SECURITY PLAN (2.5 HOURS) 6.1 PURPOSE OF THE SHIP SECURITY PLAN 6.2 CONTENTS OF THE SHIP SECURITY PLAN 6.3 CONFIDENTIALITY ISSUES 6.4 DEVELOPMENT OF THE SHIP SECURITY PLAN 6.5 APPROVAL OF THE SHIP SECURITY PLAN 6.6 IMPLEMENTATION OF THE SHIP SECURITY PLAN 6.7 MAINTENANCE AND MODIFICATION OF THE SHIP SECURITY PLAN	2.5	



SEAFARERS TRAINING CENTER

M-CSO (I)-18

COMPANY SECURITY OFFICER

REV. 5 -2015


SUBJECT AREA	HOURS	
	L	D
7. THREAT IDENTIFICATION (1.5 HOURS) 7.1 RECOGNITION, ON A NON-DISCRIMINATORY BASIS, OF PERSON POSING POTENTIAL SECURITY RISK 7.2 RECOGNITION OF THREATS DUE TO IMPEDING PIRACY ATTACK 7.3 RECOGNITION AND DETECTION OF WEAPONS, DANGEROUS SUBSTANCES AND DEVICES 7.4 IMPLEMENTING AND CO-ORDINATING SEARCHES 7.5 METHODS OF PHYSICAL SEARCHES AND NON- INSTRUCTIVE INSPECTIONS 7.6 TECHNIQUES USED TO CIRCUMVENT SECURITY MEASURES INCLUDING THOSE USED BY PIRATES 7.7 CROWD MANAGEMENT AND CONTROL TECHNIQUES	1.0	0.5
8. SHIP SECURITY ACTIONS (1.0 HOURS) 8.1 ACTION REQUIRED BY DIFFERENT SECURITY LEVELS, INCLUDING ACTIONS TO BE TAKEN TO PREVENT PIRACY AND ARMED ROBBERY 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	
9. EMERGENCY PREPAREDNESS, DRILLS, AND EXERCISE (2.0 hours) 9.1 CONTINGENCY PLANNING 9.2 SECURITY DRILLS AND EXERCISES 9.3 ASSESSMENT OF SECURITY DRILLS AND EXERCISES	2.0	
10. SECURITY ADMINISTRATION (1.0 HOURS) 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	1.0	
11. SECURITY TRAINING (3.0 HOURS) 11.1 TRAINING REQUIREMENTS 11.2 INSTRUCTIONAL TECHNIQUES	2.0	1.0
TOTAL : 18.0 HOURS	15.5	2.5

L – Lecture, D – Demonstration/Exercise


	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

COURSE TIME TABLE

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
1	1. INTRODUCTION 1.1. COURSE OVERVIEW 1.2. COMPETENCES TO BE ACHIEVED 1.3. HISTORICAL PERSPECTIVE 1.4. COURRENT SECURITY THREATS AND PATTERNS 2. MARITIME SECURITY POLICY 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 3. SECURITY RESPONSIBILITIES 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 OFICER 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 DUTIES 3.11. OTHER PERSONNEL 4. SHIP SECURITY ASSESSMENT AND ON-SCENE INSPECTIONS 4.1. RISK ASSESSMENT METHODOLOGY 4.2. ASSESSMENT TOOLS	4.3. ON-SCENE SECURITY INSPECTION 4.4. SECURITY ASSESSMENT DOCUMENTATION


