SEAFARERS TRAINING CENTER INC

SECURITY TRAINING FOR SEAFARERS WITH DESIGNATED SECURITY DUTIES

MODEL COURSE 3.26

SCOPE

This course is intended to provide the knowledge required for Seafarers with designated security duties in connection with a Ship Security plan (SSP) to perform their duties in accordance with the requirements of chapter XI-2 of SOLAS 74 as amended, the ISPS code, and section A-VI/6 of the STCW Code, as amended.

OBJETIVE

Those who successfully complete the course should be able to demonstrate sufficient knowledge to undertake the duties assigned under the SSP. This knowledge shall include, but is not limited to:

1. Knowledge of current security threats and patterns;
2. Recognition and detection of weapons, dangerous substances and devices;
3. Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
4. Techniques used to circumvent security measures;
5. Crowd management and control techniques;
6. Security related communications;
7. Knowledge of emergency procedures and contingency plans;
8. Operation of security equipment and systems;
9. Testing, calibration and at-sea maintenance of security equipment and systems;
10. Inspection, control, and monitoring techniques; and
11. Methods of physical searches of persons, personal effects, baggage, cargo, and ship stores.

ENTRY STANDARDS

It is assumed that those attending this course will be serving seafarers or other shipboard personnel and are likely to have designated security duties in connection with the Ship Security Plan.

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 for “Security Training for Seafarers with Designated Security Duties”.

COURSE INTAKE LIMITATIONS

The maximum number of trainees will be 25 persons.

STAFF REQUIREMENTS

The instructor in charge of the course should have knowledge of the requirements of chapter XI-2 of SOLAS74 as amended, the ISPS Code, and security – related provisions of the STCW Code, as amended.

The instructors have appropriate training in or be familiar with instructional technical 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 player, TV, slide projector, overhead projector, etc.

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

Video(s)

Distance learning package (s)

National legislative and regulatory references

BIBLIOGRAPHY

Best Management Practices for Protection against Somalia Based Piracy (Published by Witheerby Publishing Group Ltd, Edinburg, Schotland, UK)

Fernandez, L. & Merzer, M (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. (2004). Pirates and Armed Robbers: A master's guide. (4th ed.). London: Marisec publication.

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

Sullivan, J.P., et al. (2002). Jane's Unconventional Weapons Response Handbook. (I s ted.). Alexandria: Jane's information group.

United States Coast Guard. (2002). Risk-based Decision Making Guidelines. PB2002500115 washington: NTIS.

United States Department of transportation. Volpe National Transportation System Center. (1999). Intermodal Cargo Transportation: Industry Best Security Practices. Cambridge: Volpe Center.

Violis, P., et al. (2002). Jane's Workplace Security Handbook. (1st ed). Alexandria: Jane's information group.

Timetable

- **Course Outline**

Subject Area	Approximate (Hours)	time
	Lecture	**Practical**
1. Introduction **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	1.0	
2. Maritime Security Policy **2.1.** Familiarity with relevant international conventions, codes, and recommendations **2.2.** Familiarity with relevant government legislation and regulations **2.3.** Definitions **2.4.** Handing sensitive security-related information and communications	0.75	
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 Officer **3.7.** Company Security Officer **3.8.** Port Facility Security Officer **3.9.** Seafarers with designated security duties **3.10.** Port facility personnel with designated security duties	1.25	

3.11. Other personnel		
4. Ship Security Assessment **4.1.** Assessment tools **4.2.** On-scene security surveys	1.0	
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	1.0	
6. Threat Identification, Recognition and Response **6.1.** Recognition and detection of weapons, dangerous substances and devices **6.2.** Methods of physical searches and non-intrusive inspections **6.3.** Execution and coordination of searches **6.4.** Recognition, on a non-discriminatory basis, of persons posing potential security risks **6.5.** Techniques used to circumvent security measures **6.6.** Crowd management and control techniques	1.5	
7. Ship Security Actions **7.1.** Actions required by different security levels **7.2.** Maintaining security of the ship/port interface **7.3.** Familiarity with the Declaration of Security **7.4.** Reporting security incidents **7.5.** Execution of security procedures	1.0	
8. Emergency Preparedness, Drills and Exercises **8.1.** Execution of contingency plans **8.2.** Security drills and exercises	1.0	
9. Security Administration	0.5	

9.1. Documentation and records		
Total:	**9**	

- **Course Timetable**

Day / Period	1st Period (2.0 hours)	2nd Period (2.0 hours)	3rd Period (2.5 hours)	4th Period (2.5 hours)
Day 1	**1 Introduction** 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 **2 Maritime Security Policy** 2.1 Familiarity with relevant international conventions, codes, and recommendations 2.2 Familiarity with relevant government legislation and regulations 2.3 Definitions	3.3 The company 3.4The ship 3.5 The port facility 3.6 Ship Security Officer 3.7 Company Security Officer 3.8 Port Facility Security Officer 3.9 Seafarers with designated security duties 3.10 Port facility personnel with designated security duties 3.11 Other personnel **4 Ship Security Assessment** 4.1 Assessment tools 4.2 On-scene	**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 Threat Identification, Recognition and Response** 6.1 Recognition and detection of weapons, dangerous substance and	**7 Ship Security Actions** 7.1 Actions required by different security levels 7.2 Maintaining security of the ship/port interface 7.3 Familiarity with the Declaration of Security 7.4 Reporting security incidents 7.5 Execution of security procedures **8 Emergency Preparedness, Drills and Exercises** 8.1 Execution of contingency plans 8.2 Security drills and exercises **9 Security**

	2.4 Handling sensitive security-related information and communication **3 Security Responsibilities** 3.1 Contracting governments 3.2 Recognized Security Organizations	security surveys	devices 6.2 Methods of physical searches and non-intrusive inspections 6.3 Execution and coordination of searches 6.4 Recognition, on a non-discriminatory basis, of persons posing potential security risks 6.5 Techniques used to circumvent security measures 6.6 Crowd management and control techniques	**Administration** 9.1Documentation and records

Manual

1. Maritime Security Policy

1.1Preamble

Maritime activity has always been a risky venture. Even in the early years, apart from the perils of the sea, pirates have posed immense danger to ships and seafarers. In the early middle Ages, the Vikings — natives of Scandinavia —raided and terrorized ships and settlements on the European coasts. Indian pirates, mostly from the Malabar Coast, too used to raid ships plying in the waters of the North Arabian Sea, Oman Sea and the

Persian Gulf and settlements along these coasts. They were so dreaded by the Persians, that they made the river Tigris inaccessible by placing massive stones at the mouth —which were removed only by Alexander the Great to make it navigable, on his return from India. Sailing ships, loaded with spices and gold from India and the far East, were easy targets to marauding pirates in their fast moving sailing vessels.

In the olden days, however, manpower was abundant and cheap (even free) and profits impressive. Shipowners could, therefore, afford to spend on security, to the extent that they armed their ships so they had the capability to retaliate and resist — and even commit acts of piracy on their own! Even Kings and Monarchs took measures to protect their shipping with some measure of success and at times even raided each other's ships for political and economic gains. With the advent of modern day nation states and the rule of international law, the world became more organized and united in rooting out evils like piracy; but it still exists in some parts of the world like the West Coast of Africa, Malacca Straits, etc. While yesterday's pirate had a patch over one eye. cutlass in his teeth and a parrot on his shoulder and sailed in a fast moving cutter, flying the Jolly Roger or the Skull and Crossbones, today's pirate is most often armed with AK-47 rifles and grenades and is a ruthless killer who moves in a speed boat. The only thing in common between both of them is probably the grapnel and rope to board the victim vessel. In more recent years, however, another dangerous phenomenon has raised its ugly head, i.e. terrorism.

1.2 Genesis of the ISPS Code

The Al Qaeda attack in the United States on September 11, 2001 brought about a drastic change in maritime legislation regarding security. On 13th December 2002, the IMO agreed to nine amendments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74). The SOLAS convention was chosen as the vehicle to expedite the imposition of the legislation as it was already in force and already applicable to *all passenger and cargo vessels over 500 tons engaged in international voyages and to mobile offshore oil and gas rigs.* This was implemented by merely redesignating Chapters and inserting a new one as the ISPS Code. (The existing chapter XI was amended and re-identified as Chapter XI-land a new Chapter XI- 2 was adopted on special measures to enhance maritime security). The ISPS code is divided into two Parts, i.e. Part 'A' and Part `13'**:** Part 'A' is divided into 19

regulations and 2 appendices and consists of the mandatory requirements regarding the provisions of Chapter XI-2 of SOLAS, 1974, as amended; which deals with special measures to enhance the maritime security. Part '13' consists of guidance regarding the provisions of Chapter XI-2 of SOLAS, 1974, as amended.

The chronology of events leading up to birth of the ISPS Code is as follows: chronology of events leading up to birth of the ISPS Code is as follows:

- November 2001 - Maritime Security Committee (MSC) establishes intercessional working group on Maritime Security.
- November 2001 - IMO adopts Resolution A.924 (22) for review of measures and procedures against terrorism.
- Feb 2002 - MSC Intercessional working group hold this first meeting.
- Mar. 2002 - The outcome of the meeting discussed by MSC.
- Sept. 2002 - MSC intercessional working group meets again.
- Dec. 2002 - MSC considered the outcome of the group meet and agrees that the proposed text be considered by the Diplomatic Conference.

- 12 December 2002 - Diplomatic Conference on Maritime Security held in London adopts new amendments to SOLAS — 74 and ISPS Code.

1.3ISPS Code — Objectives

To establish an international framework to detect security threats and take preventive measures against security incidents affecting ships and port facilities used in international trade. To establish the respective roles and responsibilities of all parties concerned at the national and international level for ensuring maritime security.

Parties involved in the implementation of the ISPS Code

- Contracting Government
- Government Agencies
- Shipping Industries
- Port
- Industries
- Local Administrations

1.4Definitions

The definitions of various terms used in the ISPS code are as follows Convention

Convention means the International Convention for the Safety of Life at Sea, 1974, as amended (SOLAS 74).

Regulation: Regulation means a regulation of the Convention.

Chapter: Chapter means a chapter of the Convention.

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

Port Facility Security Plan (PFSP): Port facility security plan (PFSP) 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.

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

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

Port Facility Security Officer: 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 the liaison with the ship security officers and company security officers.

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

Security Level 2: Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time. This could be due to heightened risk of a security incident.

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

Ship: The term "ship" when used in ISPS Code includes mobile offshore drilling units and high-speed crafts as defined in regulation XI-2/1.

2. Security Responsibilities

2.1 Contracting Governments

Subject to the provisions of regulations 3 and 7 of chapterXI-2 of SOLAS 74, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

(i) The degree that the threat information is credible,

(ii) The degree that the threat information is corroborated,

(iii) The degree that the threat information is specific or imminent, and

(iv) The potential consequences of such a security incident.

Contracting Governments, when they have set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected. Contracting Governments may delegate to a recognized security organization some of their security-related duties under chapter XI-2 of SOLAS 74 and this Part A of ISPS Code with the exception ISPS - I of:

- ✓ Setting of the applicable security level,
- ✓ Approving a port facility security assessment and subsequent amendments to an approved assessment,
- ✓ Determining the port facilities, which will be required to designate a Port Facility Security Officer,
- ✓ Approving a port facility security plan and subsequent amendments to an approved plan,
- ✓ Exercising control and compliance measures pursuant to Regulation 9 of Chapter XI-2 of SOLAS 74, and
- ✓ Establishing the requirements for a Declaration of Security,
- ✓ Shall to the extend they consider appropriate test the effectiveness of the ship security plan or the port facility security plan, or of amendments to such plans, they

- ✓ have approved, or in the case of ships, of plans which have been approved on their behalf,
- ✓ Should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to security assessment and port facility security plan, and to individual assessments or plans.
- ✓ May identify a Designated Authority within Government to undertake assessments or plans.
- ✓ May identify a Designated Authority within Government to undertake their security duties relating to a port facility as set out in chapter XI-2 of SOLAS 74 or Part A of ISPS Code.

The International Ship and Port facility Security Code (ISPS) was implemented by the International Maritime Organization (IMO) to establish a framework involving maritime nations and the shipping industry to enhance security at the sea.

Several steps have been taken under the ISPS code to enhance the security of ships. The main objective of ISPS code is to build co-operation between governments of maritime nations and the international shipping industry to detect security threats related to maritime operations.

Under the ISPS code, governments of maritime nations abiding by the implement rules are known as contracting governments (CG). The contracting government plays a vital role in order to ensure that the ISPS code is followed properly by the companies and port authorities. It is also the duty of the CG to assimilate information regarding possible maritime threats and their consequences. This information is then to be provided to the ships and ports in form of instructions and security guidelines.

It is also the duty of Contracting Government to carry out the following:

- ✓ Assign appropriate security levels after assessing the security information obtained
- ✓ To develop a port facility security plan (PFSP) to ensure that security measures are designed and assigned in a systematic manner for the protection of ships, ports, cargo, and ship personnel
- ✓ If required, the contracting government must assign a port facility security officer (PFSO) who will be responsible for the development, implementation, revision, and maintenance of the port facility security plan
- ✓ Exercise control and compliance of the ISPS code.
- ✓ Exercising the requirement of declaration of security (DOS). Declaration of security is a set of minimum security requirements, which a ship can ask for when dealing with another ship or port.
- ✓ Develop and test the performance of the ship security plan (SSP) and port facility security plan (PFSP), and amend them as and when required

It is necessary that the contracting governments work in coordination with the ISPS authority, gathering and assessing information regarding security threats to the shipping industry.

2.2 Recognized Security Organizations

Contracting Governments may authorize a Recognized Security Organization (RSO) to undertake certain security-related activities, including:

- ✓ Approval of a ship security plan, or amendment thereto, on behalf of the Administration;
- ✓ Verification and certification of compliance of a ship with the requirements of Chapter XI-2 of SOLAS 74 and Part A of ISPS Code on behalf of the Administration.
- ✓ Conducting port facility security assessment required by the Contracting Government.
- ✓ An RSO may also advise or provide assistance to a Company or port facility on security matters, including ship security assessment, ship security plan, port facility security assessment and port facility security plan. This can include completion of an SSA or SSP or PFSA or PFSP. If an RSO has done so in respect of an SSA or SSP that RSO is not authorized to approve that SSP. When authorizing a RSO, Contracting Governments should give consideration to the competency of such an organization. A RSO should be able to demonstrate.
- ✓ Expertise in relevant aspects of security.
- ✓ Appropriate knowledge of ship and port operations, including knowledge of ship design and construction and if providing services in respect of port facilities.

Information submitted by Member States under MSC/Circ.1010-MEPC/Circ.382 on flag States' authorizations to carry out surveys and issue certificates on their behalf is available in the Recognized Organizations module of GISIS.

The Sub-Committee on Flag State Implementation (FSI) developed a new code for recognized organizations (ROs), with discussion on its purpose, framework and structure, based on all existing requirements and recommendations of IMO instruments regarding recognized organizations. Some important resolutions relating to ROs include resolutions A. 739(18) on Guidelines for the authorization of organizations acting on behalf of the Administration and A.789(19) on Specifications on the survey and certification functions of recognized organizations acting on behalf of the Administration.

The Code provides a consolidated instrument containing criteria against which ROs are assessed and authorized/recognized, and gives guidance for subsequent monitoring of ROs by Administrations.

2.3 The Company

The ISPS code lays down specific requirements for the Company. It is the aim of this chapter to guide the Ship Owners in interpreting these guidelines so as to arrive at specific implementation actions. The ISPS code specifies the following requirements for the Company.

Master's Authority

The ship security plan must clearly emphasize the Master's overriding authority and responsibility to make decisions to ensure security of the ship. The Master may request the assistance of the Company or any Flag or Port State as may be necessary.

Company's Responsibility

Each shipping company or the operator must designate at least one Company Security Officer to be responsible for developing, implementing, and maintaining Ship Security Plan for every Ship in the company fleet. Likewise, the company or the operator must designate a Company Security Officer for each ship in the Company fleet of ships.

Company Support

The company must ensure that the Company Security Officer, each Master, and each ship security officer have the necessary support to fulfill their duties and responsibilities outlines in SOLAS 74 and the ISPS Code and the ISPS – I Ship Security Plan. The necessary information that must be provided by the Company to the Master includes the following: Parties, such as the ship management company, manning agents, contractors, and/or concessionaires, who are responsible for appointing shipboard personnel.

- ✓ Parties who are responsible for deciding the employment of the ship, for example bareboat charterer(s).
- ✓ Contact information for time or voyage charterers, when a ship is employed under a charter party agreement.

