SETRAC COLLEGE OF OFFSHORE TRAINING

SECURITY TRAINING FOR SEAFARERS

ISSUE DATE – Oct 2017		
DATE	REVISION	REVISED BY
01 Jan 2016	Rev 01	Training Coordinator
01 Jan 2020	Rev 02	Training Coordinator
01 Jan 2023	Rev 03	Training Coordinator
1 Jan 2024	Rev 04	Training Coordinator

INDEX

‘

Chapter 1

Introduction

Course Objective

Those who successfully complete the course should be able to demonstrate sufficient knowledge to undertake the duties assigned under the VSP. 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 behavioral 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 vessel stores.

Course overview

This model course is intended to provide the knowledge required for vessel personnel who are assigned specific security duties in connection with a Vessel Security Plan (VSP) to perform their duties in accordance with the requirements of the Maritime Transportation Security Act of 2002 and/or Chapter XI-2 of SOLAS 74 as amended and/or the IMO ISPS Code and/or U.S. Coast Guard regulations contained in 33 CFR Chapter 1 Subchapter H.

Competences to be achieved

1. Every seafarer who is designated to perform security duties, including anti-piracy and anti-armed-robbery-related activities, shall be required to demonstrate competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2.

2. The level of knowledge of the subjects in column 2 of table A-VI/6-2 shall be sufficient to enable every candidate to perform on board designated security duties, including anti-piracy and anti-armed-robbery-related activities.

3. Every candidate for certification shall be required to provide evidence of having achieved the required standard of competence through:

3.1 demonstration of competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2, in accordance with the methods for demonstrating

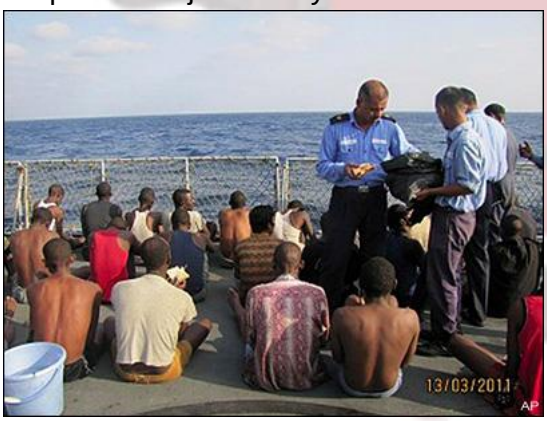
competence and the criteria for evaluating competence tabulated in columns 3 and 4 of that table; and

3.2 examination or continuous assessment as part of an approved training programme covering the material set out in column 2 of table A-VI/6-2.

Current security threats and patterns

Piracy and armed attacks continue to occur on an all too frequent basis. Attacks occur mostly in portareas, whereas piracy, by definition, usually involves ships at sea. In fact, the United Nations Convention on the Law of the Sea, Article 101, defines piracy as any of the following acts: illegal acts of violence or detention or any act of depredation committed for private ends by the crew or the passengers of a private vessel or private aircraft and directed on the high seas against another vessel or aircraft or against persons or property on board such vessel or aircraft. It also includes such acts against a vessel, aircraft, person or property in a place outside of the jurisdiction of any State.

Terrorism usually involves violence, or the threat of violence, by extremist groups seeking to gain political objectives by malicious means. A terrorist group may hope to make a statement by using various types of bombs, making bomb threats or hijacking a vessel. Increasingly, terrorists are acting in connection with extremist religious sects that promote suicidal behavior. Contraband smuggling, a criminal activity, may result in large financial loss to the vessel owner whose vessel is being used by the smugglers. Often, drugs are the commodity being smuggled and they may be brought on board in a number of creative ways such as in luggage, stores, on or in a person's body, or in electronic equipment. Weapons are also a frequent item associated with smuggling. Like drugs, weapons, too, find their way on board in various ways, such as in cargo containers.



Cargo theft, an age-old problem, continues to plague the maritime industry and causes financial losses in staggering amounts. Prevention is normally the most effective method of dealing with this security threat.

