	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>


## **SEAFARERS TRAINING CENTER INC**



# **SECURITY AWARENESS TRAINING FOR ALL SEAFARERS**

***IMO MODEL 3.27***

***In accordance to International  
Convention on Standards of Training,  
Certification and Watchkeeping for  
Seafarers (STCW), 1978, as amended.***

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

**SCOPE**

This course is intended to provide knowledge required to enable personnel without designated security duties in connection with a Ship Security Plan (SSP) to enhanced ship security in accordance with the requirements of chapter XI-2 of SOLAS 74 as amended, the ISPS Code, and section A-VI/6-1 of the STCW Code.

**OBJECTIVES**

Those who successfully complete this course should achieve the required standard of competence enabling them to contribute to the enhancement of maritime security through heightened awareness and the ability to recognize security.

**ENTRY STANDARD**

It is assumed that those attending this course will be serving seafarers or other shipboard personnel who will not be assigned specific security duties in connection with the Ship Security Plan.

**COURSE CERTIFICATE, DIPLOMA OR DOCUMENT**

A certificate will be issued to those who have successfully completed this course.

**COURSE INTAKE LIMITATION**


The maximum number of trainees will be 25 persons.

**STAFF REQUIEMENTS**

The instructor in charge of the course should have adequate experience in maritime security matters and should have knowledge of the requirements of chapter XL-2 of SOLAS 74 as amended, the ISPS code, and security-related provisions of the STCW Code.

**BIBLIOGRAPHY**


International Convention for the Safety of Life at Sea, 1974 (SOLAS 1974), as amended.  
International Ship and Port Facility Security (ISPS) Code

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

## TIMETABLE


### COURSE OUTLINE

SUBJECT AREA	HOURS
<b>1. INTRODUCTION</b> 1.1. Course overview 1.2. Competences to be achieved 1.3. Current security threats and patterns 1.4. Ship and port operations and conditions	0.75
<b>2. MARITIME SECURITY POLICY</b> 2.1. Awareness of relevant international conventions, codes and recommendations 2.2. Awareness of relevant government legislation and regulations 2.3. Definitions 2.4. Handling sensitive-related information and communications	0.75
<b>3. SECURITY RESPONSIBILITIES</b> 3.1. Contracting governments 3.2. The company 3.3. The ship 3.4. The port facility 3.5. Ship Security Officer 3.6. Company Security Officer 3.7. Port Facility Security Officer 3.8. Seafarers with designated security duties 3.9. Port Facility personnel with designated security duties 3.10. Other personnel	0.5
<b>4. THREAT IDENTIFICATION, RECOGNITION AND RESPONSE</b> 4.1. Recognition and detection of weapons, dangerous substances and devices 4.2. Recognition, on a non-discriminatory basis, of persons posing security risks 4.3. Techniques used to circumvent security measures	1.0
<b>5. SECURITY ACTIONS</b> 5.1. Action requires by different security levels 5.2. Reporting security incidents	0.5
<b>6. EMERGENCY PREPAREDNESS, DRILLS AND EXERCISES</b> 6.1. Awareness of contingency plans 6.2. Security drills and exercises	0.5
<b>7. Theoretical Exam</b>	1.0
<b>TOTAL</b>	<b>5.0</b>

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

### COURSE TIMETABLE

DAY/ PERIOD	1 <sup>st</sup> PERIOD (2.0 HOURS)	2 <sup>nd</sup> PERIOD (2.0 HOURS)
Day 1	<p><b>1. INTRODUCTION</b></p> <p>1.1. Course overview</p> <p>1.2. Competences to be achieved</p> <p>1.3. Current security threats and patterns</p> <p>1.4. Ship and port operations and conditions</p> <p><b>2. MARITIME SECURITY POLICY</b></p> <p>2.1. Awareness of relevant international conventions, codes and recommendations</p> <p>2.2. Awareness of relevant government legislation and regulations</p> <p>2.3. Definitions</p> <p>2.4. Handling sensitive-related information and communications</p> <p><b>3. SECURITY RESPONSIBILITIES</b></p> <p>3.1. Contracting governments</p> <p>3.2. The company</p> <p>3.3. The ship</p> <p>3.4. The port facility</p> <p>3.5. Ship Security Officer</p> <p>3.6. Company Security Officer</p> <p>3.7. Port Facility Security Officer</p> <p>3.8. Seafarers with designated security duties</p> <p>3.9. Port Facility personnel with designated security duties</p> <p>3.10. Other personnel</p>	<p><b>4. THREAT IDENTIFICATION, RECOGNITION AND RESPONSE</b></p> <p>4.1. Recognition and detection of weapons, dangerous substances and devices</p> <p>4.2. Recognition, on a non-discriminatory basis, of persons posing security risks</p> <p>4.3. Techniques used to circumvent security measures</p> <p><b>5. SECURITY ACTIONS</b></p> <p>5.1. Action requires by different security levels</p> <p>5.2. Reporting security incidents</p> <p><b>6. EMERGENCY PREPAREDNESS, DRILLS AND EXERCISES</b></p> <p>6.1. Awareness of contingency plans</p> <p>6.2. Security drills and exercises</p>

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

## MANUAL

### 1. Introduction

#### 1.1. Course overview

In response to ongoing international security threats, the International Maritime Organization (IMO) developed new Maritime Security Regulations that were implemented July 1, 2004. These new security regulations require that each ocean going vessel implement a Ship Security Plan, which outlines the security policies, procedures and practices that must be maintained onboard, while in port or at sea.

All crewmembers play a vital role in the safe and secure implementation of the Ship Security Plan. This Maritime Security Awareness Training will help you understand the security regulations and your security responsibilities and duties.

#### 1.2. Competencies to be achieved


The trained will acquire the following competences:

- Contribute to the enhancement of maritime security through heightened awareness ,
- Recognition of security threats.
- Understanding of the need for and methods of maintaining security awareness and vigilance.