	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
2	5. SECURITY EQUIPMENT 5.1. SECURITY EQUIPMENT AND SYSTEMS 5.2. OPERATIONAL LIMITATIONS OF SECURITY EQUIPMENT AND SYSTEMS 5.3. TESTING, CALIBRATION AND MAINTENANCE OF SECURITY EQUIPMENT AND SYSTEMS 6. SHIP SECURITY PLAN 6.1. PURPOSE OF THE SHIP SECURITY PLAN	6.2. CONTENTS OF THE SHIP SECURITY PLAN 6.3. CONFIDENTIALITY ISSUES 6.4. DEVELOPMENT OF THE SHIP SECURITY PLAN 6.5. APPROVAL OF THE SHIP SECURITY PLAN 6.6. IMPLEMENTATION OF THE SHIP SECURITY PLAN	6.7. MAINTENANCE AND MODIFICATION OF THE SHIP SECURITY PLAN 7. THREAT IDENTIFICATION 7.1. RECOGNITION, ON A NON-DISCRIMINATORY BASIS, OF PERSONS POSING POTENTIAL SECURITY RISK 7.2. RECOGNITION OF THREATS DUE TO IMPENDING PIRACY ATTACK 7.3. RECOGNITION AND DETECTION OF WEAPONS, DANGEROUS SUBSTANCES AND DEVICES 7.4. IMPLEMENTING AND CO-ORDINATING SEARCHES 7.5. METHODS OF PHYSICAL SEARCHES AND NON-INTRUSIVE INSPECTIONS 7.6. TECHNIQUES USED TO CIRCUMVENT SECURITY MEASURES INCLUDING THOSE USED BY PIRATES INCLUDING THOSE USED BY PIRATES	7.7. CROWD MANAGEMENT AND CONTROL TECHNIQUES 8. SHIP SECURITY ACTIONS 8.1. ACTIONS REQUIRED BY DIFFERENT SECURITY LEVELS, INCLUDING ACTIONS TO BE TAKEN TO PREVENT PIRACY AND ARMED ROBBERY 8.2. MAINTAINING SECURITY OF THE SHIP/PORT INTERFACE 8.3. USAGE OF DECLARATION OF SECURITY 8.4. IMPLEMENTATION OF SECURITY PROCEDURES

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

DAY/ PERIOD	PERIOD 1 (1.5 HOURS)	PERIOD 2 (1.5 HOURS)	PERIOD 3 (1.5 HOURS)	PERIOD 4 (1.5 HOURS)
3	9. EMERGENCY PREPAREDNESS, DRILLS, AND EXERCISES 9.1. CONTINGENCY PLANNING 9.2. SECURITY DRILLS EXERCISES 9.3 ASSESSMENT OF SECURITY DRILLS AND EXERCISES 10. SECURITY ADMINISTRATION 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	11. SECURITY TRAINING 11.1 TRAINING REQUIREMENTS INSTRUCTIONAL TECHNIQUES	11.2 INSTRUCTIONAL TECHNIQUES (CONT)

CONTROLLED

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

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.Competences to be Achieved

The aim of the course is stated, competences from the course are reviewed, and the outcome of learning objective is made clear; namely, that “the expected learning outcome is that the trainee is able to...”

Instructor 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 co-ordination with various entities.


1.3.Historical Perspective

Trainees are most likely to appreciate 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 Pentagon, the hijacking of the MT HAN WEI in 2002 and the explosion on board 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 piracy, terrorism, contraband smuggling, cargo theft, and collateral damage. 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 aboard ship at sea. In

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

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 any act of depredation committed for private ends 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 person 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. The summarizing of statistics concerning piracy and armed robbery may provide motivation to trainees to acquire knowledge and skills that would enable them to counter these threats where possible.

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 hijacking a ship. Increasingly, terrorist are acting in connection with extremist religious sects that promote suicidal behavior.

Contraband smuggling, a criminal activity, may result in large financial loss to ship owner whose ship is being used by smugglers. Often, drugs are the commodity being smuggled and they may be brought or 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 in cargo containers.


Cargo theft, an age 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 hitch on the list of security threats and requires solution 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 minimize the consequences of this type of damage.

2. Maritime security policy

2.1.Relevant international conventions, codes, and recommendation 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 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 Armed Robbery against can be listed here. These will be studied in more depth in later sections of the course.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

It must be emphasized, at this 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 seafarer's 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 regulation

Trainee will be helpful for trainees to understanding that some Governments have acted on a national level to produce legislation and/or regulations concerned with measures to enhanced maritime security. Instructors may wish to use examples developed by their own nations and /or those 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 and the Best Management Practices to Deter Piracy off the Coast of Somalia and the Arabian Sea Area (BMP3). These terms may well need clarification may an experienced instructor in order for trainees to reach the necessary levels of understanding. For instance, it might require emphasis or other clarification by the instructor to establish that the Ship Security Office is a person on board the ship and in that sense it may be impossible for a Company Security Officer to also act 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 conversations, therefore, may result in disastrous consequences.

All personnel will need to appreciate the risk of security leaks trough communication by improper methods or to the wrong persons.

3. Security responsibilities

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

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

3.1. Contracting governments

SOLAS Chapters XI-1 and XI-2 discuss the roles of contracting Governments and their obligations in the overall scheme to enhance maritime security. And understanding of this will help trainees to comprehend how and why 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 Governments or the designated authority set security levels for their port facilities and administrations for ships. If, however, an imminent threat imposes a security risk to a ship or port facility, and an immediate response is 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 will 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

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 designated 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 Part 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

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

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. Trainees should also understand the role of personnel in organizations that are involved in responding to attacks and attempted attacks by pirates and armed robbers.