The company must keep all information current and updated for changes that may occur. Only current, up-to-date information on any given date must be kept on board. The Company is not responsible for keeping or providing information that relates to a previous owner or operator of the ship. As required by the IMO, the name of the persohn or organization who appoints the members of the crew or other persons employed or engaged on board the ship in any capacity on the business of the ship is:

- ✓ Ship´s Owner (Name and Address);
- ✓ Company Security Officer;
- ✓ Ship´s Manager/Operator (Name and Address);
- ✓ Company Responsible for Employment of Ship (including sub charterer if any) (Name and Address); and
- ✓ Company Responsible for Manning (Name and Address).

2.4 <u>The Ship</u>

It is required to act upon the security levels set by Contracting Governments.

At level 1:

- ✓Ensure the implementation of all tasks related to security;

- ✓Controlling access to the ship;
- ✓Ensure the immediate availability of the means to security communication.
- ✓Controlling the embarkation of persons and their effects;
- ✓Monitoring restricted areas to have access only to authorized persons;
- ✓Monitoring deck areas and areas surrounding the ship;
- ✓Supervising the handling of cargo and ship's stores; and
- ✓Ensure the immediate availability of the means to security communication.

At level 2:

The additional protective measures specified in the ship security plan shall apply;

At level 3:

- ✓The other concrete protection measures specified in the ship security plan shall apply;
- ✓When the Administration establish a level 2 or 3, the ship shall acknowledge receipt of the instructions on changing the level of protection;
- ✓Before entering a port within the territory of a Contracting Government that has set security level 2 or 3, or whilst on it, the ship shall acknowledge receipt of the instruction and confirms the security officer of the port facility has started the implementation of appropriate procedures and actions identified in the ship security plan; and, in the case of security level 3, the instructions given by the Contracting Government that has set security level.
- ✓The ship shall report any difficulties for implementation. In these cases, the security officer of the port facility will remain in contact with the ship security officer to coordinate appropriate actions.

If the Administration requires a vessel to establish a more elevated level than the port it intends to enter or already are, or if the ship was operating at that level, the vessel shall report this fact immediately Protection the competent authority of the Contracting Government within whose territory the port facility is located security officer and port facility.

✓In such cases, the ship security officer shall liaise with the security officer and port facility coordinate appropriate actions, if necessary.

The Company and the Ship

Any shipping company operating ships to which the Code applies shall appoint a Company Security Officer (CSO) for the company and a Ship Security Officer (SSO) for each of its ships. The responsibilities of these officers are defined, as are the requirements for their training and drills. The training needs and requirements of the SSO are being developed in the context of the STCW Convention. The CSO's responsibilities include ensuring that a Ship

Security Assessment (SSA) is undertaken and that a Ship Security Plan (SSP) is prepared for each ship to which the Code applies.

The Ship Security Plan indicates the minimum operational and physical security measures the ship shall take at all times, i.e. while operating at security level 1. The plan will also indicate the additional, or intensified, security measures the ship itself can take to move to security level 2. Furthermore, the Plan will indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by the authorities responding at security level 3 to a security incident or threat. The need for these plans to be ultimately incorporated in the ISM Code has been acknowledged. The Ship Security Plan must be approved by, or on behalf of, the ship's Administration. The Company and Ship Security Officer are required to monitor the continuing relevance and effectiveness of the Plan, including the undertaking of independent internal audits. Any amendments to specified elements of an approved Plan will have to be resubmitted for approval.

SOLAS chapter XI-2 and the ISPS Code include provisions relating to the verification and certification of the ship's compliance with the requirements of the Code on an initial, renewal and intermediate basis. The ship must carry an

International Ship Security Certificate (ISSC) indicating that it complies with the Code. The ISSC is subject to Port State Control (PSC) / maritime security control and compliance inspections but such inspections will not extend to examination of the Ship Security Plan itself. The ship may be subject to additional control measures if there is reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

The ship may be required to provide information regarding the ship, its cargo, passengers and crew prior to port entry and it is the responsibility of the company that up to date information relating to the ownership and control of the vessel is available on board. There may be circumstances in which entry into port could be denied, if the ship itself, or the port facility it served before, or another ship it interfaced with previously, are considered to be in violation with the provisions of SOLAS chapter XI-2 or part A of the ISPS Code.

Further guidance on control and compliance measures and reporting requirements are given in:

Annex 2 to MSC/Circ.1111 on Guidance relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code (also adopted as Resolution MSC.159 (78) on Interim Guidance on Control and Compliance Measures to Enhance Maritime Security);

MSC/Circ.1113 on Guidance to Port State Control Officers on the non-security related elements of the 2002 SOLAS Amendments;

MSC/Circ.1130 on Guidance to masters, Companies and duly authorized officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port;

MSC/Circ.1133 on Reminder of the obligation to notify flag States when exercising control and compliance measures; and

MSC/Circ.1156 on Guidance on the access of public authorities, emergency response services and pilots onboard ships to which SOLAS chapter XI-2 and the ISPS Code apply.

The implementation of the mandatory fitting of ship-borne Automatic Identification Systems (AIS) for all ships of 500 gross tonnage and above, on international voyages was accelerated, through amendments to Regulation 19 of SOLAS Chapter V, to 31 December 2004, at the latest.

There is also a requirement for fitting ships with a ship security alert system (SSAS) for seafarers to use to notify authorities and other ships of a terrorist hijacking, and appropriate performance standards and procedures for fitting such systems on board ships have been developed. Further guidance on SSAS is given in MSC/Circ.1072 on "Guidance on provision of ship security alert systems", MSC/Circ. 1073 on "Directives for maritime rescue co-ordination centres (MRCCs) on acts of violence against ships", MSC/Circ. 1109 on "False security alerts and distress/security double alerts" and MSC/Circ. 1155 on Guidance on the message priority and the testing of the ships security alert systems.

IMO considered the issue of maritime security equipment and measures to prevent unauthorized boarding in ports and at sea. It is recognized that the type of equipment to be used on board would depend largely on risk assessment
(e.g. ship types, trading areas). The section of the ISPS Code addressing the Ship Security Plan includes the consideration of such equipment and measures.

It was recognized that urgent action on an up-to-date seafarer identification document was needed. In this regard, new specifications for seafarer identification have been agreed as the Seafarers Identity Documents (Revised), Convention (No. 185), which was adopted by ILO in June 2003, and which revises ILO Convention No. 108.

2.5 The Port Facility

A port facility is required to act upon the security levels set by 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 without, or delay to, passengers, ship, ships personnel and visitors, goods and services. At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in Part B of ISPS Code, in order to identify and take preventive measures against security incidents.

- ✓ Ensuring the performance of all port facility security duties;
- ✓ Controlling access to the port facility;
- ✓ Monitoring of the port facility, including anchoring and berthing area(s);

- ✓ Monitoring restricted areas to ensure that only authorized persons have access;
- ✓ Supervising the handling of cargo;
- ✓ Supervising the handling of ship`s stores; and
- ✓ Ensuring that security communication is readily available.

At security level 2, additional protective measures, specified in the Port Facility Security Plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in Part B of this Code. At security level 3, further specific measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in Part B of ISPS Code. In addition, at security level 3, port facility is required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located. When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of Chapter XI-2 of SOLAS 74 of ISPS code or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the Port Facility Security Officer and the Ship Security Officer shall liaise and co-ordinate appropriate actions. When a Port Facility Security Officer is advised that a ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

Contracting Governments are required to undertake Port Facility Security Assessments (PFSA) of their Port Facilities. These assessments shall be undertaken by the Contracting Government, a Designated Authority, or the Recognized Security Organization. Port Facility Security Assessments will need to be reviewed periodically. The results of the Port Facility Security Assessment have to be approved by the Government or Designated

Authority and are to be used to help determine which Port Facilities are required to appoint a Port Facility Security Officer (PFSO).

The responsibilities of the Port Facility Security Officers are defined in the ISPS Code, as are the requirements for the training they require and the drills they are responsible for undertaking. The Port Facility Security Officer is responsible for the preparation of the Port Facility Security Plan (PFSP).

Like the Ship Security Plan, the Port Facility Security Plan shall indicate the minimum operational and physical security measures the Port Facility shall take at all times, i.e. while operating at security level 1. The plan should also indicate the additional, or intensified, security measures the Port Facility can take to move to security level 2.
Furthermore the plan should indicate the possible preparatory actions the Port Facility could take to allow prompt response to the instructions that may be issued by the authorities responding at security level 3 to a security incident or threat.

The Port Facility Security Plan has to be approved by the port facility’s Contracting Government or by the Designated Authority. The Port Facility Security Officer must ensure that its provisions are implemented and monitor the continuing effectiveness and relevance of the approved plan, including commissioning independent internal audits of the application of the plan. The effectiveness of the plan may also be tested by the relevant Authorities. The Port Facility Security Assessment covering the Port Facility may also be reviewed. All these activities may lead to amendments to the approved plan. Major amendments to an approved plan will have to be submitted to the approving authority for re-approval.

2.6 Ship Security Officer

Ship security officer (SSO) means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers. The company designates the SSO. The SSO is the executive instrument of the Ship Security Plan. Needless to say that an excellent security plan will yield no results unless it is implemented by an intelligent and security conscious individual.

Ship's security is one of the greatest concerns for every shipping company whose ships ply in international waters. Though there are advanced systems such as ship security alert system (SSAS) and ship security reporting system (SSRS) to enhance maritime security, contribution of the crew towards ship's security play a very important role.

The main duties of the ship security officer (SSO) include implementation and maintenance of a ship security plan, while working closely with the company security officer (CSO) and the port facility security officer (PFCO).

According to the ISPS code, every ship must have a ship security officer, who has the full responsibility of the ship's security.

The main responsibilities of ship security officer (SSO) are:

- ✓ Implementing and maintaining the ship security plan (SSP)

- ✓ Conducting security inspections at regular intervals of time to ensure that proper security steps are taken
- ✓ Making changes to the ship security plan if need arise
- ✓ Propose modifications to the ship security plan by taking various aspects of the ship into consideration
- ✓ Help in ship security assessment (SSA)
- ✓ Ensure that the ship's crew is properly trained to maintain a high ship security level
- ✓ Enhance security awareness and vigilance on board ship
- ✓ Guide ship's crew by teaching ways to enhance ship's security
- ✓ Report all security incidents to the company and the ship's master
- ✓ Taking view and suggestions of the company security officer and the port facility security officer into consideration while making amendments to the ship security plan.
- ✓ Help company security officer (CSO) in his duties
- ✓ Take into account various security measures related to handling of cargo, engine room operations, ship's store etc.
- ✓ Coordinate with ship board personnel and port authorities to carry out all ship operations with utmost security.
- ✓ Ensure that the ship security equipment is properly operated, tested, calibrated, and maintained.

The duties of ship security officer might change, increase, or decrease, depending on the type of the ship and situation. However, the main duties remain the same as mentioned above.

The importance of maritime security has substantially increased with the increase in the number of piracy attacks. This has also lead to a sudden increase in demand of maritime security jobs . Many companies offer special maritime security services to ensure high level of ship and port security. However, it is to note that most of the ship security related troubles can be averted by having a sound ship security plan.

Periodic Review Procedures

The SSO is responsible for ensuring a Ship Security Assessment is carried out. The SSO must review the Ship Security Plan at least twice within five years. In addition, internal audits shall be arranged by the Company Security Officer to review the effectiveness of the Ship Security Plan. The Ship Security Plan is reviewed to ensure its efficiency, continuing suitability and effectiveness, with a view to consider the need for improvement. The aim is to re-examine all the procedures in use to see whether any improvements can b e done and whether the procedures are still relevant. Procedures may need to' be amended due to instructions from owners or fitting of new equipment. When the SSP has been put to use as a response to a Security Level 2 or 3, or in a drill, all parties directly involved shall comment on the effectiveness of the SSP and its content to the SSO.

2.7 Company Security Officer

A Company Security Officer (CSO) is a person designated by the shipping company to be responsible for developing, implementing and maintaining individual Ship Security Plan for all or part of the company fleet of ships. Depending on how the fleet of ships is organized, a Company may designate more than one CSO as long as it is clear who the CSO for a particular ship is. Company security officer also 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 SSO

The company security officer designated by a company would be responsible for one or more than one ships, depending on the number and types of ships the company operates. This responsibility is clearly identified.

Every shipping company assigns a set of responsibilities for the company security officer depending of the type of ships and cargo which the company operates. However, basic responsibilities of company security officer remain the same.

Responsibilities of Company Security Officer (CSO)

- ✓ Ship security plan (SSP) along with ship security assessment (SSA), play an important role in ensuring the security of the ship. The company security officer is responsible for carrying out the ship security plan in an efficient manner.
- ✓ Using the data acquired from the ship security assessment (SSA), the company security officer would advise on various threats which are likely to be encountered by the ship and would also decide the ship security level.
- ✓ The company security officer (CSO) would arrange for internal audits and reviews of security activities.
- ✓ On the basis of various observations and results from the ship security assessment, the company security officer would make developments in the ship's security plan.
- ✓ He would also seek for the approval to the submissions made on the basis of the results of the assessments.

- ✓ He would also modify the ship security plan to get rid of deficiencies in the security measures and to satisfy security requirements of each ship. Thereafter, he would ensure that the plan is implemented and maintained in the best possible manner.
- ✓ Company security officer would take measures to enhance security awareness and vigilance in his staff and also among ship personnel
- ✓ He would also arrange for the initial and subsequent verifications of the ship by the administration or the recognized security organization
- ✓ He would ensure that adequate training is provided to those responsible for the security of the ship.
- ✓ In case deficiencies and non-conformities are found during internal audits, periodic reviews, security inspections and verification of compliance, the security officer would address and deal with them to the earliest.
- ✓ He would ensure consistency between security requirements and safety requirements of the ship
- ✓ He would see to it that an effective communication and cooperation between the ship security officer and relevant port facility security officer is maintained
- ✓ In case security plan of a sister ship or fleet security system is used, he would make sure that the plan for each ship would reflect the ship-specific information accurately
- ✓ Company security officer would also ensure that the an alternative, equivalent arrangement for safety of each ship is implemented and maintained

2.8 Port Facility Security Officer

The person designated to take responsibility for the development, implementation, review and updating of the plan to protect the port facility and for coordination with security officers of ships and officers of companies to maritime security.

A port facility security officer (PFSO) shall be designated for each port facility. A person may be designated as the port security officer for one or more port facilities. In addition to those specified in ISPS Code.

Responsibilities of Port Facility Security Officer (PFSO)

- ✓ Carry out a full initial evaluation of the port facility, taking into account the relevant security assessment of the port facility;
- ✓ Ensuring the development and maintenance of the security plan of the port facility;
- ✓ Implement the plan to protect the port facility, and practice with him;
- ✓ Perform regular security inspections of the port facility to ensure that protective measures remain adequate;
- ✓ Recommending and incorporating, as appropriate, modifications to the plan to protect the port facility to correct deficiencies and to update the plan according to the changes that you have in the facility;
- ✓ Raise the level of awareness and vigilance among staff of the facility;
- ✓ Ensure that adequate training has been provided to the responsible protection of the port facility;

- ✓ Inform the relevant authorities of the events that threaten the security of the port facility and keep a record thereof;
- ✓ Coordinate the implementation of the security plan with the relevant port facility security officers of ships and officers of companies to maritime security;
- ✓ Coordinate with services, as appropriate;
- ✓ Ensure that standards for personnel responsible for the security of the port facility are met;
- ✓ Ensure the operation, calibration and test proper maintenance of protective equipment, if any; and
- ✓ Help security officers of ships to confirm the identity of persons seeking to board when asked.

2.9 Seafarers With Designated Security Duties

The seafarers working on board vessels who have designated security duties. Has the required knowledge to enhance maritime security awareness by recognizing security threats, and understanding the need for and methods of maintaining security awareness and vigilance.

You should understand their responsibilities for ship security and port facilities, as described in the plan of ship security and protection plan of the port facility, and should have sufficient knowledge and ability to perform the duties as assigned.

Tasks may require:

- ✓ Knowledge of current trends and threats related to protection;
- ✓ Recognition and detection of weapons, dangerous substances and devices;
- ✓ Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- ✓ Techniques used to circumvent security measures;
- ✓ Management techniques and crowd control;

- ✓ Communications relating to protection;
- ✓ Operation of equipment and systems;
- ✓ Testing, calibration and maintenance of equipment and systems;
- ✓ Technical inspection, control and monitoring;
- ✓ Methods of physical searches of persons, personal effects, baggage, cargo and ship's stores.
- ✓ Knowledge of emergency procedures and contingency plans of the ship;

2.10 <u>Port Facility Personnel with Designated Security Duties</u>

Vessel Personnel with Specific Security Duties

The Master is responsible for the safety and security of the crew, passengers and cargo. The development of general security policies and procedures is the responsibility of the CSO. The SSO is responsible for implementing, maintaining and supervising the Ship Security Plan. The specific security duties for each personnel will be laid down in the Ship Security Plan.