#### 1.3. Current security threats and patterns

Threats to the maritime transport industry include those given below.

- **TERRORISM:** Looking at the past the main danger to merchant ships was due to war between states. However, today's maritime challenges go beyond the narrow conception of defense in a scenario of interstate conflict. They are more diverse, complex, unpredictable, and intertwined. First, since the attacks of 11 September 2001, the threat posed by international terrorism has gained a new dimension. Incidents such as the USS Cole and Limburg attacks have demonstrated that terrorists are interested in and capable of using the maritime domain to achieve their objectives. Preventing terrorists from attacking at or from the sea and from crossing maritime borders has thus become a major preoccupation for European and North American governments. Particular attention has been given to addressing the vulnerability to terrorist attacks of sea-based critical energy infrastructure and of maritime flows of energy resources. One should also mention the threat that "terror mining" in large harbors such as Rotterdam, Antwerp or New York, could pose to maritime trade. A second and related threat is the use of maritime routes by terrorists or state actors for the proliferation of weapons of mass destruction material and technology. Third, the increase in the illegal movement of drugs, human beings and arms as well as the growing flow of illegal immigrants, particularly from Africa to Europe, has raised the problem of effective maritime governance and border control, in particular on the porous maritime borders.
- **PIRACY AND ARMED ROBBERY.**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Historically the sea has been the hunting ground for armed robbers or pirates as they came to be called for as long as merchant ships have been sailing in them. After the second half of the last century the world saw modern day pirates using powered craft and automatic weapons hijacking and robbing ships. The Far Eastern waters like Malacca and China Sea were very much in the news for a considerable period of time. Incidents also took place in other areas worldwide. The dramatic upsurge in incidents of piracy and armed robbery off the coast of Somalia and the Arabian Sea in recent years have shown that this “old” threat is far from extinct. Especially where one finds extreme state weakness and attacks take place along vital maritime trade routes, piracy can pose a threat not only in terms of local or regional security, but also international security. The situation in Somalia has also raised the specter of a possible collusion of interests between terrorists and pirates. Other unstable regions, such as the Niger Delta, also continue to face significant piracy problems.

➤ **COLLATERAL DAMAGE.**


Collateral damage is damage to things that are incidental to the intended target. It is frequently used as a military term where it can refer to the incidental destruction of civilian property and non-combatant casualties. The use of military means to free hijacked ships in the Gulf of Aden off the Somalia coast, though successful, has resulted in “retaliative” action. According to one expert a comprehensive approach is required to deal with the piracy problem. Military action has been lauded by the media, but there has been collateral damage. For instance, the master of “MV Samho Jewelry” was shot in the process of rescue and the deaths of the American civilians onboard the yacht “Quest” was also caught up in a military response.

➤ **CONTRABAND SMUGGLING.**

In the past the ships were usually carrying narcotics as part of the criminal activities of organized crime. Now also these drugs are carried by maritime transport units but with increased sophisticated methods, except that now weapons and explosives can also be included. The financial gains can be astronomical and so there is now an increase of organized crime gangs linked with terrorists, who use these finances. The links between pirates and terrorists/organized crime gangs is also suspected.

➤ **CARGO THEFT.**

This has been a problem for the maritime industry since the ships evolved. It can be small scale pilferage to stealing the whole cargo. Even though containerization has reduced the quantity yet it occurs in all segments of the marine cargo carriage trade. Thieves can range from the corporate type using modern day information technology to the poorly clad fisherman turned robber climbing up from the anchor cable in some third world port.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

➤ STOWAWAYS AND REFUGEES.

Extreme economic disparity between the rich and poor states and the hope of a better life force the people to migrate and many will resort to illegal ways like stowing away on board a ship. The others are who fear for their life due to conflict or persecution and want to get away from their country. This is a worldwide phenomenon and no particular region can be singled out.

**1.4. Ship and port operations and conditions**


When we talk about the carriage of goods by ships sailing on the world's waterways then we must be aware that like other forms of transport vehicles using land or air there are at present direct links between these different modes. A cargo package during its journey from the shipper to consignee can use all modes of transport. Ships will interface with the sea/river port and usually the land transport truck or rail will also interface with them, as well as with the airport. Sometime you will also have an intervening Dry Port. Therefore, this inter-modal nature of transportation makes the security solution much more complex, due to the many more vulnerable entry points.

**2. Maritime Security Policy**

**2.1. Awareness of relevant international conventions, codes, and recommendations**

The mariner must be aware that IMO has making efforts towards maritime security through relevant international conventions, codes and recommendations. It will worth mentioning here that previous efforts towards maritime security were by promulgation of such documents as the MSC/Circ.443, SUA Act, etc. In November 2001 (After the 9/11 USA incident), the IMO Assembly adopted Resolution A.924(22), on the review of measures and procedures to prevent acts of terrorism, which threaten the security of passengers and crew and the safety of ships.

Then IMO's Maritime Safety Committee (MSC) and its Maritime Security Working Group did intensive work for ONE YEAR and came out with the ISPS CODE. The International Maritime Organization's (IMO) Diplomatic Conference of December 2002 adopted new Regulations to enhance maritime security through amendments to SOLAS Chapters V and XI. Chapter XI, previously covering ship safety has been split into two new chapters, XI-1 and XI-2. Chapter XI-1, Special Measures to Enhance Maritime Safety, has been enhanced to include additional requirements covering ship identification numbers and carriage of a Continuous Synopsis Record. Chapter XI-2, Special Measures to Enhance Maritime Security, has been created and includes a requirement for ships and companies to comply with the International Ship and Port Facility Security (ISPS) Code. The ISPS Code contains two parts. Part A is mandatory, while Part B is recommendatory and contains guidance for implementation of the Code.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

The USCG has decreed that sections of Part B of the Code will also be taken into consideration. Chapter XI-2 also sets out requirements for ship security alert systems and control and compliance measures for port states and contracting governments. As well as the new Regulations in SOLAS Chapter XI-2, the Diplomatic Conference has adopted amendments to extant SOLAS Regulations accelerating the implementation of the requirement to fit automatic identification systems (AIS) (Chapter V). The Diplomatic Conference has also adopted a number of Conference Resolutions including technical co-operation, and the co-operative work with the International Labor Organization and World Customs Organization. Review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these two organizations. These requirements form a framework through which ships and port facilities can co-operate to detect and deter acts which pose a threat to maritime security. The regulatory provisions do not extend to the actual response to security incidents or to any necessary clear-up activities after such an incident.