4. Ship security assessment and on-scene inspections

4.1. Risk assessment methodology

Ship security assessment is an essential and integral part of the process of developing and updating the ship 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 to complete a security assessment and to determine appropriate security measures for a vessel. 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.

4.2. Assessment tools

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

- General layout of the ship;
- Location of areas that should have restricted access, such as the bridge, engine room, radio room, etc.;
- Location and function of each actual or potential access point to the ship;
- Open deck arrangement including the height of the deck above water;
- Emergency and stand-by equipment available to maintain essential services;
- Numerical strength, reliability, and security duties of the ship's crew;
- Existing security and safety equipment for protecting the passengers and crew;
- Existing agreements with private security company for providing ship and waterside security services;
- Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

4.3. On scene-security inspection

Trainees in the Company Security Officer course should be taught that the on-scene security survey is an integral part of any Ship Security Assessment. They should understand that the survey should fulfill the following functions:

- Identification of existing security measures, procedures and operations;
- Identification and evaluation of key shipboard operations that is important to protect;
- Identifications of possible threats to the key shipboards operation and the likelihood of their occurrence, in order to establish and prioritize security measures; and



- Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

It should be emphasized to course participants that the on-scene inspection should examine and evaluate existing shipboard protective measures, procedures and operation for:

- Ensuring the performance of all ship security duties;
- Monitoring restricted areas to ensure that only authorized persons have access;
- Controlling access to the ship, including any identification systems;
- Monitoring of deck areas and areas surrounding the ship both at sea and in port, with particular attention to the prevention of piracy and armed robbery;
- Controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and the personal effects of ship's personnel);
- Supervising the handling of cargo and the delivery of ship's stores, and
- Ensuring that ship security communication, information, and equipment are readily available.

4.4. Security assessment documentation


Trainees should understand that the Ship Security Assessment shall be documented, reviewed, accepted and retained by the company. Upon completion of the Ship Security Assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

5. Security equipment

5.1. Security equipment and systems

Course participant 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
- Ship security alert system
- Locks
- Lighting
- Night vision binoculars
- 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

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

- Long range acoustic device (LRAD)
- Razor wire
- Electric fencing
- Yacht radar
- Netting
- Slippery foam
- Security glass film
- Water and foam monitors
- Other anti-piracy devices

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 Company Security Officer may well be in a 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 measures 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 attacked by pirates and armed robbers. Even a simple act such as the application of grease on railings can delay boarding. The use of water hoses to deter boarding should also be discussed. Safety precautions related to the use of these devices must be explained to the trainees.


While describing the Ship Security Alert System, the Instructor should emphasize that the Competent Authority receiving the alert, which may include the Company Security Officer, must be in a state of continuous readiness in case emergency calls are received from the SSAS system and inform the administration of the same in a timely fashion.

5.2.Operational limitations of security equipment and system

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 rang, environment 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 insuring the continuing accuracy, efficiency, and operational readiness of selected items of security equipment and associated systems. They 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.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

Trainees should be made cognizant of the risks and benefits inherent in the use of security equipment and systems that may be employed to deter and mitigate attacks by pirates and armed robbers against ships. Particular concern should be paid to the extent to which the use of such equipment may expose seafarers to personal danger, escalate conflict with boarders, or compromise the safety of the ship and/or cargo.

6. Ship security plan

6.1. Purpose of the ship security plan

The Ship Security Plan is defined in the ISPS Code Part A Section 2.1 as a ship-specific plan that will ensure the application of measures on board the ship to provide protection from the risk of a security incident. Therefore it is imperative that all candidates for the Ship Security Officer and Company Security Officer position fully understand the nature of the Ship Security Plan. The Ship Security Officer will need to ensure that such a plan is developed, that it is submitted for approval, and thereafter that it is implemented and maintained. These are considerably different requirements and this course has addressed these differences in both content and time allotted for subject.

6.2. Contents of the ship security plan


The contents of the Ship Security Plan are most clearly established in the ISPS Code Part A. Section 9.4, with additional information provided in section 9 of the Part B of the Code. Trainees should be familiar with the contents of the plan generic fashion thus knowing what to expect as they are assigned to various ships and experience various Ship Security Plans. As future Company Security Officers, trainees in this course should understand the elements of the plan as it relates to specific threats such as explosive devices, piracy, and armed robbery. 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 Company Security Officer.