Duties and Responsibilities of the Security Watch

The security watch must be aware of the:

- Security level the ship is operating in. A sharp lookout shall be maintained.
- Suspicious persons, objects and activities and malfunctions of security equipment shall be reported to the duty officer.

Communication

To summon assistance, the security watch shall be provided with means of communications to keep in touch with the duty officer.

Briefings

All officers and crewmembers are to be briefed about their duties and the security level the ship is in at every change of security level, on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

Officer of the Watch (OOW)

It is the responsibility of the Watch Officer on the Deck or Bridge to

- ✓ Familiarize him-herself with all current security standing orders before before coming on duty**.**
- ✓ Be responsible for all specific security duties being carried out on board and/or any additional duties passed on by the Master.
- ✓ Know the current Security Level and the security measures that have been implemented.
- ✓ Be aware of the immediate recall procedures in case of an emergency.
- ✓ Brief the on coming watches as to the current security level, their standing orders and any additional specific security measures in place.
- ✓ Ensure all watches are in acceptable dress and are neat and tidy in appearance.
- ✓ Ensure all watches are equipped with the proper security equipment to enable them to carry out their duties.
- ✓ Ensure gangway and roving patrol watches are relieved promptly for meals and at the end of the tour of duty. Ensure that a copy of the standing orders for each post is available at the post.
- ✓ Ensure all watches know how to report any incidents or problems.
- ✓ Check the gangway log and visitor badge issue arrangements when coming on duty and at least once between at the beginning and end of watch.
- ✓ Visit all duty personnel at least once before midnight and once between midnight and 0600.
- ✓ Record all visits in the security log.
- ✓ Ensure the Master and Ship's Security Officer's contact details in case of emergency.
- ✓ Tour the ship randomly and visit all restricted areas, check all mooring lines, rat guards lounge areas and all around berthing area.

- ✓ Brief relieving OOW as to the current security level, the standing orders and any additional specific security measures in place.
- ✓ Record the handover/takeover of duties in the security log.

All other Ship's Officers

- ✓ Assist the SSO for reporting a security incident or potential security breaches.
- ✓ Assist the SSO in implementing security measures at each security level and report any nonconformities or failures.
- ✓ Be responsible, while on duty, for implementing the requirements of the SSP relevant to their position.

2.11 Other Personnel

Crew Members

All crew members and employees should make themselves familiar with the contents of the SSP and relevant supporting orders. They are to be familiar with their duties as laid down in ship security plan. The Security requirements of a port facility will be determined through port facility security assessment. The security duties of various port facility personnel will depend upon the type and degree of security required at the various port facilities. These duties will be contained in the port facility security plan.

- ✓ Have sufficient knowledge of the relevant provisions of the protection plan and be familiar with the following:
- ✓ The meaning of each of the levels of protection and the resulting requirements;
- ✓ Knowledge of emergency procedures and contingency plans on ships;
- ✓ Recognition and detection of weapons, dangerous substances and devices;
- ✓ Attribution, non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security; and
- ✓ Techniques used to circumvent security measures.

3. Ship Security Assessment

Security Assessment is a risk-based decision making tool. It is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual and function and, based on that, to identify actions to reduce the Vulnerability and mitigate the consequences of a security breach. The Ship Security Plan is based on the results of the Security Assessment. The most essential part of developing or updating an effective Ship Security Plan is undertaking a comprehensive, written Ship Security Assessment. The Ship Security Assessment is the responsibility of the Company. Security Office, even through he may delegate the task to other competent people with appropriate skills and experience. Such as a "Recognized Security Organization" authorized by the Flag State. Security Survey means an inspection, check -and / or audit to control and improve the mitigation strategy. Protective measures and actions in the Ship Security Plan. The ship security assessment shall he documented, reviewed, accepted and retained by the Company.

The Ship Security Assessment (SSA) is to be carried out before developing the Ship Security Plan (SSP), and is a major element in the process of developing or updating the SSP.

It is the responsibility of the Company Security Officer (CSO) to ensure that the SSA is carried out by persons with appropriate skills, for each ship in the company fleet.

The SSA shall include the following steps, which should than be adapted to each type of ship:

- ***Identification of key shipboard operations***

In this step, the company is to clearly identify what are the key shipboard operations with respect to security, this is to identify:

- ✓ The operations
- ✓ The systems and equipment
- ✓ The areas and spaces on-board the ship

- ✓ The crew and personnel on-board
- ✓ All elements, which can be considered as critical if, subjected to a security incident

As an example:

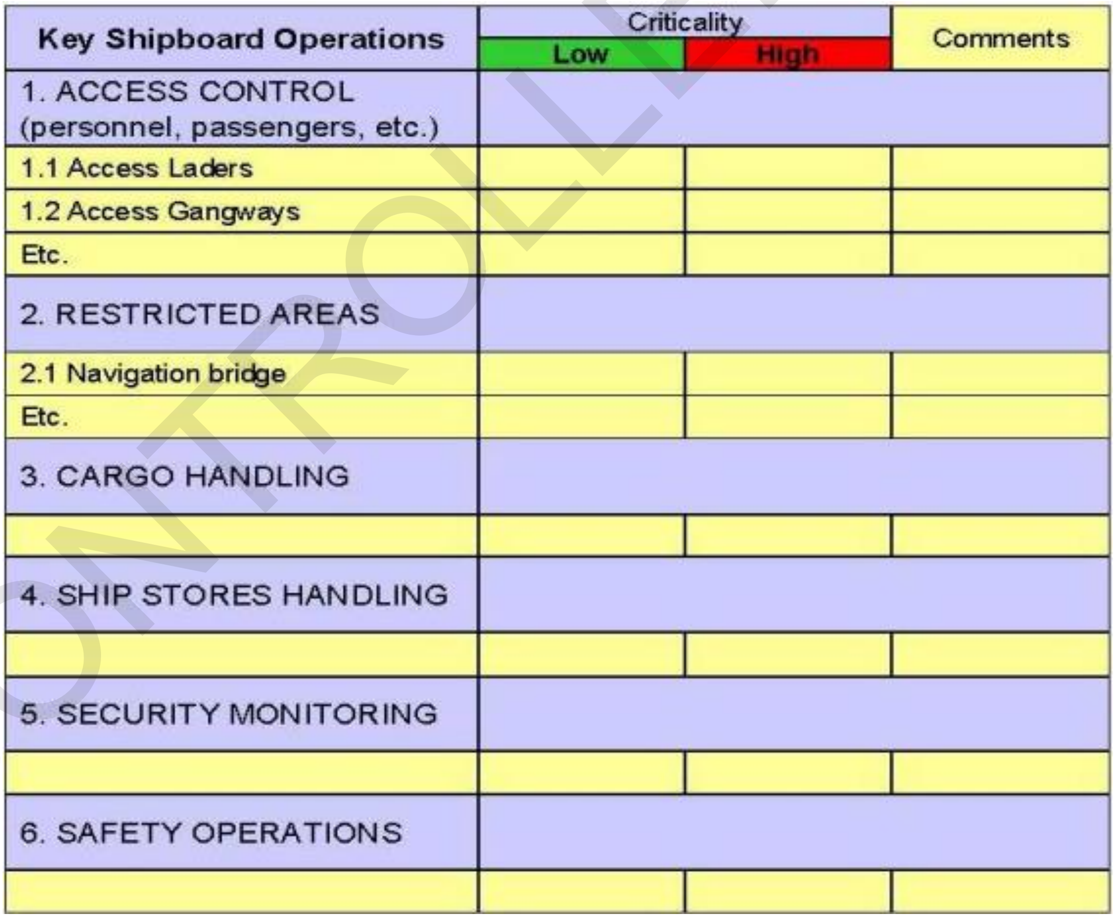
The critical operations may include the cargo handling, the ship stores handling, and the navigation.

The critical spaces may include the stores, the bridge, the machinery spaces including the Engine

Control Room (ECR) and the steering control station.

The critical systems may include the security alert system.

The company may list these "key shipboard operations", for each ship, and prioritize these operations:



Key Shipboard Operations	Criticality		Comments
	Low	High	
1. ACCESS CONTROL (personnel, passengers, etc.)			
1.1 Access Laders			
1.2 Access Gangways			
Etc.			
2. RESTRICTED AREAS			
2.1 Navigation bridge			
Etc.			
3. CARGO HANDLING			
4. SHIP STORES HANDLING			
5. SECURITY MONITORING			
6. SAFETY OPERATIONS			

Key Shipboard Operations

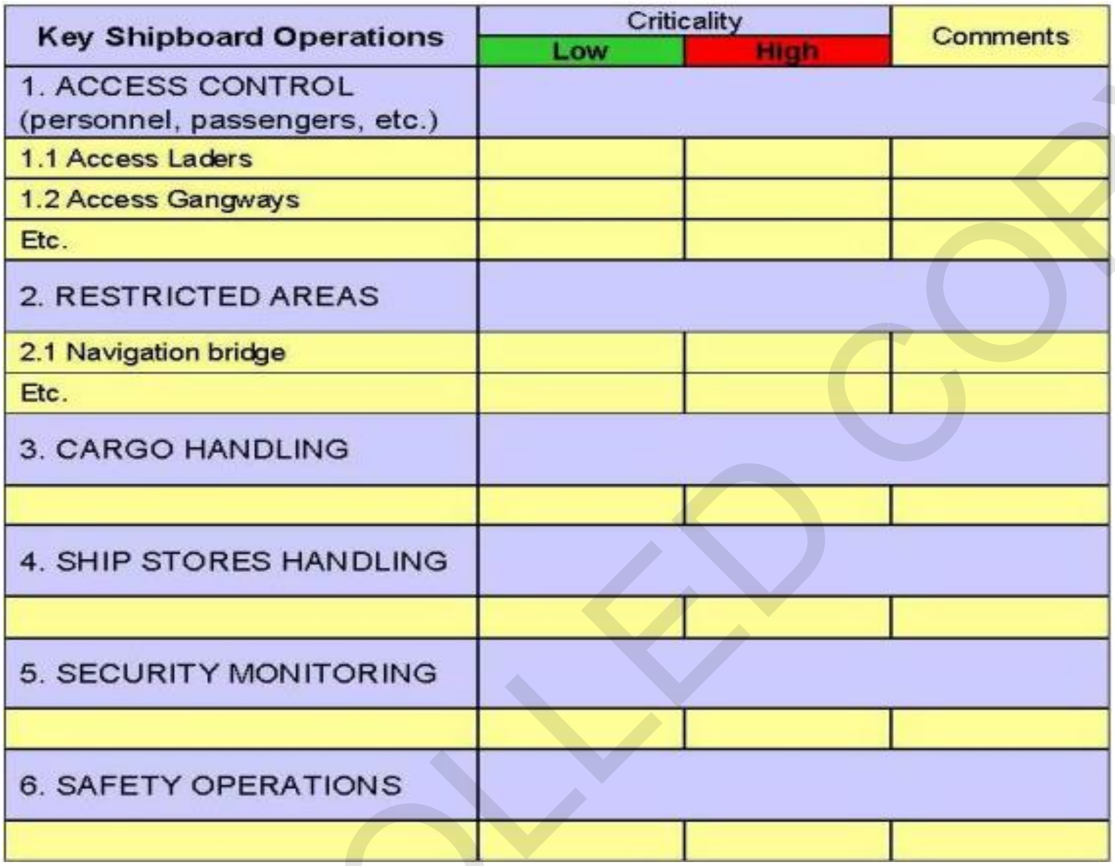
- ***Identification of existing security measures and procedures***

The aim of this step is, for the company, to clearly identify and describe the existing security measures, procedures and operations.

As an example, security procedures may include (but are not limited to):

- ✓ Procedures for response to emergency conditions (fire, flooding…)
- ✓ Procedures for security patrols
- ✓ Procedures for handling surveillance equipment, if any
- ✓ Procedures for handling security communication systems
- ✓ Procedure for handling security doors, barriers and lighting

The company may list the existing measures / procedures for each key shipboard operation. This will allow the company to identify any key shipboard operation with inappropriate security measure, inexistent, too limited or weak:



Key Shipboard Operations	Criticality		Comments
	Low	High	
1. ACCESS CONTROL (personnel, passengers, etc.)			
1.1 Access Laders			
1.2 Access Gangways			
Etc.			
2. RESTRICTED AREAS			
2.1 Navigation bridge			
Etc.			
3. CARGO HANDLING			
4. SHIP STORES HANDLING			
5. SECURITY MONITORING			
6. SAFETY OPERATIONS			

Existing security measures and procedures

- ***Identification of potential threats (refers to threat scenarios)***

In this step, the company is to clearly identify the potential threat scenarios to a ship under specific circumstances.

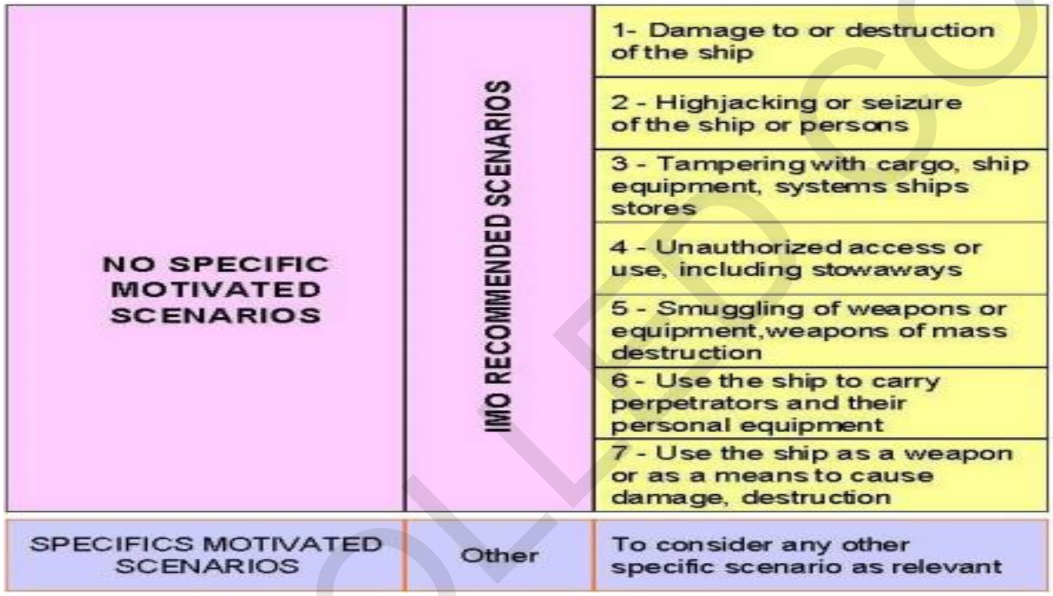
It is of the utmost importance that the threat scenarios that are identified as being possible remain "credible", in order for the Ship Security Assessment to be as efficient as possible.

These threat scenarios should consequently encompass the specific features of the ship in terms of type of ship, crew, cargo, trade, area and ports. To this end, it will be useful to consider what are the possible situations, which could motivate security threats:

- ✓ Political
- ✓ Image
- ✓ Economical
- ✓ Fear driven

For any of these situations, the review should aim at establishing whether the motivation factors are unlikely, probable or likely to occur. Particular threat scenarios should then be considered accordingly.