In summary the ISPS Code:

- Enables the detection and deterrence of security threats within an international Framework
- Establishes roles and responsibilities
- Enables collection and exchange of security information
- Provides a methodology for assessing security
- Ensures that adequate security measures are in place.

It requires ship and port facility staff to:

- Gather and assess information
- Maintain communication protocols
- Restrict access; prevent the introduction of unauthorized weapons, etc.
- Provide the means to raise alarms

Put in place vessel and port security plans; and ensure training and drills are conducted. The STCW Code has also added security related provisions wherein all persons employed on ships as well as persons on ship having designated security duties are to undergo training and attain competencies as per regulation VI/6 and section A-VI/6.

IMO has issued from time to time Guidance to Ship-owners, Companies, Ship Operators, Shipmasters and Crews on Preventing and Suppressing Acts of Piracy and Armed Robbery against Ships.


## **2.2. Awareness of relevant government legislation and regulations**

Similarly, National Administrations make laws and issue regulation in this matter which is binding on their flag vessels as well as vessels when in their areas of control.

## **2.3. Definitions**

- **Ship Security Plan**



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

➤ **Company Security Officer**

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

➤ **Ship Security Officer**

Means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers.

➤ **Port Facility**

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

➤ **Ship/Port Interface**

➤ Means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship

➤ **Ship-To-Ship Activity**

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

➤ **Port Facility Security Officer**

Means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

➤ **Designated Authority**

Means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.

➤ **Recognized security organization**

Means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by this chapter or by part A of the ISPS Code.


➤ **Declaration of Security**

Means an agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement.

➤ **Security incident**

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

➤ **Security level**


	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Means the qualification of the degree of risk that a security incident will be attempted or will occur.

- **Security level 1**  
Means the level for which minimum appropriate protective security measures shall be maintained at all times.
- **Security level 2**  
Means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- **Security level 3**  
Means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.
- **Terms relating to Piracy and Armed robbery.**  
This consists of any of the following acts:
  - (a) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
    - (i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
    - (ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
  - (b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
  - (c) Any act inciting or of intentionally facilitating an act described in subparagraph (a) or (b)."
- **Port Facility Security Plan**  
Means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.
- **International Ship and Port Facility Security (ISPS) Code**  
Means the International Code for the Security of Ships and of Port Facilities consisting of part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization.

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

Types of Sensitive Information Given the number of potential threats to information security, it follows that there must be something of interest in the information held onboard your ship. Imagine that a terrorist group is looking for a means to transport weapons from one country to another and is considering hijacking your ship. What types of information do you think might be of interest to them? Information about your ship's timings, locations, routes, design and procedures are all of interest to terrorists and other groups planning illegal activities. This information is described as sensitive

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

information and must be protected to prevent unauthorized people and groups from accessing it. Hence the importance of keeping it confidential. Threats to Information Security Before you can maintain the security of the Information on board your ship, you need to be aware of the numerous threats to information security! These threats come under four main categories subversion, espionage, sabotage and terrorism.

**Subversion:** -The threat of subversion can come from hostile intelligence services or extremist groups. These groups will often try to persuade you to help them in their cause and divulge classified information. They may also try to exploit your weaknesses and change your beliefs so that you become sympathetic to their cause.

**Espionage:** -Attempts by groups to acquire information covertly or illegally in order to assist foreign power or a political or commercial competitor are forms of espionage. Information is considered compromised if any or all of it gets into the hands of someone not authorized to have it. Communication systems are particularly vulnerable to espionage from eavesdropping or phone taps. Some intelligence agencies also recruit individuals to obtain information for them through spying or undercover surveillance.

**Sabotage:** -An act or a failure to act that has the intent to cause physical damage with the goal of assisting a foreign power, furthering a subversive aim, or reducing or destroying a commercial operation is characterized as sabotage. Communication systems are always at high risk when sabotage is used to further a political cause. Green Peace attacks on whaling vessels are a good example.

**Terrorism:** -Bombings and hostage takings by groups like Al Qaeda are acts of terrorism. They are unlawful uses of force against individuals or property to achieve political, religious or ideological goals. Unlawful threats of force are also considered acts of terrorism.


There are many other threats to information security, such as the ones listed below!

- Investigative journalists from tabloids or newspapers.
- Criminals such as drug cartels.
- Disaffected or dishonest staff.
- Computer hackers that obtain or manipulate information stored in computers.
- Computer viruses that damage computer systems and information. The most common ways in which information security is unintentionally revealed are:
- Incorrect document handling such as leaving documents unattended in inappropriate places.
- Insufficient document control or security.
- Discussions of information in public places such as pubs and restaurants.
- Insufficient control over document access.

#### Safeguarding Your Ship's Sensitive Information

There are three aspects to information security - personnel security, physical security, and cryptographic and computer security - and each one has methods for protecting your ship's sensitive information.

#### Personnel Security.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Your ship's personnel include the crew, officers, subcontractors, shore personnel, suppliers, inspectors and others working or visiting your ship at any given time.