Security Threat at Sea

The attack, stated to be by Al Qaeda, on the US naval ship USS Cole at Aden in October, 2000, and the subsequent investigation into that incident gave birth to concerns that international terrorists might expand their acts of terrorism from the land to the sea. Terrorist groups of West Asia and the Liberation Tigers of Tamil Eelam (LTTE) had indulged in acts of maritime terrorism

even before October, 2000, and the LTTE, through its fleet of ships, ostensibly used for legitimate commercial purposes, had been using the sea for the clandestine transport of arms and ammunition and other material required for its acts of terrorism on the land. However, such uses had limited tactical objectives and did not think in terms of mass casualties or mass damage to be inflicted on the global economy as a whole.

The 9/11 terrorist strikes in the US and the precision and the evil ingenuity with which they were planned and executed created a wave of alarm about the likelihood of similar strikes at coastal and maritime targets. Since 9/11, there is hardly any discussion, governmental or non-governmental, on threats to national security and to international peace and security in which possible threats from maritime terrorism do not figure prominently.Post-9/11, scenario-building exercises have invariably included scenarios involving possible catastrophic acts of maritime terrorism. Four of these possible scenarios are or should be of major concern to national security managers:

First, terrorists hijacking a huge oil or gas tanker and exploding it in mid-sea or in a major port in order to cause huge human, material and environmental damage. There were 67 reported attacks on oil and gas tankers by pirates during 2004. This despite the stepped-up patrolling by the Navies of different countries. What pirates with no ideological motive and with no suicidal fervour can do, ideologically-driven suicide terrorists can do with equal, if not greater, ease. Second, terrorists hijacking an oil or gas tanker or a bulk-carrier and exploding it or scuttling it in maritime choke-points such as the Malacca Strait in order to cause a major disruption of energy supplies and global trade. There were 52 reported attacks on bulk carriers by pirates during 2004. If the pirates can do it despite naval patrolling, so can the terrorists.Third, terrorists smuggling weapon of mass destruction material such as radiological waste or lethal chemicals or even biological weapons in a container and having it exploded through a cellular phone as soon as the vessel carrying the container reaches a major port.Fourth, sea-borne terrorists attacking a nuclear establishment or an oil refinery or off-shore oil platforms.

Vessel Personnel with Specific Security Duties

Although there may not be violence or political issues involved in most cargo theft cases, this matter remains high on the list of security threats and requires solutions discussed in this course. Instructors should convey that cargo theft is only one of the various threats to the security of cargo. Other such security threats should be discussed during this section of the course.Collateral damage occurs when a nearby fire, explosion, or attack results in damage to a vessel or facility. While the damage is sometimes unintended, the costs are nevertheless real. There are measures that may minimize the consequences of this type of damage.

Chapter 2

Maritime Security Policy

Maritime Security

The term maritime security represents the broadest approach to issues and aspects which pertain to the sea and have an important bearing on the country's security.. This volume would go a long way in generating fuller understanding of the different aspects of the maritime dimensions of India's security.

As the seas of peninsular India and the Indian Ocean become more important than even before to the security of the country, it is imperative to examine the maritime dimensions of Indian security in a comprehensive manner. India's Maritime security provides, for the first time, a holistic assessment of the economic, political, and military aspects of India's maritime security.

The term maritime security is defined as comprising those issues which pertain to the sea and have a critical bearing on the country's security. These include seaborne trade and commerce in energy resources, the management of living and non-living marine resources, the delimitation of international seaward boundaries, and the deployment and employment of naval and military forces in the Indian Ocean.

Maritime Security Policy

All nations and port authorities can benefit from a coordinated policy for maritime security ctivities that involve cooperation with foreign governments, international and regional organisations, and the private sector.

The oceans are the largest part of the surface of our planet, a continuous domain with few visible traces of nations' 'territorial seas' and 'exclusive economic zones.'The oceans are largely borderless, and in countries with coastlines the many agencies responsible for maritime security have overlapping territories and mandates, which makes coordination and information sharing absolutely necessary in today's security environment.

Different nations' agencies assign security roles in different ways, but the need for information sharing is the same.In India Maritime Security is looked after by Navy and Coast Guard. In the recent years the Police department have also started developing infrastructure and expertise for coastal security. DG Shipping certifies the security of ships and ports.

A large number of US maritime security policy documents explicitly state the need for cooperation with the agencies of other governments and with scores of international, regional and industry organisations, many of which are listed in an appendix to the US State Department's International Outreach and Coordination Strategy for the National Strategy for Maritime Security (NSMS), released in November 2005.