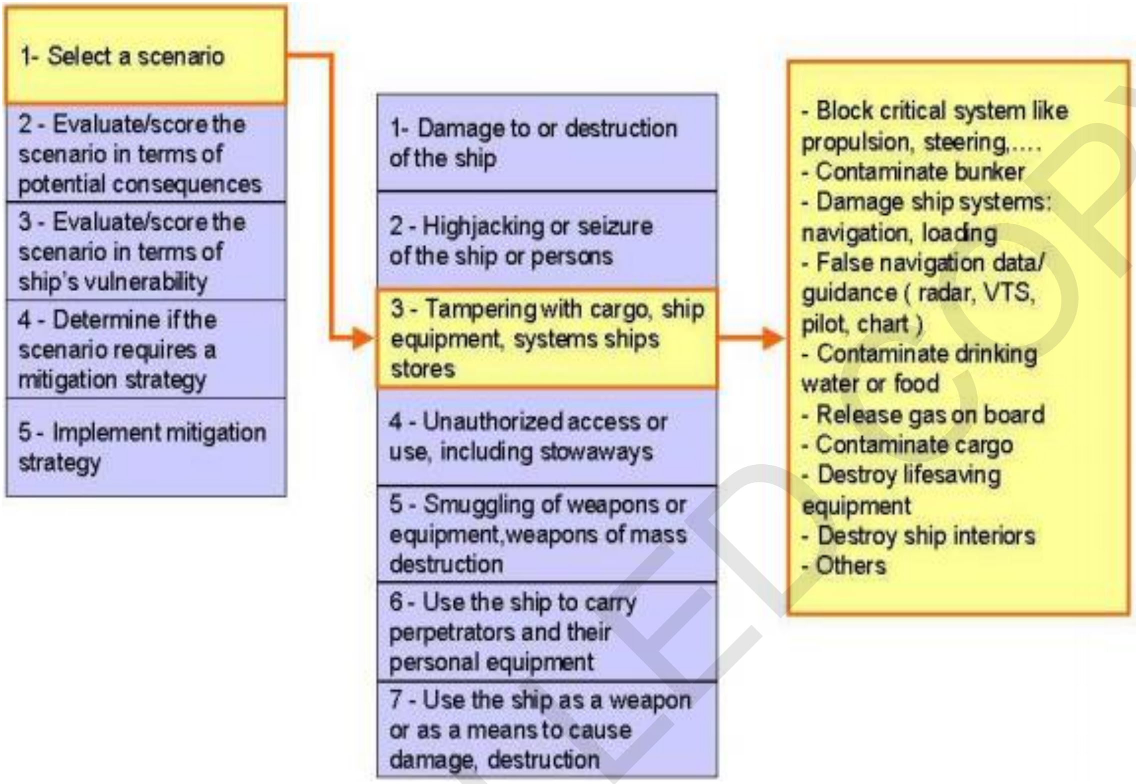
The company may then list and describe the potential threat scenarios, especially the ones it considers particularly relevant in its case:



NO SPECIFIC MOTIVATED SCENARIOS	IMO RECOMMENDED SCENARIOS	1- Damage to or destruction of the ship
		2 - Highjacking or seizure of the ship or persons
		3 - Tampering with cargo, ship equipment, systems ships stores
		4 - Unauthorized access or use, including stowaways
		5 - Smuggling of weapons or equipment,weapons of mass destruction
		6 - Use the ship to carry perpetrators and their personal equipment
		7 - Use the ship as a weapon or as a means to cause damage, destruction
SPECIFICS MOTIVATED SCENARIOS	Other	To consider any other specific scenario as relevant

Potential threat scenarios

A consequence assessment (in terms of injury or death, economic and environmental impact) and a risk (vulnerability) assessment should then be carried out for each scenario, in order to determine whether existing security measures and procedures are sufficient, whether they shall be improved or whether additional new security measures and procedures are required.



1- Select a scenario

2 - Evaluate/score the scenario in terms of potential consequences

3 - Evaluate/score the scenario in terms of ship's vulnerability

4 - Determine if the scenario requires a mitigation strategy

5 - Implement mitigation strategy

1- Damage to or destruction of the ship

2 - Highjacking or seizure of the ship or persons

3 - Tampering with cargo, ship equipment, systems ships stores

4 - Unauthorized access or use, including stowaways

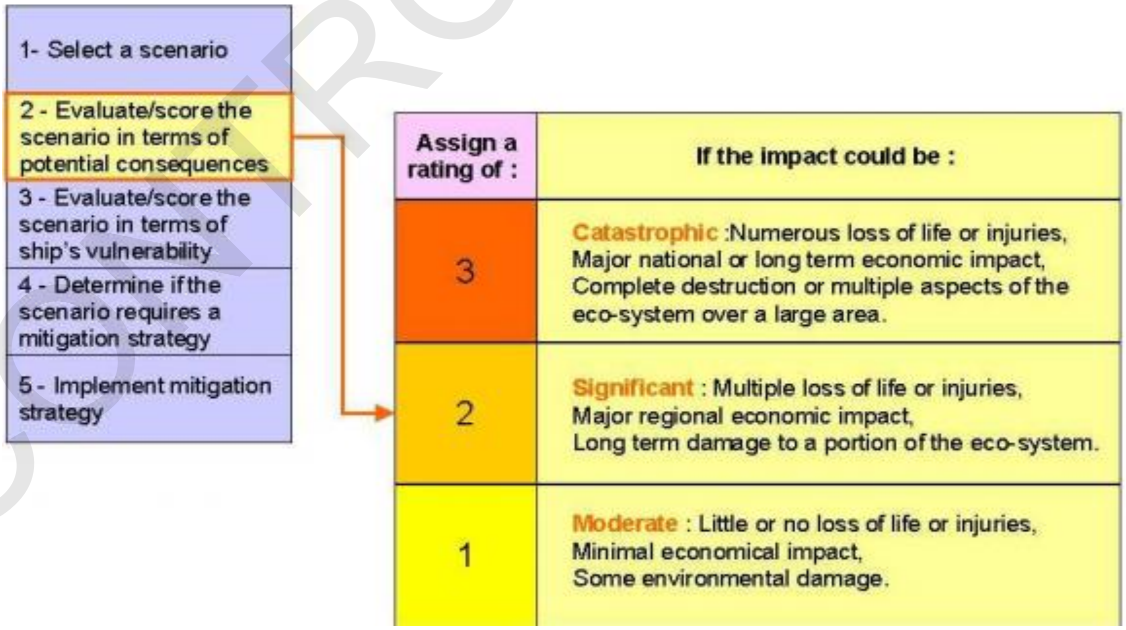
5 - Smuggling of weapons or equipment,weapons of mass destruction

6 - Use the ship to carry perpetrators and their personal equipment

7 - Use the ship as a weapon or as a means to cause damage, destruction

- Block critical system like propulsion, steering,....
- Contaminate bunker
- Damage ship systems: navigation, loading
- False navigation data/ guidance (radar, VTS, pilot, chart)
- Contaminate drinking water or food
- Release gas on board
- Contaminate cargo
- Destroy lifesaving equipment
- Destroy ship interiors
- Others

Select a scenario



1- Select a scenario

2 - Evaluate/score the scenario in terms of potential consequences

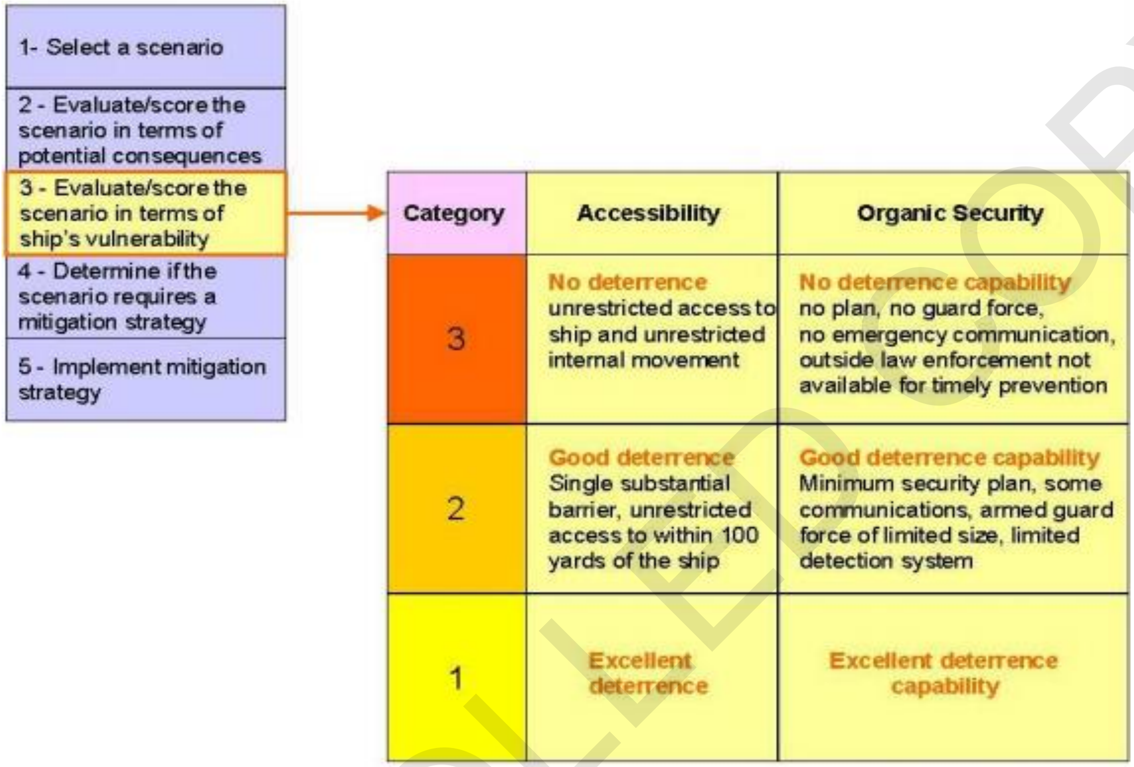
3 - Evaluate/score the scenario in terms of ship's vulnerability

4 - Determine if the scenario requires a mitigation strategy

5 - Implement mitigation strategy

Assign a rating of :	If the impact could be :
3	Catastrophic :Numerous loss of life or injuries, Major national or long term economic impact, Complete destruction or multiple aspects of the eco-system over a large area.
2	Significant : Multiple loss of life or injuries, Major regional economic impact, Long term damage to a portion of the eco-system.
1	Moderate : Little or no loss of life or injuries, Minimal economical impact, Some environmental damage.

Consequence score



1- Select a scenario

2 - Evaluate/score the scenario in terms of potential consequences

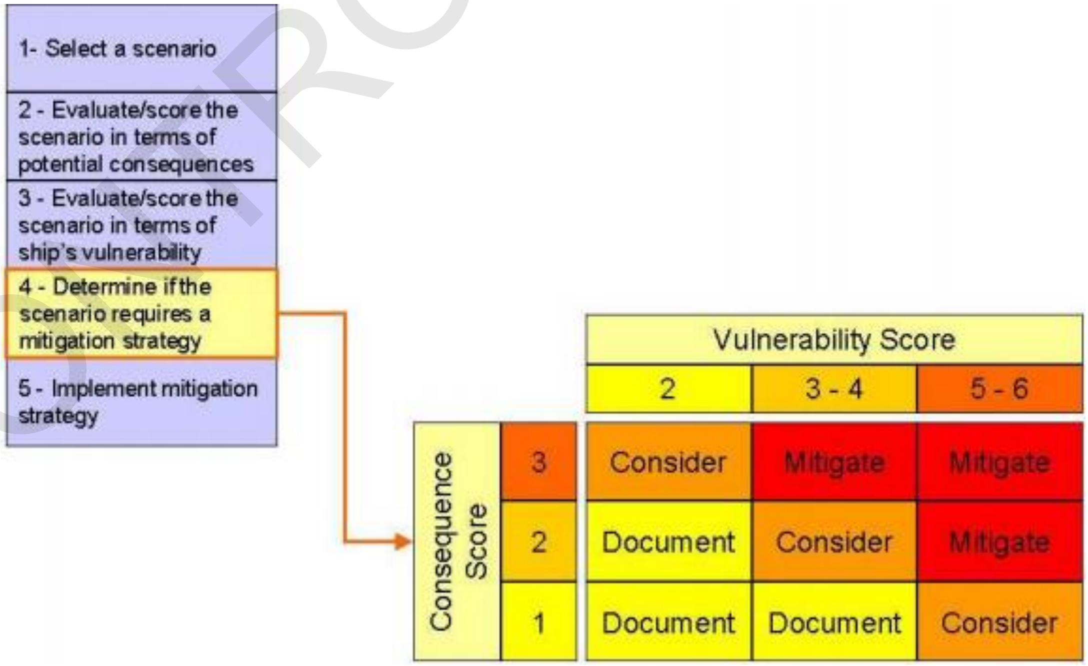
3 - Evaluate/score the scenario in terms of ship's vulnerability

4 - Determine if the scenario requires a mitigation strategy

5 - Implement mitigation strategy

Category	Accessibility	Organic Security
3	No deterrence unrestricted access to ship and unrestricted internal movement	No deterrence capability no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention
2	Good deterrence Single substantial barrier, unrestricted access to within 100 yards of the ship	Good deterrence capability Minimum security plan, some communications, armed guard force of limited size, limited detection system
1	Excellent deterrence	Excellent deterrence capability

Vulnerability score



1- Select a scenario

2 - Evaluate/score the scenario in terms of potential consequences

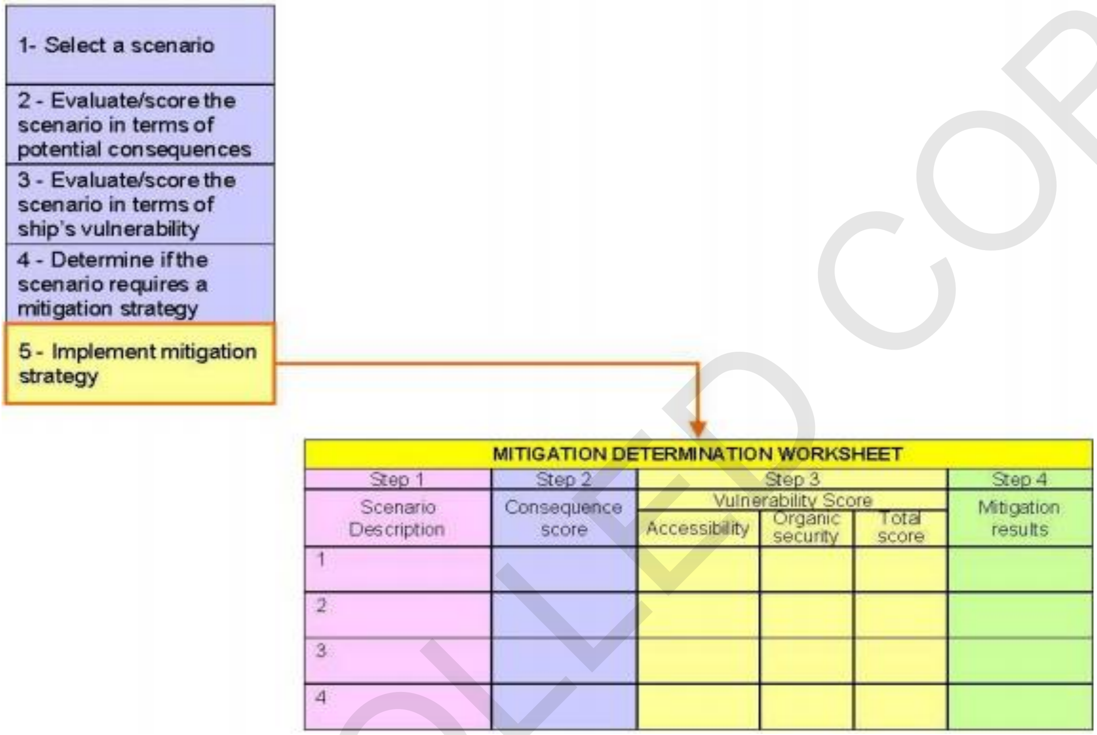
3 - Evaluate/score the scenario in terms of ship's vulnerability

4 - Determine if the scenario requires a mitigation strategy

5 - Implement mitigation strategy

		Vulnerability Score		
		2	3 - 4	5 - 6
Consequence Score	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

Scenario requiring a mitigation strategy


1- Select a scenario
2 - Evaluate/score the scenario in terms of potential consequences
3 - Evaluate/score the scenario in terms of ship's vulnerability
4 - Determine if the scenario requires a mitigation strategy
5 - Implement mitigation strategy

MITIGATION DETERMINATION WORKSHEET					
Step 1	Step 2	Step 3			Step 4
Scenario Description	Consequence score	Vulnerability Score			Mitigation results
		Accessibility	Organic security	Total score	
1					
2					
3					
4					

Mitigation determination

- ***Performance of an on-scene security survey***

The on-scene security survey is a very important part of the SSA.

Its objective is the examination and evaluation of existing shipboard protective measures, procedures and operations for:

- ✓ Ensuring the performance of all 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
- ✓ Controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel effects)
- ✓ Supervising the handling of cargo and the delivery of the ship's stores

- ✓ Ensuring that the ship security communication, information and equipment are readily available consequently, the one-scene security survey is an onboard assessment of the ship security, in order to:
- ✓ Confirm the correct implementation of existing security measures
- ✓ Identify the non-existent or insufficient security measures, with particular respect to:
  - ➢ Interference between security and safety measures
  - ➢ Interference between shipboard duties and security assignments
  - ➢ Watch keeping and manning constraints
  - ➢ Deficiencies on security equipment / items

- ***Identification of weakness in both the infrastructure and in the procedures***

This is the last step of the Ship Security Assessment.

The objective is here to identify in details which remedial actions are needed (as an example, new security measures to be implemented), based on the conclusions of both the vulnerability assessment and the on-scene security survey.