Personnel security aims to ensure that only those, whose reliability, trustworthiness and circumstances that are not in doubt have access to sensitive material. And, that the necessary permission or clearance needed to access information is limited to those who require it to do their jobs. This need to know approach makes it harder for subversive individuals to obtain information about your ship's operations. There are many methods of personnel security. There are different levels of security checks from basic checks to counter terrorist checks.

The level of security check required depends on the individual's responsibilities and the extent to which he or she has access to sensitive information-individuals in a higher position of trust should be checked to a higher standard. Individuals' circumstances can change - they may get into debt, befriend criminals or move to a high-risk area - and this may make them more susceptible to criminal activities. It's a good idea to maintain close and continuous supervision and to conduct periodic reassessments of security clearances.

#### Physical Security.

The physical measures that need to be in place to protect your ship's information will vary according to the threat, the value of the information to be protected and the sensitivity or value of the information to terrorist, subversive, or criminal groups. The measures may also vary according to your ship's location and the level of detail and strategic importance of the information. Cryptographic and Computer Security Employing methods to safeguard the electronic storage and communication of your ship's sensitive information helps to prevent hacking, the interception of information and the exposure and analysis of information useful to terrorists. There are various methods of cryptographic and computer security.

To obtain the information needed to determine an individual's potential security threat, profilers need to:

- Check documentation;
- Pose questions in a discreet manner; and
- Observe body language and behavior.

#### Checking Documentation

Checking documentation may seem obvious, but it is important. All documents related to the purpose of a shipboard visit should be examined and the ID of all visitors and crew verified.

#### Tips on Questioning.

Use a combination of open-ended and closed-ended questions.

#### Open questions

Are usually preceded with "what, when, who, where, how and why" and that require a person to give more than a "yes" or "no" answer. Examples include:

- Where have you travelled from?



- When did you leave your last stop?
- Who packed your bag?
- Why are you carrying this?
- How did you obtain this?
- What is the nature of your journey?

#### Closed questions

Can only be answered with a "yes" or "no". They can be used to establish facts or obtain statements that may be used in evidence later. Some examples are:

- Is this your bag?
- Is this your passport?
- Are you the person named in this document?
- Did you apply for this visa in person?
- Has anyone asked you to carry any thing for \_him or her?
- Is this the item you were asked to carry? Check to see that the answers to your questions match up with what you already know about a crewmember or the purpose of a shipboard visit. And, ensure that the answers tie in with any items being carried or transported.

#### Asking Good Questions

Questioning is an important part of profiling. Questions draw out important information and should be asked in such a manner as to not arouse the suspicion of the person selected. There are many questions you could ask! Remember, your goal is to ask questions and get answers that will help you determine whether an individual poses a potential risk to your ship's security.


#### Examples of questions to crew

- Are you coming directly from another ship or were you on \_leave?
  - Where did you travel to while on leave?
  - Did you bring any mementos from your travels?
  - Examples of questions to visitors
  - What is the purpose of your visit?
  - Are you bringing onboard any tools or equipment?
  - Were you on another service call before joining us today?
- #### Recognizing Suspicious Behavior

When asking questions, paying attention to the body language and behavior of individuals being questioned is just as important as listening to their answers. Are they nervous? Do they react when you go near their equipment or baggage? Are they sweating or restless? Are they becoming aggressive? Are they overly happy or trying to be overly friendly? Are they trying to avoid eye contact? If you are suspicious of a person's behavior, stay calm and inform someone else of your suspicions. Do some additional checks or perform a search of the individual's belongings or equipment. Allow them onboard only after you are satisfied they do not pose a security risk.

#### Dealing with Suspicious Items

If during profiling, you suspect that an individual is carrying a suspicious object or package - such as drugs or an explosive device - be careful that you don't let the person know that you suspect something. You never know how he or she will react! Never touch or pick anything up. If a suspicious object is an explosive it may be fitted with an

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

anti-handling device. Inform someone of your suspicions, discreetly, so that they can summon assistance. Never use a radio within 25 meters of a suspicious object. If it is an explosive with a radio-controlled device, a transmission by your radio may activate it. If you suspect that the package is a bomb, take these additional steps: Confirm that a device actually exists; Clear the immediate area; Cordon off the area around the suspicious object and Control the area so that only authorized persons have access.

### **3. Security Responsibilities**

As per the requirements of SOLAS, the ISPS code and STCW code (ships personnel training) there are defined requirements for compliance by ships and the ports that service them. Below we give them as set out in the above mentioned documents

#### **3.1. Contracting governments**

Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag. When changes in security level occur, security-level information shall be updated as the circumstance dictates.

Contracting Governments shall set security levels and ensure the provision of security-level information to port facilities within their territory, and to ships prior to entering a port or whilst in a port within their territory.


When changes in security level occur, security-level information shall be updated as the circumstance dictates. With regards to STCW Code the States must ensure that compliance with the new requirements of Security Familiarization training for persons working on ships as well as Security Awareness Training for All Seafarers and Security Training for Seafarers with Designated Security Duties plus the upgrading of Ship Security Officer training are implemented as per the IMO agreements

#### **3.2. The company**

Companies shall comply with the relevant requirements of SOLAS chapter XI and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code. The Company shall ensure that the Master has available on board, at all times, information through which officers duly authorized by a Contracting Government can establish:

- Who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship?
- Who is responsible for deciding the employment of the ship; and
- In cases where the ship is employed under the terms of charter party, who are the parties touch charter party.

#### **3.3. The ship**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Ships shall comply with the relevant requirements of SOLAS chapter XI-2 and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code, and such compliance shall be verified and certified as provided for in part A of the ISPS Code.

- Prior to entering a port or whilst in a port within the territory of a Contracting Government, a ship shall comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship.
- Ships shall respond without undue delay to any change to a higher security level.
- Where a ship is not in compliance with the requirements of this chapter or of part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

#### **3.4. The port facility Port**


Facilities will comply with the relevant requirements of SOLAS chapter XI-2 and the ISPS Code.