Plans for port security programmes include terms like 'maritime intelligence integration,' 'coordinated response,' and 'standardised procedures.'The previously mentioned document includes this sentence "maritime domain awareness will be achieved by improving our ability to collect, fuse, analyse, display, and disseminate actionable information and intelligence to

operational commanders and decision makers.Geospatial interoperability refers to the ability of diverse systems to transparently exchange diverse kinds of geospatial information and services and to support the query/response mechanisms of geospatial Web services.

Such communication depends on transmitting or exchanging through a common system of interfaces and encodings. Standardisation means 'agreeing on a common system,' so standardisation on interface and encoding specifications is a maritime security, and port security, requirement.Criminals and individual terrorists who belong to international networks are more likely to be noticed by civil sector agencies than by defense agencies.

Because maritime domain awareness requires that both defense and civil sector agencies be able to "collect, fuse, analyse, display, and disseminate actionable information and intelligence," it is important that the same geospatial standards are being agreed upon by both types of agencies.

Regulations

The International Maritime Organization (IMO) has adopted a number of resolutions and conventions to this end. For example, Resolution A.545(13)--Measures To Prevent Acts Of Piracy And Armed Robbery Against Ships was signed in 1983. In 1985 came IMOResolution A.584 (14)--Measures To Prevent Unlawful Acts Which Threaten Safety Of Ships AndSecurity Of Passengers (this was later reviewed in November of 2001 with IMO Resolution A.924(22)).

Then in 1986 the IMO approved MSC/Circ.443--Measures To Prevent Unlawful Acts Against Passengers And Crew On Board Ships. In 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) treaties aimed at ensuring that appropriate judicial action is taken against persons committing unlawful acts against ships. Unlawful acts would include the seizure of vessels by force, acts of violence against persons on board vessels, and placing devices on board a vessel which are likely to destroy or damage it. The convention obliges contracting governments either to extradite or prosecute alleged offenders. The SUA came into effect on March 1, 1992.

Following the tragic events of September 11, 2001 the twenty-second session of the IMO, in November of 2001, unanimously agreed to incorporate security regulations. They approved the development of new measures relating to the security of vessels and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 in December of 2002 (the Diplomatic Conference). This timetable of little more than a year represents a landmark achievement for IMO. It provides a clear indication of the gravity of the situation as well as the intention to protect world shipping against security incidents and threats.

The meeting of the Diplomatic Conference in December of 2002 resulted in amendments to SOLAS 74. These amendments enter into force on July 1, 2004. A brief summary of these amendments should be carried out with mention of changes to Chapter V but with emphasis on the changes to Chapter XI, Regulations 3 and 5 and the new Chapter XI-2 Regulations 1-13 and the ISPS Code.

Definitions

2.1 For the purpose of this part, unless expressly provided otherwise:

.1 *Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.

.2 *Regulation* means a regulation of the Convention.

.3 *Chapter* means a chapter of the Convention.

.4 *Ship security plan* 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.

.5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons**,** cargo, cargo transport units and ship.s stores within the port facility from the risks of a security incident.

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

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

.8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

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

.10 *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

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

2.2 The term .ship., when used in ISPS Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term .Contracting Government. in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the .Designated Authority.

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

Handling sensitive security-related information and communications

Ship communicate internally as well as with external agencies on various matters of ship operation. Some of this information may be sensitive and may jeoperdise the ship safety in case it is leaked to unautorised personnel.It therefore needs to be appreciated that certain information and communications will be considered security sensitive and that the level of sensitivity may change, as do levels of security 1, 2, and 3. Seemingly benign conversations, therefore, may result in disastrous consequences. All personnel will need to appreciate the risk of security leaks through communication by improper methods or to the wrong persons.

Chapter 3

Security Responsibilities

RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

Subject to the provisions of regulation XI-2/3 and XI-2/7, 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:

.1 the degree that the threat information is credible;
.2 the degree that the threat information is corroborated;
.3 the degree that the threat information is specific or imminent; and
.4 the potential consequences of such a security incident.