The following steps should be considered:

1. Determination of mitigation strategy (protective measures)

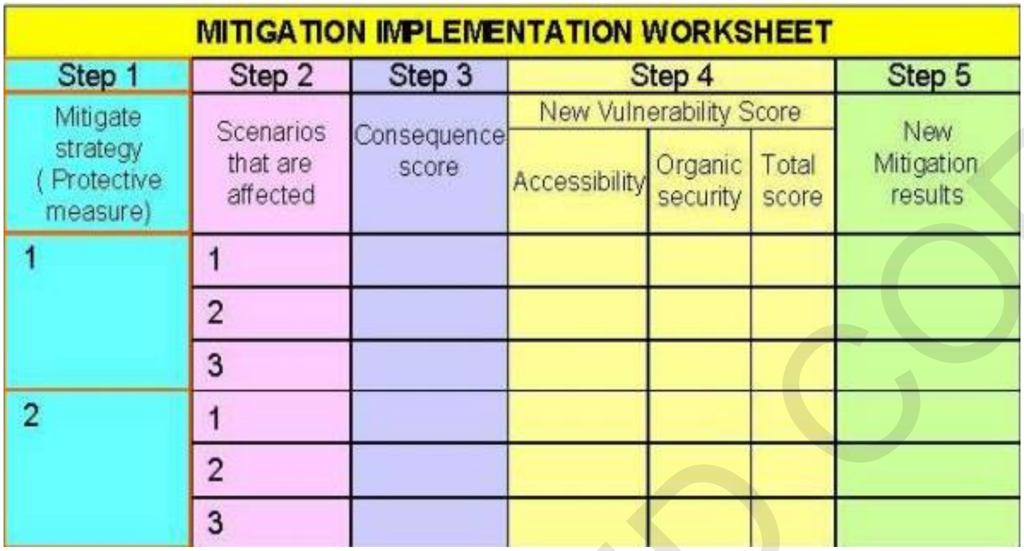
2. List of all the scenario from the previous table that would be affected by the selected protective measures

3. Refer to the same consequence score for each scenario as in table Mitigation determination.

4. Re-evaluate vulnerability score

5. With the consequence score and new vulnerability score, use table Vulnerability score to determine the new mitigation results

The results of this assessment may be reported in a table similar to Mitigation implementation, each above steps corresponding to one each column.



MITIGATION IMPLEMENTATION WORKSHEET						
Step 1	Step 2	Step 3	Step 4			Step 5
Mitigate strategy (Protective measure)	Scenarios that are affected	Consequence score	New Vulnerability Score			New Mitigation results
			Accessibility	Organic security	Total score	
1	1					
	2					
	3					
2	1					
	2					
	3					

This way of carrying out the Ship Security Assessment is a solid basis to the Ship Security Plan.

Ship Security Assessment Requirements

(a) The Vessel (Ship) Security Assessment (SSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single SSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the SSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a SSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel and vessel-to-facility interface practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

(e) The following background information must be provided to any person who conducts the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) The locations where the ship's stores and essential maintenance equipment is stored;

(vii) Changes in the tide which may have an impact on the vulnerability or security of the ship

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous SSA, if any;

(4) Emergency and stand-by equipment available to maintain essential services;

(5) Number of ship personnel and any existing security duties to which they are assigned;

(6) Training requirements and practices for personnel on board the vessel;

(7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and ship's personnel;

(8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;

(9) Existing agreements with private security companies providing waterside or vessel security services; and

(10) Existing security measures and procedures, including:

(i) Inspection and control procedures;

(ii) Identification systems;

(iii) Surveillance and monitoring equipment;

(iv) Personnel identification documents;

(v) Communication systems;

(vi) Alarms;

(vii) Lighting;

(viii) Access control systems; and

(ix) Other security systems.

(f) An on-scene survey of each vessel must be conducted. The on-scene survey is to verify or collect required information. It consists of an actual survey that examines and evaluates protective measures, procedures, and operations. (See 4/3.2)

(g) In conducting the SSA, the Company Security Officer must analyze the vessel background information and the on-scene survey, and provide recommendations for the security measures the vessel should include in the Ship Security Plan (SSP). This includes but is not limited to the following:

(1) Restricted areas;

(2) Response procedures for fire or other emergency conditions;

(3) Security supervision of ship personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.

(4) Frequency and effectiveness of security patrols;

(5) Access control systems, including identification systems;

(6) Security communication systems and procedures;

(7) Security doors, barriers, and lighting;

(8) Any security and surveillance equipment and systems;

(9) Possible security threats, including but not limited to:

(i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;

(ii) Hijacking or seizure of the vessel or of persons on board;

(iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;

(iv) Unauthorized access or use, including presence of stowaways;

(v) Smuggling dangerous substances and devices;

(vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;

(vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;

(viii) Attacks from any side while at berth or at anchor; and

(ix) Attacks while at sea; and

(10) Evaluating the potential of each identified point of access, including open weather decks that might be used to breach security.

(h) SSA report.

(1) A written SSA report must be included as part of the SSP. The SSA report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) Existing security measures, procedures, and operations;

(iii) A description of each vulnerability found during the assessment;

(iv) A description of security countermeasures that could be used to address each vulnerability;

(v) A list of the key vessel operations that are important to protect;

(vi) The likelihood of possible threats to key vessel operations; and

(vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.

(2) The SSA report must address the following elements on board or within the vessel:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility.

(3) The SSA must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Vessel personnel;

(ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;

(iii) Capacity to maintain safe navigation and emergency response;

(iv) Cargo, particularly dangerous goods or hazardous substances;

(v) Vessel stores;

(vi) Any vessel security communication and surveillance systems; and

(vii) Any other vessel security systems, if any.

(4) The SSA must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on vessel personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The SSA must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the vessel, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Supervising the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the vessel; and

(vii) The ready availability of security communications, information, and equipment.

(6) The SSA must be documented and the SSA report retained by the Company with the SSP. The SSA and SSP must be protected from unauthorized access or disclosure.

(i) The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

(j) Upon completion of the SSA, 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.

(k) If the SSA has not been carried out.

3.1 Assessment Tools

The Ship Security Assessment shall include at least the following:

An on-scene security survey.

- ✓ Identification of existing security measures, procedures and operations.
- ✓ Identification and evaluation of key shipboard operations that it is important to protect.

- ✓ Identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and priorities security measures and
- ✓ Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Each Ship Security Assessment must consider:

- ✓ Threats that may be unique for the ports at which the ship will call.
- ✓ Types of port facilities.
- ✓ Port facility security measures.

The Ship Security Assessment must address the following areas of the ship that, if damaged or used for illicit purpose, could endanger people, property; or operations on the ship or within the port facility.

- ✓ Physical Security.
- ✓ Structural Integrity of the ship and/or port facilities.
- ✓ Personnel protective systems.
- ✓ Policies and procedures.
- ✓ Communication systems, including radios and telecommunications.

The Ship Security Assessment must be reviewed, accepted or approved and retained by the Company. The completed Ship Security Assessment must include a summary report that describes how the assessment was conducted and identified the vulnerabilities that were found along with the countermeasures to be used for any vulnerability. The Ship Security Assessment will contain information that should be kept confidential. The Ship Security Assessment itself should be protected against unauthorized access and/or disclosure.

3.2 <u>On-Scene Security Surveys</u>

The "On-Scene" Security Survey should examine and evaluate the existing shipboard security protective measures, procedures, and operations for:

- ✓ Ensuring the performance of all ship security duties,
- ✓ Monitoring restricted areas to prevent unauthorized access,
- ✓ Controlling access to the ship,
- ✓ Monitoring deck areas and areas surrounding the ship,
- ✓ Controlling the embarkation/disembarkation of person and their belongings,
- ✓ Supervising cargo handling and delivery of ship stores,
- ✓ Ensuring the ready availability of ship security equipment and communication systems, and
- ✓ Handling of unaccompanied baggage.

Expert Assistance

The CSO should consider soliciting the assistance of outside experts in the following areas to prepare a complete and adequate Ship Security Assessment (SSA) by concentrating on the following issues:

- Knowledge of security threats and patterns.
- Recognizing and detecting weapons, dangerous substances and devices.
- Recognizing characteristics and behavior of persons who are likely to threaten security.
- Techniques used to circumvent security measures.
- Methods used to cause a security incident.
- Effects of explosives on ship structure and equipment.
- Ship security
- Standards practices, actions for ship and port facility
- Contingency planning, emergency preparedness and response.
- Physical security
- Radio and telecommunication, including computer equipment and networks

- Marine engineering
- Ship and port facility operations

Ship Specific Information

Prior to conducting the on-scene security survey, the following information of the ship must be collected:

- General Layout
- Location of “restricted area”
- Access points
- Tidal changes that could affect the vulnerability or security of the ship
- Cargo spaces and stowage arrangements
- Location of stores
- Location of unaccompained baggage
- Emergency and standby equipment designed to maintain essential services.
- Number of shipboard personnel along with existing security duties and training
- Existing security and safety equipment for protecting the ship personnel and passengers
- Evacuation routes and assembly station for orderly emergency abandonment of the ship
- Agreements for private security services for protecting the ship or port facilities. Existing security equipment, measures, and procedures, including cargo inspection and control procedures, surveillance and monitoring equipment, required personnel identification documents; security communication and lighting.

Points of Access

The SSA should identify and examine all points of access including open weather decks and evaluate the potential for each such point to be used by individuals for unauthorized entry.

Security Measures and Guidance

Considering existing security measures, guidance procedures and operations, the SSA should determine specific security guidance for the following:

- Restricted areas
- Emergency response procedures, including fire emergencies
- Supervision of ship personnel, passengers, visitors, vendors, repairmen and dock workers
- Frequency and effectiveness of security patrols
- Access control system, including identification requirements
- Security communication equipment and procedures
- Security doors, barriers and lighting
- Security equipment including surveillance equipment

Security threats

The SSA should consider all possible security threats that may include the following:

- Damage to the ship or port facility caused by an explosive device, arson, sabotage or vandalism
- Hijacking or seizure of the ship or of personnel or passengers
- Tampering with cargo, stores or critical ship equipment
- Unauthorized access, including stowaways
- Smuggling of weapons or the use of the ship to transport terrorists and / or their equipment
- Use of the ship itself as a weapon to cause damage or destruction
- Attacks from the sea while at berth, at anchor or at sea

Vulnerabilities

The SSA should consider vulnerabilities including:

- Conflicts between safety measures and security measures
- Conflicts between regular shipboard duties and security assignment
- Watch keeping duties, limited number of shipboard personnel and the effects of fatigue on alertness and performance
- Inadequate security training
- Inadequate or poorly maintained security equipment including communication equipment

The CSO shall ensure that persons with appropriate skills to evaluate the security of a ship carry out the SSA. The SSA in addition to the above requirements shall also include an examination of the threats to the ship, which can and do rapidly change. A ship's location, the time of the day and international events can dramatically alter the threat to a -ship. As a consequence, it is critical for the SSO to regularly monitor events to determine potential threats in the path of the ship as it travels to its next destination. Information about potential threats is available from a variety of sources. These include port authorities, local law enforcement officers, consular or diplomatic representatives. A variety of government, industry and international business organizations also provide information on potential threats. For example, governments issue warning for areas with high security risks. Internet sites are also available that compile data on piracy and other threats.

4. Security Equipment

4.1 Security Equipment and Systems

After studying this unit, you should be able to list security equipment and systems, describe threat identification methods, and explain about methods of physical searches.

Better Nose

Explosives emit distinct odors that dogs can be trained to detect. However, search dogs need to rest about every half-hour. The Department of Energy's Sandia National

Laboratories in Albuquerque, has developed an essential part of what may be aptly described as an electronic dog. The key to the handheld "sniffer" is a component known as a chemical preconcentrator. It draws in a large volume of air, collects heavy organic compounds from the air stream onto a filter and then vaporizes these compounds in the presence of an explosives detector. The unit is so sensitive, a person who had handled a bomb or a suitcase containing explosives would register as having 100,000 times more residue than a "clean" passenger, says co-developer Dave Hannum.

X-Rays

The next part of the security system that could use improvement is the passenger scanner. The current method for inspecting individual passengers is to use a metal detector, which is unable to detect nonmetallic objects such as explosives. The solution lies in weaker, not stronger, X-rays just powerful enough to look through clothes. It takes a front and back scan of a passenger in a little more than 6 seconds. Plastic explosives taped to his chest and back stand out, along with a pistol, bullets and pocket change. What is significant about the X-ray is that, while you can see the man's shin bones, which are very close to the skin, no internal organs appear on the image. This is because the subject is scanned with a narrow beam of X-rays that cannot penetrate more than a fraction of an inch into the body. Most of the rays are scattered back in the opposite direction. This energy is then gathered by sensitive X-ray detectors, and the information gleaned from these sensors is used to generate images. The amount of radiation a person receives during the 6-second scan is roughly equivalent to the radiation to which he is exposed during 20 seconds on a commercial airliner at cruising altitude.

Robots

The MR-5 has been developed as a standard to a new generation of Explosive Disposal Robots (EDR). Police, military, fire, nuclear and other hazardous response personnel can utilize the multipurpose MR-5. The MR-5 is capable of surveillance, neutralizing, and handling such items as improvised explosive devices (IEDs), hazardous chemicals, and radioactive materials. The MR-5 is an allweather, all terrain in-door and out-door mobile robot. The MR-5 features the latest robotic and computer technologies hazardous packaged into a mobile robot for hazardous environment operations The MR-5 is remotely controlled, and consists of a robust vehicle and dexterous robot arm. The six-axis manipulator arm has turret, shoulder, elbow and a three-axis wrist. Various end-effecter tools and modular equipment can be attached to the arm. The tools and modules are quick connect/ disconnect units. The MR-5 is rugged and precise; it is capable of carrying very large and very small payloads with the same gripper and same dexterity. Also, it can carry a variety of weapons, sensors and detectors, such as disrupters, lasers and mine detectors.

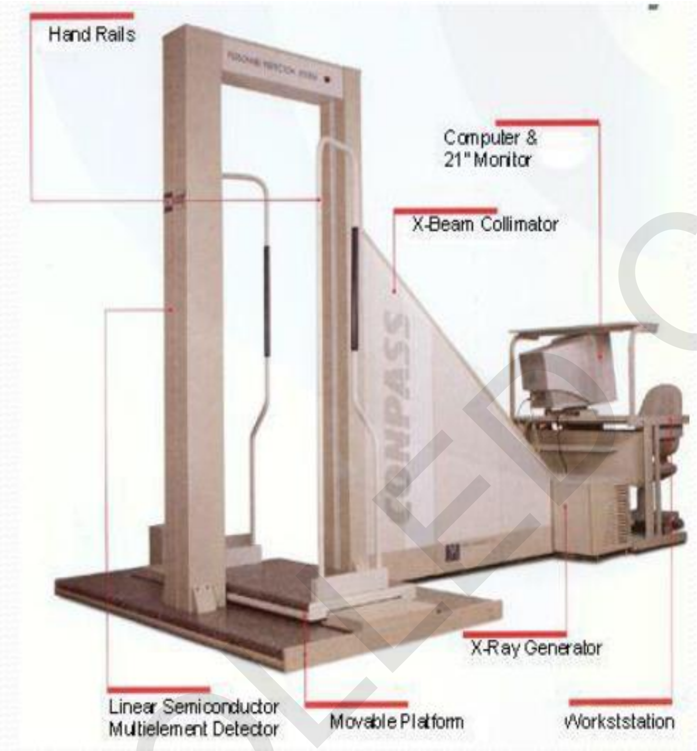
Explosion Detection Systems (EDS)

All In Vision 8 CTX EDS machines locate and identify explosive devices concealed in checked baggage. As the conveyor moves each bag through the machine, the system produces a scanned projection X-ray image. From this image, the powerful onboard computer determines which areas need "slice" images, taken by the rotating X-ray source. The CTX 9000 DSi system is the world's fastest FAA-certified Explosives Detection System (EDS) - at 542 bags per hour, it features alternate operational modes yielding even higher throughputs. Using sophisticated computer algorithms, the CTX 9000 DSi analyses these images, and compares their CT properties with those of known explosives. If a match is found, the system alarms and displays the object on the screen. The operator views the screen image to determine whether a real threat exists and then follows established protocols for threat resolution.

Explosives Trace Detection (ETDS)

IONSCAN has the capability of detecting trace amounts of more than 40 explosive or narcotic substances in a quick 8-second analysis. The color coded display presents instrument status information and results to the operator in an easy to understand fashion. If detection is made, the specific explosive or narcotic is identified on the display. The IONSCAN ® was widely deployed at Salt Lake City Airport for the 2002 Winter

Olympics. In a matter of days, over 80 systems were installed at the ticket check-in ISPS-111 counters to screen checked baggage.