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

#### **3.5. Ship security officer**

A ship security officer shall be designated on each ship. The duties and responsibilities of the ship security officer shall include, but are not limited to:

- Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- Maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
- Coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
- Proposing modifications to the ship security plan;
- Reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
- Enhancing security awareness and vigilance on board;
- Ensuring that adequate training has been provided to shipboard personnel, as appropriate;
- Reporting all security incidents;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

### **3.6. Company Security Officer**

The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates, provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate, designate several persons as company security officers provided it is clearly identified for which ships each person is responsible. In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the company security officer shall include, but are not limited to:


- Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- Ensuring that ship security assessments are carried out;
- Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- Ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- Arranging for internal audits and reviews of security activities;
- Arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;
- Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
- Enhancing security awareness and vigilance;
- Ensuring adequate training for personnel responsible for the security of the ship;
- Ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;
- Ensuring consistency between security requirements and safety requirements;
- Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

### **3.7. Port facility security officer**

A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities. The duties and responsibilities of the port facility security officer shall include, but are not limited to:

- Conducting an initial comprehensive security survey of the port facility, taking into account the relevant port facility security assessment;
- Ensuring the development and maintenance of the port facility security plan;
- Implementing and exercising the port facility security plan;
- Undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

- Recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;

Enhancing security awareness and vigilance of the port facility Personnel

- Ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- Coordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- Coordinating with security services as appropriate;
- Ensuring that standards for personnel responsible for security of the port facility are met;
- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
- Assisting ship security officers in confirming the identify of those seeking to board the ship when requested.

### **3.8. Seafarers with Designated Security Duties.**

In addition to the Ship Security Officer other members of the crew on a ship may have Designated Security Duties in support of the Ship Security Plan. These security duties include anti-piracy and anti-armed-robbery activities. These seafarers will have received training as per regulation VI/6 -4 and to attain competency to the level as given in section A-VI/6 para 6-8 of STCW Convention 78', as amended.

### **3.9. Port Facility Personnel with designated security duties.**

In addition to the Port facility security officer other personnel at the port facility may be having designated security duties in support of the Port facility security plan.


### **3.10. Other Personnel.**

Maritime security can be enhanced further by allowing flexibility according to circumstances, of using other personnel who may be or may not be from the ships or ports industry. Similarly for prevention, suppression and reporting of piracy and armed robbery against ships the military, industry and other government entities can have a role

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

### **4.1. Recognition and detection of weapons, dangerous substances and devices**

Types of weapons used are ranging from knives, machetes, spears etc. to firearms of many kinds like pistols, guns, machine guns, grenades etc. Some images of which are shown during the lectures. Look at the pictures and recognize them. The use of these can cause injuries of varying degrees as well as death. They can also cause damage to assets either directly or indirectly like causing an explosion or a fire. Explosives are also

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

used and basically it is a very fast chemical reaction of substances producing gas at high temperature and pressure with such velocity to cause damage. They kill by pressure blast, high temperature and shrapnel used to fill the device in which it is used. Some explosives examples are black powder, nitro glycerin, ammonium nitrate, C4, etc.

The device is consisting of the explosive, the detonator and the triggering mechanism. Some of the very common devices are improvised from ordinary everyday use things and are called I.E.D (improvised explosive device). These will always be in disguise. Few other criminal acts raise as much fear and concern as bombings, so it's no coincidence that crime and terrorist groups routinely use them as a means to achieve their goals whether they are loss of life, intimidation, extortion or government or commercial disruption. Most terrorist and crime groups use Improvised Explosive Devices or IED's. Detonated onboard a ship, an IED can create a serious hull break or start a dangerous fire, both of which can lead to injury and loss of life. So what does an IED look like? During the lecture have a look at some images shown to you. Let's see if you can recognize one! Pictured on the screen are various images.

All of these images are clever disguises of IED's! IED's are homemade weapons that are easily manufactured and limited in their form only by the imagination of their creator! Because they often take the shape of everyday items, it's critical to always be on the look-out for objects that seem out of place or out of context and to be able to recognize the components of an IED.

### **Common Components**


Despite their differences in appearance, all IED's have four components in common - a timer, a power source, a detonator and an explosive. Sometimes a timer power unit (TPU) is used and consists of a homemade unit that contains the timer and a power source and is connected to a detonator and an explosive. Power sources are usually batteries. Detonators are usually commercially available electric or blasting cap detonators that contain very small quantities of a very sensitive explosive. Industrial explosives may be commercial or military grade. Commercial explosives are readily available to license holders and are commonly used in the quarrying and construction industries. High power military explosives are available from eastern bloc countries and states supporting terrorism. Liquid explosives are available, but difficult to find. Terrorist and criminal groups have devised ways to make homemade explosives because other types of explosives are not always readily available. These explosives are usually derived from chemicals found in fertilizer or other industrial products.

### **Incendiary Devices**

Incendiary Devices are a commonly used type of IED. They consist of a small amount of explosive supplemented by a flammable liquid. These small, but effective devices use the destructive power of fire to cause massive damage.

### **Vehicle Borne Devices**

Car bombs are another common type of IED. They are designed to carry large quantities of explosives and use vehicles as weapons. Under car booby traps are another common IED designed to kill or maim the occupants of a vehicle. Used as assassination weapons,

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

they usually contain small amounts of a high grade explosive and may be triggered by a timer, a remote control device or a mercury tilt switch.