Contracting Governments, when they 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 certain of their security related duties under chapter XI-2 and this Part of the Code with the exception of:

.1 setting of the applicable security level;
.2 approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;
.3 determining the port facilities which will be required to designate a Port Facility Security Officer;
.4 approving a Port Facility Security Plan and subsequent amendments to an approved plan;
.5 exercising control and compliance measures pursuant to regulation XI-2/9; and
.6 establishing the requirements for a Declaration of Security.

Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

Recognized Security Organizations

States may delegate some of their responsibilities to RSO who may then may take on the security-related activities of a contracting government.

OBLIGATIONS OF THE COMPANY

The Company shall ensure that the ship security plan contains a clear statement emphasizing the master.s authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities inaccordance with chapter XI-2 and this Part of the Code.

SHIP SECURITY

A ship is required to act upon the security levels set by Contracting Governments as set out below.

At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of ISPS Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship security duties;
.2 controlling access to the ship;
.3 controlling the embarkation of persons and their effects;
.4 monitoring restricted areas to ensure that only authorized persons have access;
.5 monitoring of deck areas and areas surrounding the ship;
.6 supervising the handling of cargo and ship.s stores; and
.7 ensuring that security communication is readily available.

At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of ISPS Code.

At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of ISPS Code. Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liase and co-ordinate the appropriate action than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation. In such cases, the ship security officer shall liaise with the port facility security officer
and co-ordinate appropriate actions, if necessary.

An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay. When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in the part B of ISPS Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

COMPANY SECURITY OFFICER

The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

In addition to those specified elsewhere in ISPS Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirements;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

SHIP SECURITY OFFICER

A ship security officer shall be designated on each ship. In addition to those specified elsewhere in the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

.1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.2 maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;

.3 coordinating the security aspects of the handling of cargo and ship.s stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

.5 reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

.6 enhancing security awareness and vigilance on board;

.7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.8 reporting all security incidents;

.9 co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

.10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

P ORT FACILITY SECURITY

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

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:

.1 ensuring the performance of all port facility security duties;

.2 controlling access to the port facility;
.3 monitoring of the port facility, including anchoring and berthing area(s);
.4 monitoring restricted areas to ensure that only authorized persons have access;
.5 supervising the handling of cargo;
.6 supervising the handling of ship.s stores; and
.7 ensuring that security communication is readily available.

At security level 2, the 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 ISPS Code. At security level 3, further specific 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 ISPS Code. In addition, at security level 3, port facilities are 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 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 ship security officer shall liase 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 liase with the ship security officer and co-ordinate appropriate actions, if necessary.

PORT FACILITY SECURITY OFFICER

A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities. In addition to those specified elsewhere in ISPS Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.1 conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
.2 ensuring the development and maintenance of the port facility security plan;
.3 implementing and exercising the port facility security plan;
.4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
.5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
.6 enhancing security awareness and vigilance of the port facility personnel;
.7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;
.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
.9 co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
.10 co-ordinating with security services, as appropriate;

.11 ensuring that standards for personnel responsible for security of the port facility are met;
.12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
.13 assisting ship security officers in confirming the identity of those seeking to board the ship when requested.
17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and this Part of the Code.

Vessel Personnel with Specific Security Duties

Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

On-scene security surveys

Oon-scene security survey is an integral part of any Vessel Security Assessment. They should understand that the survey should fulfil the following functions:

- identification of existing security measures, procedures and operations;
- identification and evaluation of key vessel operations that it is important to protect;
- identification of possible threats to the key vessel operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- identification of weaknesses, including human factors in the infrastructure, policies and procedures.

It should be emphasized to course participants that the on-scene survey should examine and evaluate
existing vessel protective measures, procedures and operations for:

- ensuring the performance of all security duties;
- controlling access to the vessel, through the use of identification systems or otherwise;
- controlling the embarkation of vessel personnel and other persons and their effects, including
personal effects and baggage whether accompanied or unaccompanied;
- supervising the handling of cargo and the delivery of vessel stores;
- monitoring restricted areas to ensure that only authorized persons have access;
- monitoring deck areas and areas surrounding the vessel; and
- ensuring the ready availability of security communications, information, and equipment.