Ion Track Itemiser

The Ion Track Itemiser uses Ion trap mobility spectrometry technology. Trace detection technology makes use of the minute amounts of vapors given off and the microscopic particles left behind when narcotics and explosives contraband are packaged and handled. While the analyser technology itself is quite sophisticated, it is extremely simple to use. Most importantly, it is fast, accurate and sensitive. Just how sensitive'? Billionths of a gram or the concentration equivalent of dissolving a single packet of sugar in 100 Olympic size swimming pools! Collecting samples for analysis could not be simpler. In the case of trace particle detection, the surfaces of a vehicle or luggage that are suspected of bring tainted with contraband are wiped down with a paper disk known as a sample trap. The trap is then inserted into the desktop analyzer. Once analyzed, the contraband substance is identified, along with its relative alarm strength. Visual and audible indications are provided,and the analysis can be stored and printed for use as court accepted evidence.In the case of vapor detection, the portable, handheld analyzer "sniffs" the air around the openings of closed compartments, containers or packages suspected of concealing contraband. The analyzer then identifies the contraband substance and its relative alarm strength. Again, as with the particle analyzer, both visual and audible indications are provided, and the analysis can be stored and later printed for use as court-accepted evidence.

Biometrics

Biometrics measure an individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characters include signature, voice, keystroke pattern, and gait. Of all these biometrics, technologies for fingerprint and hand are the most developed.

Something you are — BIOMETRIC
Something you have — a smart card or token like
Something you know — password, PIN or personal info
(Such as your wife's birthday)

Of all the above, a biometric is the most secure and convenient authentication tool. It cannot be borrowed, stolen or forgotten, and forging one is practically impossible. Biometrics can be integrated into any application that requires security, access control and identification or verification of people. BioEnable products are based on finger print recognition technology which is very secure, most non-intrusive and widely accepted the world over.

Fingerprint Recognition

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching pattern;

others use straight minutiae matching devices; and still others area bit more unique, including things like more fringe patterns and ultrasonics. A greater variety of fingerprint devices is available than for any other biometrics. Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the work-station access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices. Bio Enable fingerprint recognition is based on minutiae matching and intelligent scanners that can detect when a live finger is presented. How does it work? Fingerprint systems translate illuminated images of fingerprints into digital code for further software such as enrollment

(Fingerprint registration) and verification (authentication of registered users). BioEnable devices use the advanced SEIR method and CMOS image sensor to capture high contrast, high resolution fingerprint images that are virtually distortion-free. A series of powerful algorithms developed by BioEnable extract minutiae data from the image, mapping the distinguishing characteristics of fingerprint ridge stored in database. The actual fingerprint image is never stored, and cannot be constructed from templates. To identify or verify a fingerprint, a proprietary matching algorithm compares the new template made from the extracted minutiae points from the input fingerprint on the optical module to a previously stored sample. The entire matching process takes roughly one second. Authentication takes place either locally or on a server, depending on system configuration.

Finger Print

However, an extensive database identification system may be largely unnecessary as humans carry a built-in identity card, in the pattern of their iris. What's more, the eye can be scanned passively, from a distance of a few feet away. In late October, Indian Technologies of Moorestown, New Jersey, and John Enschede Security Solutions of Haarlem, Netherlands installed an automated iris recognition border-crossing system at Amsterdam's School

Airport. During the trial period, passengers who were nationals of the European Economic Cooperation nations could enroll in the iris-recognition system. The system measures 247 independent variables for each iris and stores this information on a so-called smart card. The variability in iris patterns is so great that it is even different between identical twins. The chances of two persons having the same iris code are *as low as I in 7 billion.* One plan being considered would require iris-matched ID cards for all visitors to the United States. One of the most attractive features for immigration officials is that it would then take less than 2 seconds to verify each person's identity.

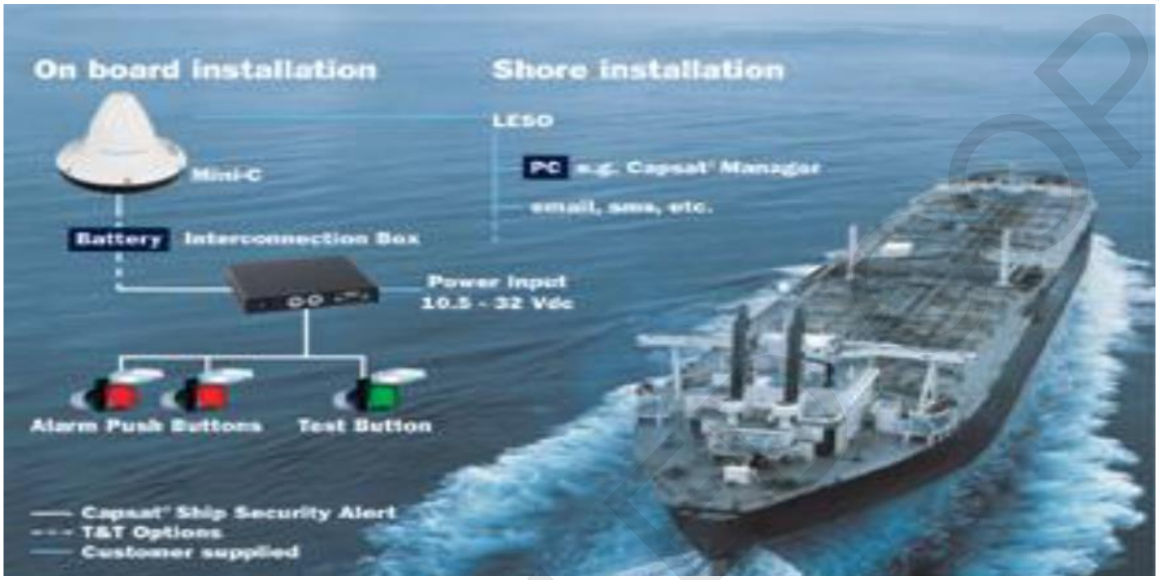
Who's Who

When it comes to spotting and stopping *known* terrorists, the two most widely used tools – video cameras and photo identity cards – have proved to be technological dead ends. Tests of face ID systems have thus far been disappointing. In Britain, which was at the vanguard of the security camera movement, independent studies have shown that while cameras are useful for gathering evidence to prosecute crimes, they have done little if anything to prevent crime. More sophisticated safeguards on driver's licenses also have proved ineffective. California recently suffered national embarrassment as the result of its attempts to introduce more secure driver's licenses. A network television investigative reporting team revealed that added security measures, including holograms and online verification of Social Security numbers, failed to stop fraud by corrupt state workers and only increased the price for illegal licenses, from $ 1500 to $ 2300.

Equipment Prescribed by SOLAS 74

Ships Security Alert System

Each ship must be fitted with a Ship Security Alert System, or "silent alarm", which when activated will transmit a ship-to-shore security alert that identifies the ship. The ship's location, and indicates that the ship is under threat or has had a breach of a security. Transmissions from the Ship Security Alert System must not alert any other ship or sound any alarm on the ship. Further it must continue until reset. The Ship Security Alert System must be designed to be activated from the navigational bridge and from one other place on the ship.



Automatic Identification System (AIS)

The AIS was conceived as an electronic aid to navigation – specifically collision avoidance. This equipment, along with VDR (Voyage Data Recorder), was made mandatory for various ship types in a phased manner through Chapter V (Safety of Navigation) in SOLAS 74 – the final cut-off date being 1 July 2008. With the implementation of ISPS Code, however, the fitment schedule of AIS has been accelerated and the equipment itself has been converted into a security/surveillance equipment for implementation of the ISPS. In its present configuration, the effective range of this equipment is 50 to 70 nautical miles (i.e. VHF range). Moves are, however, afoot by the US to increase the range to 2000 nautical miles using satellite and HF communications equipment so that ships may be identified and tracked well before they hit US shores under a scheme called Long-range Identification and Tracking (LRIT). The purpose of AIS is to ensure automatic transmission of ship's identity, position and other relevant data.

Other Security Equipment

During the Ship Security Assessment, the Company Security Officer and Ship Security Officer must evaluate the need for other appropriate security equipment that may be used to protect the security of the ship, e.g. closed circuit cameras may be used for surveillance (when personnel are available to monitor the cameras) or metal detectors and/or x-ray equipment may be appropriate for screening passengers and their belongings. The Ship Security Plan must identify all the ship security equipment and establish procedures for inspecting, testing, and maintaining all security equipment in accordance with the equipment manufacturer's instructions.

Testing, calibration and maintenance of ***Security Equipment and Systems***

It is the duty of the Ship Security Officer to ensure that all the security equipment is in a perfect working order at all times. In this task, he is to be assisted by the Ship's Master and the Company.

5. Threat Identification, Recognition and Response

5.1 Recognition and Detection of Weapons, Dangerous Substance and Devices

Recognition and Detection of Weapons, Dangerous Substances and Devices In order to pre-empt and prevent a terrorist action on board, it is imperative that the terrorist is prevented from bringing his instruments of destruction on board. Further, it is likely that the terrorist will try to smuggle his weapons in parts and these parts at first look would look like machinery spare parts or tools for carrying out repairs on board. It is therefore important that personnel on board have at least a basic knowledge of these instruments and how they look like. The AK-47 has been one of the most popular arms of the terrorist. If this is smuggled on board in parts, it is unlikely that a member of the crew will be able to recognize it.

Explosives

Any explosive material has the following characteristics

(a) It is chemically or otherwise energetically unstable.

(b) The initiation produces a sudden expansion of the material accompanied by large changes in pressure (and typically also a flash or loud noise), which is called the explosion. Given below are details of chemical explosives. There are many other varieties of more exotic explosive material, such as nuclear explosives and antimatter, and other methods of producing explosions such as abrupt heating with a high intensity laser or electrical arc.

Classifications

Explosives are classified by their sensitivity which is the amount of energy to initiate the reaction. This energy can be anything, from a shock, an impact, a friction, an electrical discharge, or the detonation of another explosive. High explosives will explode without confinement, are compounds, initiated by shock or heat, supersonic reaction or high brisance (brisance means the shattering effect of an explosion).

Primary Explosives

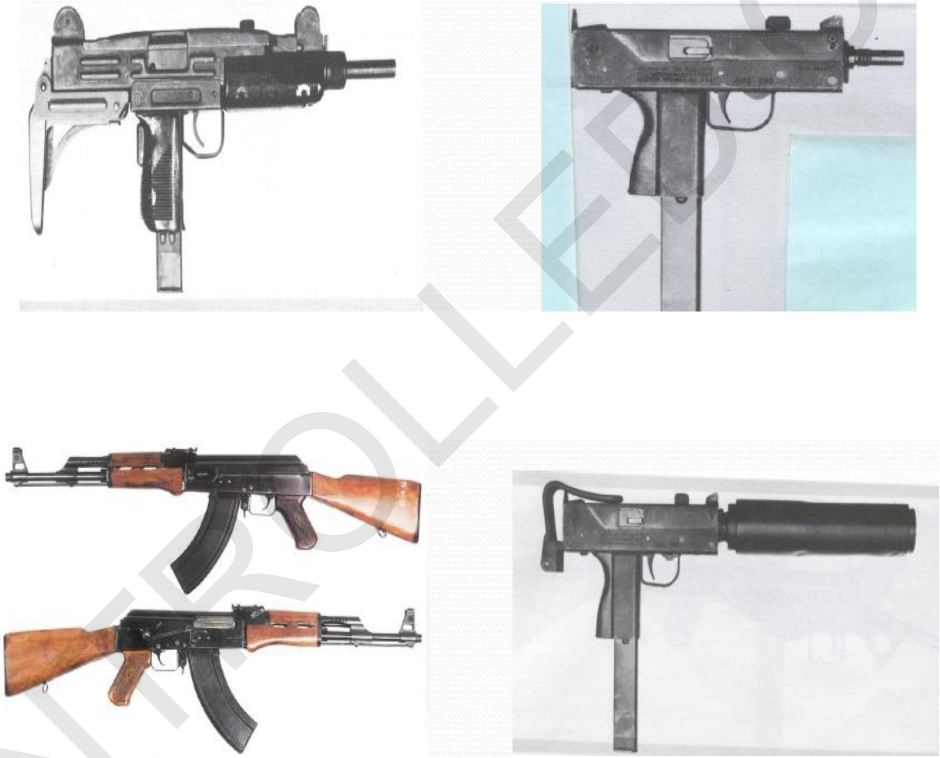
They are extremely sensitive and require a small quantity of energy to be initiated. They are mainly used in detonators to initiate secondary explosives. (Examples: Tetryl, Lead azide, Mercury fulminate, lead styphnate, tetrazene, hexanittomannitol.)

Secondary Explosives

They are relatively intensive and need a great amount of energy to initiate decomposition. They have much more power than primary explosive and are used in demolition. They require a detonator to explode. (Examples: Dynamite, TNT, RDX, PETN, HMX, ammonium nitrate, tetryl, picric acid nitrocellulose.)

Detonation

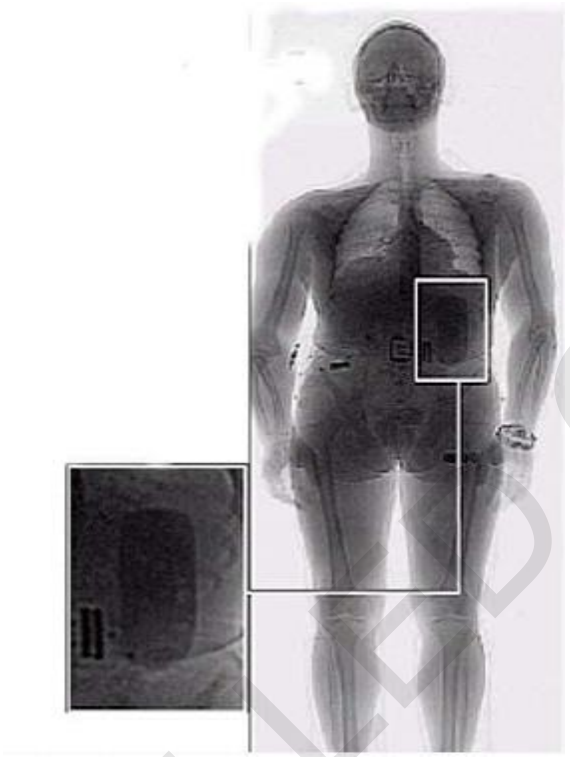
Also called an initiation sequence or a firing train, this is the sequence of events which cascade from relatively low levels of energy to cause a chain reaction to initiate the final explosive material or main charge. They can be either low or high explosive trains. Low explosive trains are something like a bullet – Primer and a propellant charge. High explosives trains can be more complex, either Two-step (e.g. Detonator and Dynamite) or Three-Step (e.g. Detonator, Booster and ANFO). Detonators are often made from tetryl.