#### **Letter and Parcel Bombs**

Terrorists sometimes use letter and parcel bombs as methods of intimidation or assassination. There are many indications that a letter or a parcel is suspicious, some of which can be recognized! Listed are all of the indications to watch-out for. It may not be obvious at first glance that a letter or package is suspicious, so it's always a good idea for crew to wear protective clothing and rubber gloves when handling mail and to use a letter opener to open envelopes. Whenever possible have all parcels x-rayed or scanned before opening them. If there are signs that a package or parcel is suspicious, crew should take these immediate actions: Make no attempt to open the envelope or package Place it in plain view on a flat surface or move it to an open space on the ship's deck. If it is left in a confined space ensure all doors and windows are left open. Clear the area. Cordon off the area and, if possible, allow nobody to within 50m or 2 bulkheads of the line of sight of the package. Notify the Duty Watch Officer. Other dangerous substances can be gases of explosive /flammable or toxic nature which can be in liquefied form or compressed. Some flammable gases are natural gas (methane/ethane), LPG (propane /butane), hydrogen and acetylene. Toxic gases are Ammonia, H<sub>2</sub>S, SO<sub>2</sub>, Cyanide, Phosgene etc.

Dangerous liquids, solids, can be so due to being flammable, toxic or having properties to cause damage to human body like corrosion burns or cancer/mutation of cells. Substances having radioactive properties are an example. Also we have seen that some powders used by terrorists caused anthrax or lung problems to people.


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

##### **Profiling.**

Profiling helps us get beneath the outer shell of an individual to obtain a more complete picture. It has many applications. In the context of ship security, profiling will help you identify whether and to what extent the crew and visitors to your ship pose a security risk. Profiling techniques like document checks, questioning and observation ensure that judgments are based on more than just appearances. Random selection of individuals for profiling ensures that patterns are not established. It also prevents allegations that individuals are being picked on? Whenever behaviors or items arouse suspicion, action should always be taken to respond to the perceived threat whether that means additional checks, searches or the cordoning off and containing of an explosive device. Averting a security incident is worth the extra time and effort!

##### **The Many Uses of Profiling.**

It's easy to see how appearances can be deceiving. And yet, we commonly make judgments about people based on how they look. Profiling is a method used to get beneath the outer shell of an individual to obtain a more complete picture. It has many applications.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

### **Criminal**

Criminal profiling is used to obtain information about an individual or an offender. Matching DNA samples and reviewing past offenders' files to establish trends and patterns during investigations are two common profiling techniques.

### **Industrial**

Industrial profiling is used to obtain information about rival companies and their employees. It might include examining internet sites or employing specially trained personnel to build up the profiles.

### **Commercial**

Commercial profiling is used to obtain information about customers or employees. Many organizations use focus groups, surveys and purchase information to track and target the needs and preferences of their customers.

### **General**

Profiling information is widely available. You can obtain a multitude of information on the internet including the profile of a potential vacation destination, a residential area, or even a Doctor that you may be thinking of using!

### **Using Profiling Onboard Your Ship**

Onboard your ship, you can profile both crew and visitors at all access points to identify their level of security risk and what, if any, additional checks or measures need to be implemented before they are allowed to board. Detection equipment can also be used, but only in tandem with profiling. It cannot select for itself and only works on facts. You may spot things that the equipment won't and it's important to not ignore these gut feelings or hunches. They're an essential part of profiling! When establishing your ship's profiling program, it's vital that you maintain a random selection process. This ensures that a pattern is not established and prevents allegations that individuals are being picked on. This is especially important when checking or searching crew. One approach you can use with crew is to take a number at random between 5 and 9, say for this example 8, and search every 8th crewmember coming onboard.

### **Tasks of the Profiler**

Profilers need to gather the maximum amount of information in a limited period of time. According to Rafael, the former chief in charge of security at the German Airport Authority, a profiling interview can take as little as 90 seconds or as long as 20 minutes. It ends when the profiler is satisfied that all of the relevant areas have been addressed.

To obtain the information needed to determine an individual's potential security threat, profilers need to:

- Check documentation;
- Pose questions in a discreet manner; and
- Observe body language and behavior.

### **Checking Documentation**

Checking documentation may seem obvious, but it is important. All documents related to the purpose of a shipboard visit should be examined and the ID of all visitors and crew verified.

### **Tips on Questioning.**



Use a combination of open-ended and closed-ended questions.

#### Open questions

Are usually preceded with "what, when, who, where, how and why" and that require a person to give more than a "yes" or "no" answer. Examples include:

- Where have you travelled from?
- When did you leave your last stop?
- Who packed your bag?
- Why are you carrying this?
- How did you obtain this?
- What is the nature of your journey?

#### Closed questions

Can only be answered with a "yes" or "no". They can be used to establish facts or obtain statements that may be used in evidence later. Some examples are:

- Is this your bag?
- Is this your passport?
- Are you the person named in this document?
- Did you apply for this visa in person?
- Has anyone asked you to carry any thing for \_him or her?
- Is this the item you were asked to carry? Check to see that the answers to your questions match up with what you already know about a crewmember or the purpose of a shipboard visit. And, ensure that the answers tie in with any items being carried or transported.

#### Asking Good Questions

Questioning is an important part of profiling. Questions draw out important information and should be asked in such a manner as to not arouse the suspicion of the person selected. There are many questions you could ask! Remember, your goal is to ask questions and get answers that will help you determine whether an individual poses a potential risk to your ship's security.


#### Examples of questions to crew

- Are you coming directly from another ship or were you on \_leave?
- Where did you travel to while on leave?
- Did you bring any mementos from your travels?

#### Examples of questions to visitors

- What is the purpose of your visit?
- Are you bringing onboard any tools or equipment?
- Were you on another service call before joining us today? Recognizing Suspicious Behavior

When asking questions, paying attention to the body language and behavior of individuals being questioned is just as important as listening to their answers. Are they nervous? Do they react when you go near their equipment or baggage? Are they sweating or restless? Are they becoming aggressive? Are they overly happy or trying to

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

be overly friendly? Are they trying to avoid eye contact? If you are suspicious of a person's behavior, stay calm and inform someone else of your suspicions. Do some additional checks or perform a search of the individual's belongings or equipment. Allow them onboard only after you are satisfied they do not pose a security risk.