Chapter 4

Vessel Security Assessment

SHIP SECURITY ASSESSMENT

The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan. The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this ISPS Guidelines. A recognized security organization may be authorized by administration to carry out the ship security assessment of a specific ship. The ship security assessment shall be documented, reviewed, accepted and retained by the Company.The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key ship board operations that it is important to protect;

.3 identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

.4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Assessment tools

Trainees must be encouraged to adopt systematic and consistent approaches to the evaluation of security conditions and vulnerabilities. Vessel personnel with specific security duties may be called upon to assist in these evaluations. The use of checklists to perform assessments of security in day-to-day operations should therefore be discussed, noting the inclusion of categories such as the following:

- General layout of the vessel.
- Location of areas that should have restricted access, such as the bridge, engine room, radio room, etc.
- Location and function of each actual or potential access point to the vessel.
- Open deck arrangement including the height of the deck above water.
- Emergency and stand-by equipment available to maintain essential services.
- Numerical strength, reliability, and security duties of the vessel's crew.
- Existing security and safety equipment for protecting the passengers and crew.
- Existing agreements with private security companies for providing vessel and waterside security services.

 Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

On-scene security surveys

On-scene security survey is an integral part of any Vessel Security Assessment. The survey should fulfill the following functions:

 identification of existing security measures, procedures and operations;
 identification and evaluation of key vessel operations that it is important to protect;
 identification of possible threats to the key vessel operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
 identification of weaknesses, including human factors in the infrastructure, policies and procedures. It should be emphasized to course participants that the on-scene survey should examine and evaluate existing vessel protective measures, procedures and operations for:
 ensuring the performance of all security duties;
 controlling access to the vessel, through the use of identification systems or otherwise;
 controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;
 supervising the handling of cargo and the delivery of vessel stores;
 monitoring restricted areas to ensure that only authorized persons have access;
 monitoring deck areas and areas surrounding the vessel; and
 ensuring the ready availability of security communications, information, and equipment.

SHIP SECURITY PLAN

Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in ISPS Code. The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations. In such cases the recognized security organization, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

The submission of a ship security plan, or of amendments to a previously approved plan,for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, have been developed. Such a plan shall be developed**,** taking into account the guidance given in part B of ISPS Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

.9 procedures for training, drills and exercises associated with the plan;

.10 procedures for interfacing with port facility security activities;

.11 procedures for the periodic review of the plan and for updating;

.12 procedures for reporting security incidents;

.13 identification of the ship security officer;

.14 identification of the company security officer including 24-hour contact details;

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided;1 and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.1

9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

9.5 The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this Part of the Code.

9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim

International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. The plan shall be protected from unauthorized access or disclosure. Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9

Administrations may allow, in order to avoid compromising in any way the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of ISPS Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the noncompliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this Part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

Chapter 5

Security Equipment

Security equipment and systems

security equipment and systems that are useful in enhancing maritime security, both ashore and afloat. Examples of such equipment include:

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

Anatomy of a Metal Detector

A typical metal detector is light-weight and consists of just a few parts:

1. **Stabilizer** (optional) - used to keep the unit steady as you sweep it back and forth
2. **Control box** - contains the circuitry, controls, speaker, batteries and the microprocessor
3. **Shaft** - connects the control box and the coil; often adjustable so you can set it at a comfortable level for your height
4. **Search coil** - the part that actually senses the metal; also known as the "search head," "loop" or "antenna"

Most systems also have a **jack** for connecting headphones, and some have the control box below the shaft and a small **display unit** above.

Operating a metal detector is simple. Once you turn the unit on, you move slowly over the area you wish to search. In most cases, you sweep the coil (search head) back and forth over the ground in front of you. When you pass it over a target object, an audible signal occurs. More advanced metal detectors provide displays that pinpoint the type of metal it has detected and how deep in the ground the target object is located.

Metal detectors use one of three technologies:

- **Very low frequency** (VLF)
- **Pulse induction** (PI)
- **Beat-frequency oscillation** (BFO)

Ship Security Alert System (SSAS) is part of the ISPS code and is a system that contributes to the International Maritime Organization's (IMO)'s efforts to strengthen maritime security and suppress acts of terrorism and piracy against shipping. The system is a joint project between Cospas-Sarsat and the IMO. In case of attempted piracy or terrorism, the ship's SSAS beacon can be activated, and appropriate law-enforcement or military forces can be dispatched. An SSAS beacon operates with similar principles to the aircraft transponder emergency code 7700.