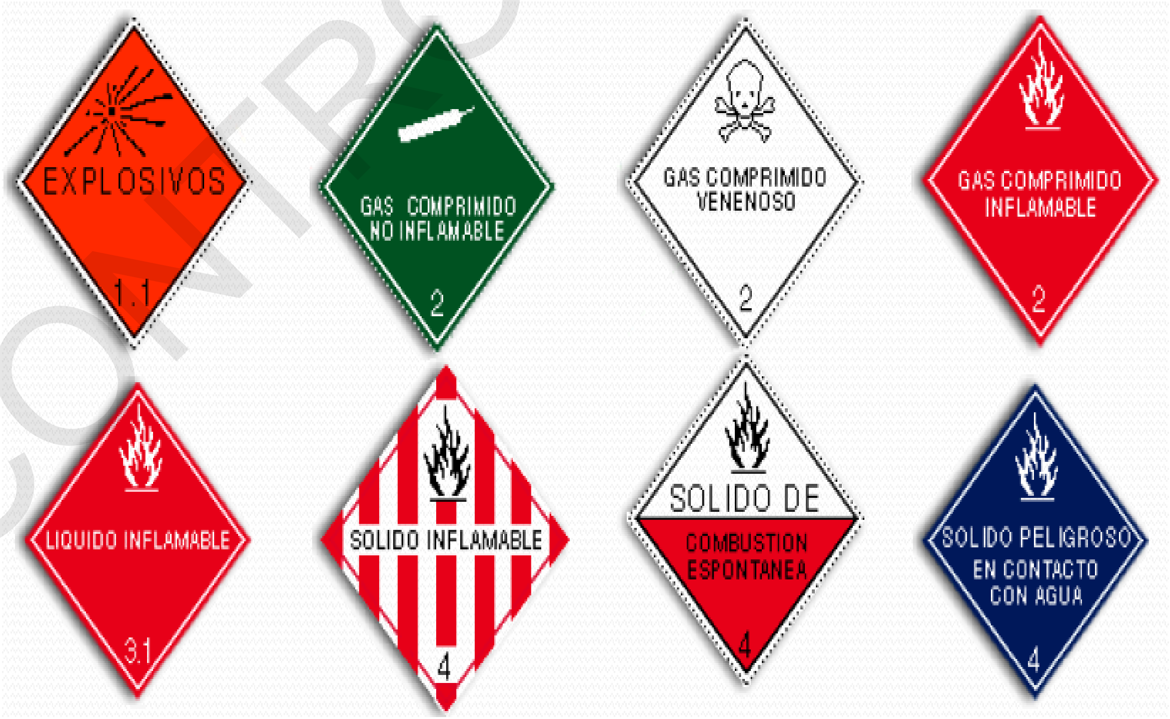
Prohibited Weapons

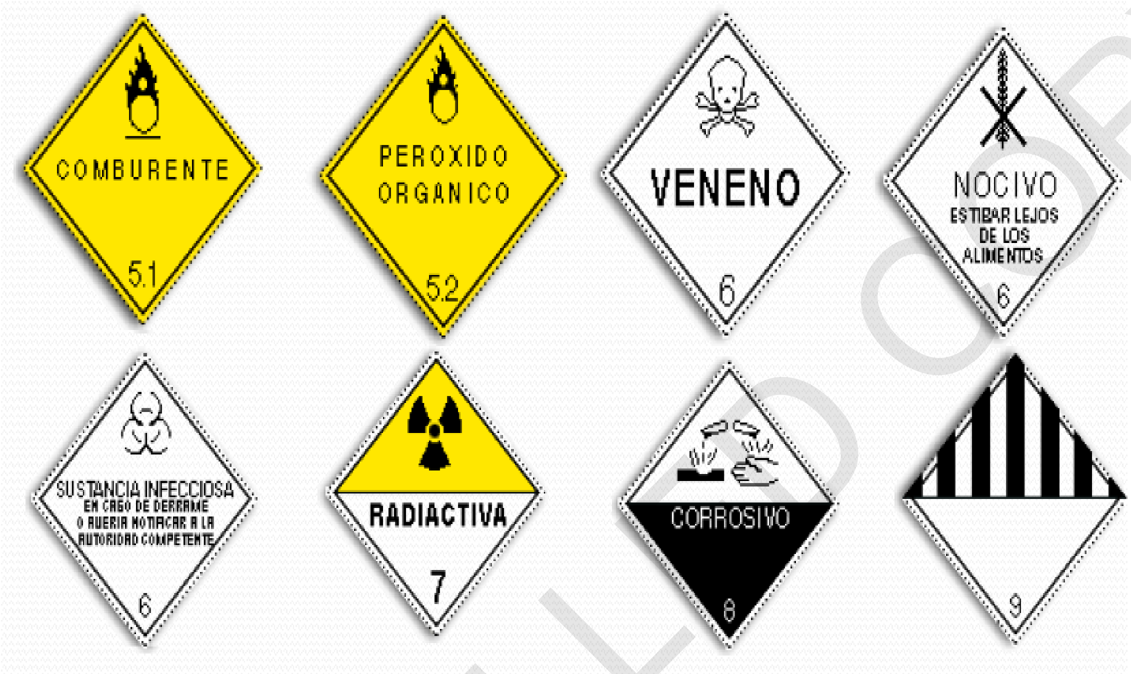
Prohibited Weapons Improvised or Concealed

Explosives: Dynamite and C-4



"Mules" with Explosives on the Body


EXPLOSIVOS
1.1
GAS COMPRIMIDO NO INFLAMABLE
2
GAS COMPRIMIDO VENENOSO
2
GAS COMPRIMIDO INFLAMABLE
2
LIQUIDO INFLAMABLE
3.1
SOLIDO INFLAMABLE
4
SOLIDO DE COMBUSTION ESPONTANEA
4
SOLIDO PELIGROSO EN CONTACTO CON AGUA
4


COMBURENTE
5.1
PEROXIDO ORGANICO
5.2
VENENO
6
NOCIVO
ESTIBAR LEJOS DE LOS ALIMENTOS
6
SUSTANCIA INFECCIOSA
EN CASO DE DERRAME O AVERIA NOTIFICAR A LA AUTORIDAD COMPETENTE
6
RADIACTIVA
7
CORROSIVO
8
9

Classification of Hazardous Materials

Revolvers and Pistols

Modified Shotguns

Rifles

5.2 Methods of Physical Searches and Non-Intrusive Inspections

Before we examine the method s of physical searches and non- intrusive inspections, it is important to understand, what it is that we are looking for. The ship security may primarily be threatened either by an individual or a self-activating device planted on or in the vicinity of the ship. For the latter, a coordinated search will have to be carried out. The weapons and explosives could also be hidden in the cargo containers. The threat from an individual could be either from the ship's crew or a passenger. As far as the crew is concerned, he is less of a threat than a passenger, because his credentials unlike a passenger would have been checked before his appointment on board the ship. Besides when the crew embarks the ship for the first time there is plenty of time to search him to ensure that he is not carrying any unauthorized materials with which he could threaten the ship security. The problem therefore primarily arises in passenger ships/ ferries where a large number of individuals enter, at times with their vehicles, in a short span of time.

Metal Detection

The most usual way of using metal detection is to process passengers and staff through an archway which is preset to alarm if a certain amount of metal is carried on the person. Hand-held metal detectors may also be used for screening individual passengers and members of staff especially those few who object h) physical search on religious or other grounds. Irrespective of which equipment used it is essential to remember that metal detectors will not pick up explosive plastic weapons or inflammable liquids carried in glass or plastic containers on the person. For this reason, metal detection alone is insufficient and *must* always be accompanied by a physical search of a proportion of those being Screened. Including some who do not alarm the detector. This combination increases the chances of detection and acts as a powerful deterrent.

Detectors Manuals Metals **Fixed Detectors Metals**

Baggage Screening

The baggage can be divided into two types, Bags hand-carried by passengers and heavy baggage for cruise liner passengers. The smuggling of weapons and the planting of IED in baggage are methods well favoured by terrorists, and bombs have been planted in several vessels this way. Methods of screening both groups of baggage include metal detectors, vapour detection probes and sytems, X-ray systems, physical search and dogs.

Baggage Inspection Equipment

Vapour Detection

Air sampling system either static or hand-held can be used to detect some explosives. However, currently no commercial system is capable of detecting all forms of explosives. They can, however, be used to supplement other systems such as X-Ray.

X-ray Systems

The most usual method of screening baggage and personal belongings is to use X-ray equipment and modern equipment are capable of producing images of good definition and penetration. However, X-ray examination can also be defeated, e.g. X-rays may not detect explosives 'and plastic weapons nor will they allow identification of the actual liquid in bottles or other containers. Moreover, it is possible to camouflage the image of weapons and devices by the use of other dense materials, such as lead crystal glass. The use of X-ray equipment must, therefore, also be accompanied by a percentage physical check of baggage including a proportion that does not arouse suspicion. The use of X-rays is a very effective method of screening bags and other items provided certain conditions are met, e.g. operator efficiency decreases significantly after only a relative short time, particularly at peak screening periods. For this reason, operators should only scan X-ray images for a maximum of 20 minutes and then be employed on other duties, such as a physical search, for 40 minutes before returning to the console. It is also essential that the image is presented for an adequate time to permit proper examination and a minimum of 5 seconds is considered necessary for this. Screening techniques will vary depending upon whether the equipment presents a fixed or scrolling (moving) image.

Physical Search

To be properly effective, physical search of bags and belongings should include a check for false compartments, often used for the smuggling of weapons and devices. Although false 'bottoms' are most usual, devices have been incorporated around the sides of cases, in the lids and in the compartments of hold ails. Very often, a smell of glue or a heavy odour to mask the smell of explosives is an indication that a lining may have been removed, a substance, such as explosive, placed behind it and the lining stuck back in position. Attention should be paid to any tampering or repair to a case, non-standard or unmatched case components, and also to greasy stains or small holes in the case exterior. The contents of bags should be assessed during search and if the weight seems disproportionate or the bag is unbalanced for no obvious reason, then a further check for a false compartment would be justified. Particular attention should be paid to electrical and electronic apparatus, such as radios, which have often been used as containers for devices to avoid detection under X-ray examination. Passengers should be questioned on the origins of the equipment and whether it has been out of their possession for any period of time. Equipment may be examined for unusual characteristics: signs of tampering, excessive weight, loose objects inside (rotate, not shake).

X-ray the equipment if suspicions are aroused. Treat all new, packaged equipment in the same manner as used models. Other containers carried in bags, which could be used to conceal weapons must also be examined. Normally this can be done visually but gift-wrapped parcels, birthday cakes, etc., can be screened by metal detectors or X-ray.

Use of Dogs

Specially trained dogs can be very effective in searching cars, baggage and freight. However, they should normally not be used near groups of passengers as they tend to alarm people who are sometimes put off by them. Dogs can also be used for searching in ships. However, they need to be familiar with the seagoing environment to achieve results. In fact to have their 'sea legs'.

Heavy Baggage

The screening of heavy baggage is normally done by central X-ray machine supported by physical search. Air sampling probes can be use in the checking of heavy baggage and it is an area where the use of dogs trained to sniff out explosives may well be beneficial. Like passenger screening; once heavy baggage has been screened it is essential it should be marked and kept under surveillance until onboard the ship.

Explosives

Explosions are highly exothermic chemical reactions that produce expanding gases and were first made by Asian alchemists more than one thousand years ago when they discovered that by making a mixture of saltpeter (KNO,) and sulphur, it could be detonated. Explosives are classified as Primary (Initiators)

That does not bum but detonate if ignited (mercury fulminate).

Trinitrotoluene (TNT)

Trinitrotoluene is a high explosive that is unaffected by ordinary shocks and, therefore, must be set off by a detonator. TNT is often mixed with other explosives such as ammonium nitrate to form amatol. Because it is insensitive to shock and must be exploded with a detonator, it is the most favored explosive used in ammunitions and construction.

Why Do Nitro Groups (NO,) Lead to Unstable Compounds?

Nitrogen has charge of + 1 and nitro group have a strong tendency to withdraw (pull) electrons from other parts of the compound. Attaching three nitro groups to a compound leads to an extremely unstable situation.

5.3 Recognition, on a Non-Discriminatory Basis, of Persons Posing Potential Security Risks

- ✓ Strangers taking pictures of the ship or the port facility;
- ✓ Strangers who try to access the ship or the port facility;
- ✓ Individuals establishing businesses or sell food off the street, in places adjacent to or in the vicinity of the port facility.
- ✓ Strangers wandering long period near the ship or the port facility areas;
- ✓ Strangers call inquiring about security, staff and procedures for normal operation of the facility;

- ✓ Vehicles with people inside, wandering around and taking photos or perhaps making a diagram of the ship or the port facility;
- ✓ Small boats with people on board and maybe taking pictures and making diagrams of the ship or the port facility;
- ✓ General Aircraft flying in the vicinity of the ship or the port facility;
- ✓ Persons with abnormal behavior loading objects that could be bombs;
- ✓ Strangers trying to get personnel or their families, information on the ship or the port facility;
- ✓ Street vendors;
- ✓ Workers who try to access port facilities to repair, replace, or install equipment to service;
- ✓ Electronic messages (e-mails) to seek information about the port facility personnel or operating procedures;
- ✓ Stop trying to leave packages or packages;
- ✓ Expressions or anti-nationalist sentiments of the employees or vendors;
- ✓ Anti-nationalist pamphlets or flyers distributed to employees or placed on the windshields of cars in parking lots;
- ✓ Phone calls out of the ordinary;
- ✓ Pleasure boats or persons on board a refugee boat, pretending to have an emergency to attract support from other vessels;

5.4 Techniques Used to Circumvent Security Measures

- ✓ Disable the alarm system components;
- ✓ Use lock picks to open locks or locks, duplicate keys;
- ✓ Disable CCTV camera;
- ✓ Block radio signals.

5.5 Crowd Management and Control Techniques

It is the ability to manage smart and disciplined an emergency situation involves a practical skill, in which the training is the determining factor for its realization.

Objective

The main objective is to optimize the chances of survival of the passengers, the crew and staff of the port facility. This objective is to keep everyone's mind that despite the adverse situation is possible to survive.

Tendency to React in Adverse Situations

- ✓Actively: 10-30%
- ✓Passively: 50 - 75%
- ✓Frightened: 1-3%
- ✓The tendency to react too late in emergencies should:
  - To believe that the danger is not immediate;
  - Want more information on the situation; and
  - Recognizing the danger, but be optimistic about getting out of the situation.

Typical Reactions

- ✓Active people face the situation and in many cases are not aware of how to do it that way, they can choose solutions that cause more damage;
- ✓Some people choose to follow passive to active, and others still waiting for help; and
- ✓The fearful can enter an emotional state of extreme panic.

Possible Scenarios

- ✓Fire in the port facility or ship;
- ✓Stranding of the ship;
- ✓Collision in harbor areas or at sea for interfaces;
- ✓Terrorist attacks;

✓Pumps for the port facility or ship; etc.

Considerations for Crowd Control

By taking charge, we must take the following considerations:

✓**Location:** explain the current situation to the passengers; crew, staff and visitors, without unnecessary detail.

✓**Task or mission:** to explain what to do.

✓**Execution:** explain how to do it and give clear orders.

✓**Administration:** procedures exist for this situation? What support is available from the emergency? Act according to the lists and procedures in emergencies.

✓**Leadership and communication:** who is responsible? Of all these, one must deal with the situation, others should support him. How should communicate with the crew and how to organize the emergency.

6. Ship Security Actions

6.1 Actions Required by Different Security Levels

Recognizing that vigilance must increase as the threat of a security incident increases, the ISPS Code establishes three different security levels that call that call for tighter protective measures when there are more likely or specific threats.

Security Level I

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

Security Level 2

Security Level 2 is used when there is a heightened threat of an attack occurring in a specific area against a specific class of targets, thus necessitating maintenance of additional protective security measures for a period of time.

Security Level 3

It 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.

The Ship Security Plan must specify the security protective measures to be taken on each ship at each security level for the following activities

- ✓Ordinary security activities.
- ✓Controlling Access to the ship.
- ✓Controlling the embarkation of persons and their belongings.
- ✓Monitoring restricted areas to prevent unauthorized access.
- ✓Monitoring deck areas and areas around the ship.
- ✓Supervising cargo and store handling.

Actions to be taken at Various Security

- ✓The actions to be taken at various security levels are summarized in the following tabulated boxes.

Access to the Ship

Action	**Level 1**	**Level 2**	**Level 3**
All access points manned	**Yes**	**Yes**	**Yes**
Electronic information protected	**Yes**	**Yes**	**Yes**
Verification of identification	**Yes**	**Yes**	**Yes**
Lock off areas not in use	**Yes**	**Yes**	**Yes**

Additional guards at access points	**Optional**	**Yes**	**Yes**
Inspection of carry-on baggage	**Yes**	**Yes**	**Yes**
Search of vehicles on ferries	**Yes**	**Yes**	**Yes**
Segregate searched from un searched	**Yes**	**Yes**	**Yes**
Consider use of boat patrols	**Optional**	**Optional**	**Optional**
Provide specific security briefings	**Optional**	**Yes**	**Yes**
Limited access to a singles point	**Optional**	**Optional**	**Yes**
Suspension of embarkation — disembarkation	**No**	**No**	**Yes**

Restricted Areas

Action	**Level 1**	**Level 2**	**Level 3**
Secure area when not in use	**Yes**	**Yes**	**Yes**
Use Closed Circuit Television (CCTV) and other surveillance equipment	**Yes**	**Yes**	**Yes**
Consider using ships personnel as security staff	**Yes**	**Yes**	**Yes**
Consider using automatic intrusion	**Yes**	**Yes**	**Yes**

detection			
Close off areas adjacent to restricted areas	**Optional**	**Yes**	**Yes**
Consider deploying additional detection devices in areas adjacent to restricted areas	**Optional**	**Yes**	**Yes**
Must have the ability to respond to a breach of a restricted area	**Yes**	**Yes**	**Yes**

Embarkation of Persons and their Effects

Action	**Level 1**	**Level 2**	**Level 3**
Sterile area to carry out checks	**Yes**	**Yes**	**Yes**
Segregation between checked and unchecked	**Yes**	**Yes**	**Yes**
Positively identifying passengers, visitors and others before all	**Optional**	**Yes**	**Yes**

embarkations			
Security briefings for all crew and passengers	**Optional**	**Yes**	**Yes**
Set search level % to reflect the threat	**Yes**	**Yes**	**Yes**
Ensure searchers are well trained and know what to look for	**Yes**	**Yes**	**Yes**
Procedures in place to deal with any prohibited items found	**Yes**	**Yes**	**Yes**
Restrict access to crew and passengers only	**Optional**	**Optional**	**Yes**
Provide escorts for service providers	**Optional**	**Optional**	**Yes**