#### Dealing with Suspicious Items

If during profiling, you suspect that an individual is carrying a suspicious object or package - such as drugs or an explosive device - be careful that you don't let the person know that you suspect something. You never know how he or she will react! Never touch or pick anything up. If a suspicious object is an explosive it may be fitted with an anti-handling device. Inform someone of your suspicions, discreetly, so that they can summon assistance. Never use a radio within 25 meters of a suspicious object. If it is an explosive with a radio-controlled device, a transmission by your radio may activate it. If you suspect that the package is a bomb, take these additional steps: Confirm that a device actually exists; Clear the immediate area; Cordon off the area around the suspicious object and Control the area so that only authorized persons have access

#### **4.3. Techniques used to circumvent security measures**

4.3.1. Having a good plan is essential to your ship's security, but a plan alone is not enough! Diligence on the part of crew in implementing the plan is just as important. Terrorists and criminals will constantly search for ways to circumvent your security measures, procedures and equipment. They will often be extremely clever and may take many months to observe you and research your equipment in order to find a way to successfully attack you. The best defense is good security awareness and observation on the part of all crew and passengers. If you get the sense that something is not right? Then it probably isn't!

Investigate until you are satisfied that all is well! Some other indicators to watch out for are:

1. Interference or jamming and monitoring of your ship's communications system. Efforts made to broadcast over the system, damage your radio transmitter or antenna, or cut telephone lines are often the first indication that an attack is imminent.
2. Damage to locks and doors such as scratches around the locks.
3. Lost or stolen keys.
4. Normally locked doors being found open for no reason.
5. Dirty finger marks on clean doors or windows, or clean marks on dirty doors.
6. False alarms on security systems. The criminal or terrorist may be testing your response time and reaction procedures, or trying to incapacitate your alarm system.
7. Apparently wanton, or accidental damage to essential equipment. This may be an indicator that an attempt is about to be made to attack you. Never rule out the possibility of collusion between the terrorists and members of the crew!

4.3.2. Methods used by pirates and armed robbers to undertake attacks against ships



.1 Commonly, two small high speed (up to 25 knots) open boats or „skiffs“ are used in attacks, often approaching from either quarter or the stern. Skiffs are frequently fitted with 2 outboard engines or a larger single 60hp engine.

.2 Pirate Action Groups operate in a number of different boat configurations. To date whatever the configuration the attack phase is carried out by skiffs. Pirate Action Group boat configurations include:

- Skiffs only – usually two.
- Open whalers carrying significant quantities of fuel often towing 2 or more attack skiffs.

- Mother ships which have included the very largest of merchant ships, fishing vessels and dhows. These Mother ships have been taken by the pirates and usually have their own crew onboard as hostages. Mother ships are used to carry pirates, stores, fuel and attack skiffs to enable pirates to operate over a much larger area and are significantly less affected by the weather. Attack skiffs are often towed behind the Mother ships. Where the size of the Mother ship allows it, skiffs are increasingly being carried onboard and camouflaged to reduce chances of interdiction by Naval/ Military forces.

.3 Increasingly, pirates use small arms fire and Rocket Propelled Grenades (RPGs) in an effort to intimidate Masters of ships to reduce speed and stop to allow the pirates to board. The use of these weapons is generally focused on the bridge and accommodation area. In what are difficult circumstances, it is very important to maintain Full Sea Speed, increasing speed where possible, and using careful maneuvering to resist the attack.

.4 Pirates seek to place their skiffs alongside the ship being attacked to enable one or more armed pirates to climb onboard. Pirates frequently use long lightweight ladders and ropes, or a long hooked pole with a knotted climbing rope to climb up the side of the vessel being attacked. Once onboard the pirate (or pirates) will generally make their way to the bridge to try to take control of the vessel. Once on the bridge the pirate/pirates will demand that the ship slows/stops to enable further pirates to board.

.5 Attacks have taken place at most times of the day. However, many pirate attacks have taken place early in the morning, at first light. Attacks have occurred at night, particularly moonlit nights, but night time attacks are less common.


.6 The majority of piracy attacks have been repelled by ship’s crew who have planned and trained in advance of the passage and applied the Best Management Practices contained within the various guidance books published by various concerned sources

## **5. Ship Security Actions**

5.1.1. The 3 security levels are LEVELS 1,2 & 3. These are described in chapter 2 of this handout in para. 2.3 in sub heading of Definitions. The actions that have to be taken in case of application of each level are given here.

### **Security level 1**

At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>


- checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc.;
- in liaison with the port facility, the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry-on items), personal effects, vehicles and their contents can take place;
- in liaison with the port Facility, the ship should ensure that vehicles destined to be loaded onboard car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP.
- segregating checked persons and their personal effects from unchecked persons and their personal effects;
- segregating embarking from disembarking passengers;
- identifying access points that should be secured or attended to prevent unauthorized access;
- securing, by locking or other means, access to unattended spaces adjoining areas to which passenger and visitors have access and
- providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance. At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches including random searches should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close cooperation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

### **Security level 2**

At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

- assigning additional personnel to patrol deck areas during silent
- limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;
- deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;
- establishing a restricted area on the shore side of the ship, in close co-operation with the port facility;
- increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;
- escorting visitors on the ship;
- providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance; and



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

- carrying out a full or partial search of the ship

### **Security level 3.**

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

- limiting access to a single, controlled, access point;
- granting access only to those responding to the security incident or threat thereof;
- directing persons on board;
- suspension of embarkation or disembarkation;
- suspension of cargo handling operations, deliveries, etc.;
- evacuation of the ship;
- movement of the ship; and
- preparing for a full or partial search of the ship

5.1.2. Recommended actions in response to attacks and attempted attacks by pirates and armed robbers. If the crew of a vessel suspects that it is coming under a pirate attack there are specific actions that are recommended to be taken during the approach stage and the attack stage. It should be noted that the pirates generally do not use weapons until they are within two cables of a vessel, therefore any period

up until this stage can be considered as “approach”, and


gives a vessel valuable time in which to activate her defenses and make it clear to pirates that they have been seen and the vessel is prepared and will resist.