6.3. Confidentiality issues

Essentially, the Ship 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 and clearly delineate those few circumstances when, and what sections of, the Ship Security Plan may be inspected by Port State Control Officers.

6.4. Development of the ship security plan

The Company Security Officer is responsible to ensure that the Ship Security Plan is prepared and submitted for approval. In this regard, Company Security Officer trainees must understand their additional duties relative to the Ship Security Officer and consequentially the need for a deeper understanding of the Ship Security Plan. Trainees should understand that all security measures in the Ship Security Plan must be in place by the time the initial verification of the plan carried out.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

6.5. Approval of the ship security plan

Ensuring that the Ship Security Plan is ultimately approved is the duty of the Company Security Officer and therefore the Company 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 Ship Security Plan and that it must be accompanied by a completed Ship Security Assessment upon application for approval.

6.6. Implementation of the ship security plan

Ensuring that the Ship Security Plan is ultimately approved is the duty of the Company Security Officer and therefore the Company Security Officer being at the front line in this Endeavour. Details concerning this shared responsibility should be presented in such a way as to not only ensure the understanding of the process but to also leave no doubt as to who is responsible for what. Both Ship Security Officer and Company Security Officer must be clear their roles in the implementation of the plan.

6.7. Maintenance and modification of the ship security plan

The Ship 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 Ship Security Plan is a living document and will require modification over time. Trainees must understand not only the provisions set out by the Ship 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 in place as new policy.

7. Threat identification

7.1. Recognition, on a non-discriminatory basis, of persons posing potential security risk

Instructor should explain suspicious patterns of behavior, while emphasizing the importance of avoiding racial profiling and ethnic stereotyping. Examples of suspicious behaviors include:

- Unknown person 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.
- Unknown persons loitering in the vicinity of ships or port facilities for extended periods of time.
- Unknown person telephoning facilities to ascertain security, personnel, on standard operating 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 aircraft operating in proximity to vessels or facilities.



- Person 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 equipment.
- E-mails attempting to obtain information regarding the facility, personnel, or standard operating procedures.
- Package drop-off/attempted drop-off.
- 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 person aboard refugee craft posing as mariners in distress to attract assistance from other vessels.
- High-speed skiffs approaching the ship on an intercepting course.
- Small craft containing ladders, grappling hooks, and other potential boarding devices.
- The presence of mother ships in the vicinity of one or more small craft.

7.2. Recognition of threats of an impending piracy attack

This section deals with recognition of a piracy attack. The instructor should, using examples, advise general signs to look out for when in piracy prone areas with other craft in the vicinity.

7.3. Recognition and detention of weapons, dangerous substances and devices


The focus of this sessions 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.

7.4. 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 searches should follow and the places on the route where weapons, devices, dangerous substances, etc., might be hidden.

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 card in conducting systematic searches. For example, a check card is a card that can be issued to each searcher specifying the route the route the follow and the areas to be searched. These cards can

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

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 list of 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.
- Searches 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 their context, as a means of disguise, such as in a toolbox in an engine room.

Participants of the course should be acquainted with the fact that there are many places on 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 frame under mattress
- Under a washbasin
- Behind removable medicine chest
- Inside radios, recorders, etc.
- 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
- Hollowed – out melding

COMPANIONWAYS

- Ducts
- Wire harnesses
- Railings
- Fire extinguishers
- Fire hoses and compartments
- Access panels in floors, walls, ceiling
- Behind or inside waters coolers, igloos.

TOILET AND SHOWERS

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

DECK


- Ledges on deck housing, electrical switch rooms, winch control panels
- Lifeboats 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

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

- Bonded store lockers, slop chest, storage rooms

7.5. Methods of physical searches and non-instructive inspections

In this segment of the course, trainees will learn techniques used to conduct physical and non-intrusive searches of persons, personal effects, baggage, cargo, and ships stores. Trainees should be informed that, unless there are clear security grounds 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.

7.6. 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.

The known methods employed by pirates and armed robbers to board ships and undertake attack should be elaborated upon. The Best Management Practices to Deter Piracy off the Coast of Somalia and in the Arabian Sea Area (BMP3) provides a helpful description of typical pirate attacks that may serve as a foundation for this discussion.

7.7. 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. Ship security actions

In general the "Ship Security Actions" section of this course is material that both the Ship Security Officer and the Company Security Officer should be very familiar with. Parts A and B of the ISPS Core are helpful in organizing material to be conveyed in this section of the course. Instructors should indicate that this section of the course is where ideas, plans, and preparation turn into actions and procedures.