Handling Unaccompanied Baggage

Action	**Level 1**	**Level 2**	**Level 3**
Ensure stores match the order before being loaded	**Yes**	**Yes**	**Yes**
Ensure immediate stowage of all ships stores	**Yes**	**Yes**	**Yes**
Checks prior to accepting stores on board	**Optional**	**Yes**	**Yes**
Work with Port Facility to subject stores to more	**Optional**	**Optional**	**Yes**

rigorous checks			
Subjecting ships stores to more extensive checking using resources available	**Optional**	**Optional**	**Yes**
Restrict the delivery of or refuse to accept ships stores	**Optional**	**Optional**	**Yes**
Routine checking of cargo transport units and spaces	**Yes**	**Yes**	**Yes**
Routine checking of cargo	**Yes**	**Yes**	**Yes**
Check that cargo loaded matches documentation	**Yes**	**Yes**	**Yes**
In liaison with Port Facility, ensure vehicle(s) searched in accordance with current security level and SSP	**Yes**	**Yes**	**Yes**
Checking of seals or other methods to prevent tampering	**Yes**	**Yes**	**Yes**
Visual and physical examination	**Yes**	**Yes**	**Yes**
Use of detection equipment where available	**Yes**	**Yes**	**Yes**
Use accredited shippers where possible	**Yes**	**Yes**	**Yes**
Detailed checking	**Optional**	**Yes**	**Yes**

of cargo transport units and spaces			
Intensified checks to ensure only intended cargo is loaded	**Optional**	**Yes**	**Yes**
Increase search of cargo in accordance with security	**Yes**	**Yes**	**Yes**
Intensifies searching of vehicles to be loaded	**Optional**	**Yes**	**Yes**
Increased frequency and detailed checks of seals	**Optional**	**Yes**	**Yes**
Suspensions of the loading or unloading of cargo	**Optional**	**Optional**	**Optional**
Verify inventory of dangerous goods and hazardous substances	**Optional**	**Optional**	**Yes**

Monitoring the Security of the Ship

Action	**Level 1**	**Level 2**	**Level 3**
Deck and access points illuminated at all times whilst in port or at anchorage	**Yes**	**Yes**	**Yes**
Maximum lighting whilst underway consistent with safe navigation	**Yes**	**Yes**	**Yes**
Ships personnel should be able to detect activities	**Yes**	**Yes**	**Yes**

beyond the ship on both shore side and waterside			
Coverage should facilitate identification at access points	**Yes**	**Yes**	**Yes**
Assign additional personnel as lookouts and patrols	**Optional**	**Yes**	**Yes**
Install additional lighting in conjunction with port facility	**Optional**	**Yes**	**Yes**
Ensure coordination with waterside and shore side patrols when provided	**Optional**	**Yes**	**Yes**
Use all devices capable of recording on board activities	**Optional**	**Optional**	**Yes**
Slow rotation of propellers to deter underwater access	**Optional**	**Optional**	**Yes**
Have the ability to respond to incidents	**Yes**	**Yes**	**Yes**

6.2 Maintaining Security of the Ship/Port Interface

Ship-Port Interface

Interactions that occur when a ship is affected by actions involving the movement of people, goods and provisions of port services to or from this ship.

Actions Required by Different Levels of Protection, Including Ship-Port Interface

Access Control Ship

Applicable safeguards should be included in:

- ✓Access stairs;
- ✓Planks landing;
- ✓Access ramps;
- ✓Access doors, side scuttles, windows and ports;
- ✓Mooring lines and anchor chains; and
- ✓Cranes and hoisting gear.
- ✓Check the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example: shipping instructions, the passenger tickets, boarding passes, work orders, etc.
- ✓In liaison with the port facility the ship should ensure that designated secure areas in which inspections and searching of persons, baggage (including carry), personal effects and vehicles can be made and its contents are designated;
- ✓In collaboration with the port facility the ship should ensure that register with the frequency required in the SSP, the vehicles to be loaded on ships for transport of cars, ships and other Ro-Ro passenger ships prior to shipment;
- ✓Separate people and personal effects have passed security checks of persons and personal effects that have not yet been subjected to them;
- ✓Separating passengers embarking from those disembarking;
- ✓Identify access points that must be secured or attended to prevent unauthorized access;
- ✓Securing, by locking or other means, access to unattended spaces adjacent to areas that are accessible to passengers and visitors; and
- ✓Inform all ship personnel on security aspects, such as possible threats, the procedures for reporting suspicious persons or suspicious objects and activities, and the need for vigilance.

Protection Level 2 Access Control

Establish measures to protect against a high risk that an event affecting maritime security through increased vigilance and tighter controls, and can be, among others, the following occurs:

- ✓Allocate more personnel to patrol deck areas during silent hours to prevent unauthorized access;
- ✓Limit the number of access points to the ship, identifying those to be closed and the means of adequately;
- ✓Deterring waterside access to the ship by the side that faces the sea, for example, boat patrols in liaison with the port facility;
- ✓Establishing a restricted area on the side of the ship which may be implemented in close collaboration with the port facility;
- ✓Increase the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;
- ✓Escorting visitors on the ship;
- ✓Inform all ship personnel on issues more specific security threats detected, emphasizing the procedures for reporting people, suspicious objects, suspicious activity, and highlight the need for vigilance; and
- ✓Perform a full or partial search of the ship.

Protection Level 3 Access Control

- ✓At level 3, the ship should comply with the instructions issued by those responding to the security incident affecting the security or to the threat thereof. The SSP should detail the security measures which can be taken by the ship, in close cooperation with those responding to the security incident and the port facility, which may be, among others, the following:
- ✓Limiting access to a single controlled point;
- ✓Allow access only to those responding to cope with the security incident or threat thereof;
- ✓Instruct people on board;

- ✓Suspending loading or unloading;
- ✓Suspend operations, cargo handling, delivery, etc.
- ✓Evacuation of the ship;
- ✓Movement of the ship; and
- ✓Preparing for a full or partial search of the ship

6.3 Familiarity with the Declaration of Security

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

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

6.4 Reporting Security Incidents

Incident Protection

Any act or circumstance that raises suspicion, that poses a threat to the security of a ship, including mobile offshore drilling units and high-speed craft, a port facility, a ship-port interface or ship to ship.

All security incidents must be reported in accordance with specific reporting requirements.

6.5 Execution of Security Procedures

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

7. Emergency Preparedness, Drills and Exercises

Training and Drills

1. The Company Security Officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in Part B of the ISPS Code.

2. The Ship Security Officer shall have knowledge and have received training, taking into account the guidance given in Part B of the ISPS Code

3. Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the Ship Security

Plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part B of the ISPS Code.

4. To ensure the effective implementation of the Ship Security Plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other.

Security Training for All Vessel Personnel

All vessel personnel, including contractors, whether part-time, fulltime, temporary, or permanent, must have knowledge of, through training or equivalent job experience, the following:

(a) Relevant provisions of the Ship Security Plan;

(b) The meaning and the consequential requirements of the different Security Levels, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

Drill and Exercise Requirements

(a) ***General*** – Drills and exercises must test the proficiency of vessel personnel in assigned security duties at all Security Levels and the effective implementation of the Ship Security Plan (SSP). They must enable the Ship Security Officer (SSO) to identify any related security deficiencies that need to be addressed.

(b) ***Drills***

(1) The SSO must ensure that at least one security drill is conducted at least every 3 months, except when a vessel is out of service due to repairs or seasonal suspension of operation, provided that in such cases a drill must be conducted within one week of the vessel’s reactivation. Security drills may be held in conjunction with non-security drills where appropriate.

(2) Drills must test individual elements of the SSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility’s scheduled drill.

(4) Drills must be conducted within one week whenever the percentage of vessel personnel with no prior participation in a vessel security drill on that vessel exceeds 25 percent.

(c) ***Exercises***

(1) Various types of exercises which may include participation of Company Security Officers, port facility security officers, relevant authorities of Contracting Governments as well as Ship Security Officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises.

These exercises should test communications, coordination, resource availability, and response.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the above.

(3) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include the substantial and active participation of relevant company and vessel security personnel, and may include facility security personnel and government authorities depending on the scope and the nature of the exercises.

(6) Company participation in an exercise with another Contracting Government should be recognized by the Administration.

Drills and Training for Rest of ship's Crew

(a) In addition to specific training for personnel that are involved in implementing security actions, all of the ship's crew should receive security awareness training as part of their general orientation and training activities. This awareness training should address issues such as:

- ✓ Limiting discussion about specifics of the ship (e.g., cargo, routes, equipment, crew size) with non-company personnel to those personnel that need to know in order to service the ship
- ✓ Reporting suspicious acts or behavior related to the ship both on/near the ship and when personnel are on shore leave
- ✓ Protection of company-supplied identification cards or other documentation

A high level of awareness by company personnel of these simple measures can help prevent the ship from becoming an easy target.

7.1 Execution of Contingency Plans

There is a famous saying: "Hope for the best and be prepared for the worst". Contingency planning relates to the second half of the saying, i.e. be prepared for the worst. In simple terms, contingency planning means planning for an unforeseen event or an emergency. Hence, depending upon the threat scenario, the ship must identify all the contingencies that can possibly take place. Once the contingencies have been identified, well thought out plans can be drawn up to avoid, minimize and mitigate the adverse effects of the contingency. Some of the contingencies that a ship can expect that would jeopardize its security are:

- ✓ Bomb threat.
- ✓ Hostage situation.
- ✓ Sabotage.
- ✓ Chemical weapon threat.
- ✓ Detection of explosives on board.
- ✓ The onboard organization to handle the contingency.
- ✓ Responsibility and duty of each personnel in tackling in the contingency.
- ✓ Detailed check off list prescribing the action to be taken by each individual.
- ✓ The communications arrangements within the ship.
- ✓ Personnel authorized to communicate with external authorities and the means of communications.
- ✓ Records to be maintained.

The contingency planning for a particular emergency-will vary from ship to ship depending upon the type and size of the ship and resources available. If there is a security threat, the ship will be at Security Level 2 or 3 as advised by the Flag State or by the Contracting Government of the Port Facility. The Security Measures to be taken are laid down in the Ship Security Plan. If the ship is at Security Level 1 and the Master or SSO considers that a security threat exists, he shall take appropriate actions to reduce the threat. He shall also inform the company, the Flag State and the Contracting Government of the Port Facility about the threat assessment.

Breaches of Security

When security is breached, the Master/SSO shall consider doing the following

- ✓ Activate the Ship Security Alert System.
- ✓ Call Emergency Stations.
- ✓ Inform the Contracting Government of the Port Facility.
- ✓ Prepare to evacuate the ship.

Prepare to leave the port.

- ✓ Act on instructions given by the contracting governments.
- ✓ Use the appropriate Contingency Plans.

7.2 Security Drills and Exercises

According to the ISPS-code Part A 9.8.1, security drills and exercises are confidential and cannot be witnessed by third parties other than flag state authorities. There is an old saying, "the more you sweat in peace, the less you bleed in war". The fight against terrorism is a war on many fronts. The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security related deficiencies, which need to be addressed. To ensure the effective implementation of the provisions of the ship security plan, drills shall 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 3 months, a drill shall be conducted within one week of the change. These drills shall test individual elements of the plan. Various types of exercises which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as assistant ship security officers, if available, shall be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises shall test communications, coordination, resource availability, and response These exercises may be:

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

Response Exercises

Company participation in an exercise with another Contracting Government shall be recognized by the Administration. To ensure effective coordination and implementation between the ship, company shore-based personnel, and port facilities, different types of larger scale exercises that include the participation of the Company Security Officer, Port Facility Security Officers, and other appropriate participants should be conducted at least once a year.

The purpose of these large scale events is to test communications, coordination, resource availability and emergency response. Security exercise may be a full-scale, real-time (live) event, involving mobilization and deployment of personnel and equipment or the exercise may be "table-up" activity, where the entire security incident is simulated. Security exercises may be combined with other emergency response exercises, such as search and rescue exercises. Shipboard drill scenarios should address a variety of appropriate threats, which may include:

(a) Damage to the ship or port facility caused by an explosive device (bomb), arson, sabotage, or vandalism.

(b) Hijacking or seizure of the ship or of ship personnel or passengers.

(c) Tampering with cargo, stores or critical ship equipment.

(a) Unauthorised access, including stowaways. ISPS-11

(b) Smuggling weapons or the using the ship to transport terrorists and/or their equipment.

(c) Using the ship itself as a weapon to cause damage or destruction.

(d) Attacks from the sea while at berth, at anchor, or at sea.

Assessment of Security Drills and Exercises

As mentioned earlier, drills and exercises are carried out with the primary aim of bringing up and keeping the personnel and the system competent and ready to contract security threats. In order to ensure that this aim is being met, the security drills and exercises being carried out must be assessed. This can be done by conducting the drills and exercises in a methodical and the prescribed procedure. The exercise and the drill must consist of following three phases

Preparation

As part of the preparation for the exercise, all personnel who are required to participate in the exercise must be thoroughly briefed on the aim of the exercise, how it will be conducted and what each individual is expected to do.

Conduct

The exercise must be conducted in as realistic a manner as possible and in accordance with the laid down procedures. All the records must be meticulously maintained.

De-brief

This is the most relevant part as far as the assessment goes. All the records must be examined. The opinion of the participants must be taken. The whole evolution must be critically examined to assess whether the aims of the drill of the exercise have been met.

8. Security Administration

Flag Administrations have a variety of security responsibilities for ships registered under their authority. These include:

- ✓ Providing guidance on the development of Ship Security Plans
- ✓ Providing guidance on measures for ships to implement at each security level
- ✓ Providing guidance on the reporting of attacks on ships
- ✓ Approving Ship Security Plans
- ✓ Issuing International Ship Security Certificates (ISSC) to ships
- ✓ Notifying ships of appropriate security levels
- ✓ Notifying other governments of ship security alerts from ships within their jurisdiction
- ✓ Specifying requirements for Declarations of Security
- ✓ Agreeing to temporary measures to be implemented if security equipment fails
- ✓ Deciding whether or not to delegate approval of Ship Security Plans, verification of ship security systems and issuing International Ship Security Certificates to Recognized Security Organizations (RSO) and overseeing such delegations.

8.1 Documentation and Records

a. *Records*

1. Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of the Ship Security Plans are being implemented.

2. Records may be kept in any format but should be protect from unauthorized access or disclosure

b. *ISPS Code Part A, Section 10 – Records*

1. Records of the following activities addressed in the Ship Security Plan must be kept on board for at least the time frame covering the previous 10 ports of call.

- ✓ Training, drills and exercises;
- ✓ Security threats and security incidents;
- ✓ Breaches of security;
- ✓ Changes in security level;
- ✓ Communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- ✓ Internal audits and reviews of security activities;
- ✓ Periodic review of the Ship Security Assessment;
- ✓ Periodic review of the Ship Security Plan;
- ✓ Implementation of any amendments to the plan; and
- ✓ Maintenance, calibration and testing of security equipment, if any including testing of the ship security alert system.

2. The records may be kept in an electronic format. In such a case, they shall be safeguarded by procedures to prevent their unauthorized deletion, destruction or amendment.

3. The records shall be protected from unauthorized access or disclosure.

Records Requirements

Vessel Record-Keeping Requirements

(a) Unless otherwise specified, the Ship Security Officer must keep required records for at least 2 years and make them available to the government authorities upon request.

(b) Records may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) Training. For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) Drills and exercises. For each drill or exercise, the date held, description of drill or exercise, list of participants; and any best practices or lessons learned which may improve the Ship Security Plan (SSP);

(3) Incidents and breaches of security. Date and time of occurrence, location within the port, location within the vessel, description of incident or breaches, to whom it was reported, and description of the response;

(4) Changes in Security Levels. Date and time of notification received, and time of compliance with additional requirements;

(5) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, the date and time, and the specific security equipment involved;

(6) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

(7) Declaration of Security (DoS). Manned vessels must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) Annual internal audits of the SSP. For each annual audit, a letter certified by the SSO stating the date the audit was completed.

(9) Annual periodic reviews of the SSA and the SSP maintained.

(c) Required security records must be protected from unauthorized access or disclosure.

(d) Records must be kept in the working language or languages of the ship or translation in either English, French or Spanish.

(e) Security-related records required under the international requirements and any additional records specified by ABS shall be kept for 5 years to allow internal audit review and to provide evidence of program compliance for periodic verification by ABS

Company and Vessel Records

(a) The Company shall ensure that the Master has available on board, updated documented information through which officers duly authorized by a Contracting Government can determine:

- ✓ Who appoints the members of the crew or other persons employed or engaged on board the ship in any capacity.
- ✓ Who decided and decides the employment of the ship; and
- ✓ In cases where the ship is employed under the terms of charter party, who signed the charter party on behalf of the owner of the ship

(b) Ships must be able to provide the following information:

- ✓ That the ship possesses a valid Certificate and the name of its issuing authority;
- ✓ The security level at which the ship is currently operating;
- ✓ The security level at which the ship operated in the 10 previous port calls;
- ✓ Any special or additional security measures that were taken by the ship in the 10 previous port calls;
- ✓ That the appropriate ship security procedures were maintained during any ship-to-ship activity within the timeframe of the previous 10 port calls; or
- ✓ Other practical, security-related information, but not details of the Ship Security Plan.