When an SSAS alert is triggered: [1]

- the Rescue Coordination Centres (RCCs) or SAR Points of Contact (SPOCs) for the country code the beacon is transmitting is notified discreetly
- national authorities dispatch appropriate forces to deal with the terrorist or pirate threat

Operational limitations of security equipment and systems

The functional limitations and operating constraints of security equipment that they may encounter are effective range, environmental sensitivities, and operator (human) error should be addressed as appropriate. Personnel using security equipment must familiarize themselves with the manufactures operation instruction including the limitations on use.

Testing, calibration and maintenance of security equipment and systems

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

Chapter 6

Threat Identification, Recognition, and Response

Methods of physical searches and non-intrusive inspections

Unless there are clear security grounds for doing so; members of the vessel's crew should not be required to search their colleagues or their personal effects. It should be conveyed that any such search shall be undertaken in a manner that fully takes into account the human rights of the individual and preserves his or her basic human dignity.

Execution and coordination of searches

Personnel on board must acquainted themselves with the utility of "check cards" in conducting systematic searches. A "check card" is a card that can be issued to each searcher specifying the route to follow and the areas to be searched. These cards can be colour-coded for different areas of responsibility, for example blue for deck, red for engine room. On completion of individual search tasks, the cards are returned to a central control point. When all cards are returned, the search is known to be complete. The findings of the search can then be discussed. Course participants should be familiar with the list of basic equipment that may be employed in conducting searches. This list may include:

- flashlights and batteries;
- screwdrivers, wrenches and crowbars;
- mirrors and probes;
- gloves, hard hats, overalls and non-slip footwear;
- plastic bags and envelopes for collection of evidence;
- forms on which to record activities and discoveries. Personnel on board ship should learn procedures to be followed so as to ensure effective and efficient searches.
- Crew members should not be allowed to search their own areas in recognition of the possibility that they may have concealed packages or devices in their own work or personal areas
- The search should be conducted according to a specific plan or schedule and must be carefully controlled.
- Special consideration should be given to search parties working in pairs with one searching
"high" and one searching "low". If a suspicious object is found, one of the pair can remain on
guard while the other reports the find.
- Searchers should be able to recognize suspicious items.

 There should be a system for marking or recording “clean” areas

 Searchers should maintain contact with the search controllers, perhaps by UHF / VHF radio,
bearing in mind the dangers of using radio equipment in the vicinity of Improvised Explosive
Devices (IEDs).

 Searchers should have clear guidance on what to do if a suspect package, device, or situation is found.

 Searchers should bear in mind that weapons and other dangerous devices may be intentionally placed to match its context as a means of disguise, such as a toolbox in an engine room. Participants in the course should be acquainted with the fact that there are many places on board a vessel where weapons, dangerous substances, and devices can be concealed. Some of these are:

Cabins

 Back sides and underneath drawers

 Between bottom drawer and deck

 Beneath bunks, e.g. taped to bunk frame under mattress

 Under wash basin

 Behind removable medicine chest

 Inside radios, recorders etc.

 Ventilator ducts

 Inside heater units

 Above or behind light fixtures

 Above ceiling and wall panels

 Cutouts behind bulkheads, pictures, etc.

 False bottom clothes closets-hanging clothes

 Inside wooden clothes hangers

 Inside rolled socks, spare socks

 Hollowed-out molding

Companionways

 Ducts

 Wire harnesses

 Railings

 Fire extinguishers

- Fire hoses and compartments
- Access panels in floors, walls, ceilings
- Behind or inside water coolers, igloos

Toilet and Showers

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

Deck

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

Engine room

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

Galleys and Stewards' Stores

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

Recognition, on a non-discriminatory basis, of persons posing potential security risks

Personnel should recognise suspicious patterns of behavior, and avoid racial profiling and ethnic stereotyping. Examples of suspicious behaviours include:

 Unknown persons photographing vessels or facilities.

 Unknown persons attempting to gain access to vessels or facilities.

 Individuals establishing businesses or roadside food stands either adjacent or in proximity to facilities.

 Unknown persons loitering in the vicinity of vessels or port facilities for extended periods of time.

 Vehicles with personnel in them loitering and perhaps taking photographs or creating diagrams of vessels or facilities.

 Small boats with personnel on board loitering and perhaps taking photographs or creating diagrams of vessels or facilities.