8.1. Action required by different security levels, including actions to be taken to prevent piracy and armed robbery

The instructor should explain the different type of security measures that should be considered for ships at sea, including measures to be taken to prevent piracy and armed robbery, and those in port, as they respond to security incidents and the meaning of 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.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

Company Security Officer trainees should thoroughly understand the types of actions required in case of attacks and attempted attacks by pirates and armed robbers. Nothing that procedures will vary depending on the construction of the vessel, the composition of the crew, and the other factors, trainees should understand recommended actions as suggested in the Best Management Practices to Deter Piracy off the Coast of Somalia and in the Arabian Sea Area (BMP3).

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 setting of security levels by the port or by 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 Part B of the ISPS Code, which may be helpful in explaining the nature and use of the declaration of security.

The trainees must also be advised that DoS is not a routine document and therefore no 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 of 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 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 deck areas and areas surrounding the ship, and so forth.



9. Emergency preparedness, drills, and exercises

9.1. Contingency planning

The 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, armed robbery, hijackings, and similar events should be discussed. The trainees are encouraged to review contingency plans to ensure procedures provided for ship staff to handle emergency situations.

9.2. Security drills and exercises


It should be conveyed to course participants that the objective of drills and exercise is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and in the identification of any security-related deficiencies that need to be addressed.

Trainees should learn that the effective implementation of the provisions of the ship security plans requires that drills be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel have been changed, at any one time, with personnel that have not previously participated in any drill on that ship within the last three months, a drills should be conducted within one week of the change. These drills should test individual elements of the plan such as:

- Damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices arson, sabotage of vandalism;
- Hijacking or seizure of the ship or of persons on board;
- Tampering with cargo, essential ship equipment or systems or ships stores;
- Unauthorized access, including presence of stowaways;
- Smuggling weapons or equipment, including weapons of mass destruction;
- Use of the ship to carry persons intending to cause a security incident, or their equipment;
- Use of the ship itself as a weapon or as a means to cause damage or destructions;
- Attacks from seaward while at berth or a anchor, and;
- Attacks while at sea including attacks by pirates and armed robbers.

Various type of exercises that may include participation of Company Security Officers, Port Facility Security Officers, relevant authorities of Contracting Governments, as well as Ship Security Officers, is available, should be carried out a least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, co-ordination, resource availability, and response. These exercises may be:

- Full scale or live;
- Tabletop simulation or seminar; or combined with other exercises held, such as search and rescue or emergency response exercises.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

9.3. Assessment of security drills and exercises

At end of each drills or exercises, the Ship 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 drills to the Ship Security Officer.

10. Security administration

10.1. Documentation and records

Drawing on Chapter XI-1 Regulation 5 and Chapter XI-2 of SOLAS, the instructor will find sufficient references to, and examples of, requirements, as well as requirements for record keeping. The international ship security certificate should be the main emphasis here while the Continuous Synopsis Record warrants coverage as well. Records of activities addressed in the Ship Security Plan must be kept on board for certain time periods that are determined by administrations. Section 10 of the ISPS Code Part A is very useful on the subject of records. The trainees should also be advised that these records, subject to, meeting the requirements in ISPS/A 9.8.1, should be readily available to be shown to Duly Authorized Officers exercising control and compliance (Port State Control).

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 suggest several sample security incidents. Protocols specifically developed for reporting incidents involving piracy and armed robbery against ships should be explained.

10.3. Monitoring and control


Here the focus of monitoring is on the Ship Security Plan itself. Proper administration of the plan indicates that the Master and the Ship Security Officer should review the Ship 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 Ship 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 nonconformities. Both the Ship Security Officer and the Company Security Officer play Key roles in this effort to keep the Ship Security Plan in an option condition.

	SEAFARERS TRAINING CENTER	M-CSO (I)-18
	COMPANY SECURITY OFFICER	REV. 5 -2015

11. Security training

11.1. Training requirements

The training requirements for shipboard personnel are set out under the ISPS Code; Parts A and B of the Code and the standards of Competence expected are specified in the STCW Code. These expectations should be explained briefly to the trainees. Instructors should clarify the requirements for who needs to be trained, what the training consist of, and where the responsibility lies for the training of various persons involved in maritime security.

11.2. Instructional techniques

The Company Security Officer carries the burden of ensuring that all shipboard personnel responsible for the security of the ship are properly trained. The Company Security Officer should have a clear understanding of instructional techniques. This information may be used directly by the company security officer as instructor or may be employed by the Company Security Officer in evaluating instructional programmers being used by, being considered for use by the company.