#### **Approach Stage**

If not already at full speed, increase to maximum to open the CPA. Try to steer a straight course to maintain a maximum speed.

Initiate the ship’s pre-prepared emergency procedures. Activate the Emergency Communication Plan

- Sound the emergency alarm and make a „Pirate Attack“ announcement in accordance with the Ship’s Emergency Plan.
- Report the attack immediately to UKMTO (+971 505 523 215). UKMTO is the primary point of contact during an attack but MSCHOA acts as a back-up contact point. Once established, maintain communication with UKMTO. Please report attack to UKMTO even if part of a national convoy so other merchant ships can be warned.
- Activate the Ship Security Alert System (SSAS), which will alert your Company Security Officer and Flag State. Make a „Mayday“ call on VHF Ch. 16 (and backup Ch. 08, which is monitored by naval units).
- Send a distress message via the Digital Selective Calling system (DSC) and Inmarsat-C, as applicable.
- Ensure that the Automatic Identification System (AIS) is switched ON. All crew, except those required on the bridge or in the engine room, should muster at the Safe Muster Point or Citadel if constructed; so that the crews are given as much ballistic protection as

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

possible should the pirates get close enough to use weapons. Where possible, alter course away from the approaching skiffs, and/or Mother ships. When sea conditions allow, consider altering course to increase an approaching skiffs exposure to Wind/waves. Activate water spray and other appropriate self-defensive measures. Ensure that all external doors and, where possible, internal public rooms and cabins, are fully secured. In addition to the emergency alarms and announcements for the benefit of the vessel's crew sound the ship's whistle /foghorn continuously to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.

Attack stage.

Reconfirm that all ship's personnel are in a position of safety.

As the pirates close in on the vessel, Masters should commence small alterations of helm whilst maintaining speed to deter skiffs from lying alongside the vessel in preparation for a boarding attempt. These maneuvers will create additional wash to impede the operation of the skiffs. Substantial amounts of helm are not recommended, as these are likely to significantly reduce a vessel's speed.

If The Pirates Take Control.


- Try to remain calm.
- Before the pirates gain access to the bridge, inform UKMTO. Ensure that the SSAS has been activated, and ensure that the AIS is switched on.
- Offer no resistance to the pirates once they reach the bridge. Once on the bridge the pirates are likely to be aggressive, highly agitated, and possibly under the influence of drugs, (including khat, an amphetamine like stimulant), so remaining calm and cooperating fully will greatly reduce the risk of harm.
- If the bridge/engine room is to be evacuated the main engine should be stopped and all way taken off the vessel if possible, (and if navigationally safe to do so). All remaining crewmembers should proceed to the designated Safe Muster Point with their hands visible.
- Leave any CCTV running.

5.2 Reporting security incidents.

5.2.1. The duty of the Ship Security Officer as given in the ISPS Code Part A para.12.2.8 requires the reporting of all security incidents. The ship security plan will have the procedures for reporting of security incidents. In the case of piracy and armed attack there are now very well defined procedures issued by IMO circulars in cooperation with the organizations handling the incidents occurring in various parts of the globe. An example is this

UKMTO– (UK) Maritime Trade Operations.

The UK Maritime Trade Operations (UKMTO) office in Dubai acts as a point of contact for industry liaison with the Combined Military Forces (CMF). UKMTO Dubai also administers the Voluntary Reporting Scheme, under which merchant ships are encouraged to send daily reports, providing their position and ETA at their next port whilst transiting the region bound by Suez, 78°E and 5°S. UKMTO Dubai subsequently tracks ships, and the positional information is

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

Passed to CMF and EU headquarters. Emerging and relevant information affecting commercial traffic can then be passed directly to ships, rather than by company offices, improving responsiveness to any incident and saving time. For further information, or to join the Voluntary Reporting Scheme, please contact MTO Dubai: ukmtodubai@eim.ae. Below we give a summary of this information. FOLLOW UP REPORT PIRACY ATTACK

1 Ship's name and call sign, IMO number

2 Reference initial PIRACY ALERT3 Position of incident/Latitude/Longitude/Name of the area4 Details of incident:

- method of attack
- description/number of suspect craft
- number and brief description of pirates
- what kind of weapons did the pirates carry
- any other information (e.g., language spoken)
- injuries to crew and passengers
- damage to ship (which part of the ship was attacked?)
- action taken by the Master and crew
- was incident reported to the coastal authority and to whom?
- action taken by the Coastal State.

5 Last observed movements of pirates / suspect craft6 Assistance required7 Preferred communications with reporting ship: Appropriate Coast Radio Station/HF/MF/VHF/Inmarsat IDs (plus ocean region code)/MMSI8 Date/time of report (UTC)

## 6. Emergency Preparedness, Drills, and Exercises

### 6.1. Awareness of contingency plans


It will be explained in a simple way basic knowledge of plans for a variety of contingencies associated with terrorism and other criminal activities that may arise in the maritime setting.

It will be discussed the cases of bombs threats, explosions, piracy, armed robbery, hijackings, and similar events should be discussed. A contingency plan will be made with trained to check the skills acquired.

### 6.2. Security drills and exercises

The drills and exercises 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.

The drills be conducted at least once every month. 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.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SATS(I)-26</b>
	<b>SECURITY AWARENESS TRAINING FOR ALL SEAFARERS</b>	<b>REV. 5 - 2018</b>

The drills and exercise will also be carried out with the company to prove that it understands and has the competence for different cases of contingencies of security.

CONTROLLED COPY