 General aviation aircraft operating in proximity to vessels or facilities.

 Persons who may be carrying bombs or participating in suicide squad activities.

 Unknown persons attempting to gain information about vessels or facilities by walking up to personnel or their families and engaging them in a conversation.

 Vendors attempting to sell merchandise.

 Workmen trying to gain access to vessels to repair, replace, service, or install equipment.

 E-mails attempting to obtain information regarding vessels, personnel, or standard operating procedures.

 Package drop-offs/attempted drop-offs.

 Anti-national sentiments being expressed by employees or vendors.

 Anti-national pamphlets or flyers distributed to employees or placed on windshields in parking lots.

 Out-of-the-ordinary phone calls.

 Recreational boaters or persons aboard refugee craft posing as mariners in distress to attract assistance from other vessels.

Techniques used to circumvent security measures

No security equipment or measure is infallible. There are techniques that can be employed to evade security systems and controls, such as the disabling of alarm systems, picking of locks, jamming of radio signals, etc.

Chapter 7

Emergency Preparedness Security drills and exercises

Vessel Security Actions

Action to be taken onboard ship will vary depending upon the prevalent security threat and what is the Security level.

Actions required by different security levels

The basic guideline sfor actions to be taken are given in ISPS Code. The actions for a particular ship are given in the Ship Security plan. Based on these, the ships will prepare their check lists for each security level to ensure that no action is overlooked for implementation.

Maintaining security of the vessel/port interface

The vessel/port interface determines the need for a Facility Security Plan and the interaction with the Vessel Security Plan. Instructors should ensure that trainees are clear on the critical importance of the interaction between the vessel security plan and that of the facility.

DECLARATION OF SECURITY

Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses to persons, property or the environment. A ship can request completion of a Declaration of Security when:

.1 the ship is operating at a higher security level than the port facility or another ship
it is interfacing with;
.2 there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
.4 the ship is at a port which is not required to have and implement an approved port
facility security plan; or
.5 the ship is conducting ship to ship activities with another ship not required to have
and implement an approved ship security plan.
5.3 Requests for the completion of a Declaration of Security, under this section, shall be
acknowledged by the applicable port facility or ship.

5.4 The Declaration of Security shall be completed by:
.1 the master or the ship security officer on behalf of the ship(s); and, if appropriate,
.2 the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each. Contracting Governments shall specify**,** bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory. Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

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 vessel, verifying and controlling the use of identification credentials, monitoring deck areas and areas surrounding the vessel, and so forth.

Execution of contingency plans

Variety of contingencies associated with terrorism and other criminal activities that may arise in the maritime setting. Possible responses in the case of bomb threats, explosions, piracy, hijackings, and similar events are included in the SSP.

Security drills and exercises

Tthe objective of drills and exercises is to ensure that vessel personnel are proficient in all assigned security duties at all security levels and in the identification of any security-related deficiencies that need to be addressed. Personnel on board ship should learn that effective implementation of the provisions of the Vessel Security Plan requires that drills be conducted at least once every three months.

In addition, in cases where more than 25 percent of the vessel's personnel have been changed, at any one time, with personnel that have not previously participated in any drill on that vessel within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as:

 damage to, or destruction of, the vessel or of a port facility, e.g. by explosive devices, arson,
sabotage or vandalism;
 hijacking or seizure of the vessel or of persons on board;
 tampering with cargo, essential vessel equipment, systems, or vessel stores;
 unauthorized access or use, including presence of stowaways;
 smuggling weapons or equipment, including weapons of mass destruction;

 use of the vessel to carry persons intending to cause a security incident, or their equipment;
 use of the vessel itself as a weapon or as a means to cause damage or destruction;
 attacks from seaward while at berth or at anchor; and
 attacks while at sea.

Various types of exercises involving participation of vessel security personnel 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. 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.

Chapter 8

Security Administration

Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

.1 training, drills and exercises;
.2 security threats and security incidents;
.3 breaches of security;
.4 changes in security level;
.5 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;
.6 internal audits and reviews of security activities;
.7 periodic review of the ship security assessment;
.8 periodic review of the ship security plan;
.9 implementation of any amendments to the plan; and
.10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included. The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment. The records shall be protected from unauthorized access or disclosure.