1.0 CONDITIONS SET OUT IN A SHIP SECURITY PLAN

1.1 Introduction

This course aims to provide knowledge and awareness to all seafarers with respect to Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, the International Ship and Port Facility Security Code (ISPS), the Ship Security Plan (SSP), and Section A-VI/6-1 of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended.

At the end of the training, trainees are expected to achieve the following competencies:

- Maintain the conditions set out in a ship security plan
- Recognize security risks and threats
- Undertake regular security inspections of the ship
- Properly use available security equipment and systems

1.2 Current security threats and patterns

Current threats to maritime security provide a basis for understanding of the recent conventions and legislation in this area and to fully grasp the importance of the training provided by this course. The prospective security officers receiving this training must clearly sense the reality of today's security issues, which include piracy, terrorism, contraband smuggling, cargo theft, and collateral damage.

- ### Threats to the Maritime Transport Industry

Armed robbery – any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State’s internal waters, archipelagic waters and territorial sea (International Maritime Organization)

Cargo theft – pilferage of ship’s cargo. This is an age-old problem that continues to plague the maritime industry and causes financial losses in staggering amounts. Cargo Theft is the **criminal taking of any cargo** including, but not limited to, goods, chattels, money, or baggage that constitutes, in whole or in part, a commercial shipment of freight moving in commerce, from any pipeline system, railroad car, motortruck, or other vehicle, or from any tank or storage facility.

Contraband smuggling – bringing on board goods that are forbidden by law to be **exported or imported illegally,** either in defiance of a total ban or without payment of duty.

Collateral damage – general term for deaths, injuries, or other damage inflicted on an **unintended target**

Hijack – to force the vessel to a nonscheduled landing point

Mutiny – forcible resistance to revolt against constituted authority on the part of the subordinates; specifically, an insurrection of seamen against the authority of their commanders

Piracy – As defined in Article 101 of UNCLOS, consists of any of the following acts:

a. Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or passengers of a private ship or a private aircraft and directed:
   (i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
   (ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
b. Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
c. Any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

Stowaways and refugees – **persons who hide aboard the ship** to obtain free passage or evade port officials; one who flees from political or religious persecution

Terrorism – the use of, or the threat of the use of, directed or indiscriminate violence against innocent victims for maximum and emotional effect, producing a long-term effect far greater than the incident itself would normally warrant in attaining political objectives

- Recent piracy incidents

	2012	2013	2014	2015	2016	2017	2018
Vessels Boarded	174	202	183	203	150	136	143
Vessels Hijacked	28	12	21	15	7	6	6
Total Actual Attacks	**202**	**214**	**204**	**218**	**157**	**142**	**149**
Attempted Attacks	67	28	28	27	22	22	34
Vessels Fired Upon	28	22	13	1	12	16	18
Total Attempted Attacks	**95**	**50**	**41**	**28**	**34**	**38**	**52**
Crew Taken Hostage	**585**	**304**	**442**	**271**	**151**	**91**	**141**
Crew Kidnapped	**26**	**36**	**9**	**19**	**62**	**75**	**83**
Crew Killed	**6**	**1**	**4**	**1**	**0**	**3**	**0**

SOURCE: Piracy and Armed Robbery against Ships Report. ICC International Maritime Bureau

1.3 Maritime security terms

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

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

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

Port facility - a specific location in a port where passengers or commodities are transferred between land and water carriers or between two water carriers, including wharves, piers, sheds, warehouses, yards, and docks.

Ship/Port interface - the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons or goods or the provision of port services to or from the ship.

Ship to ship activity - (STS) transfer operation is the transfer of cargo between seagoing ships positioned alongside each other, either while stationary or underway. Cargoes typically transferred via STS methods include crude oil, liquefied gas (LPG or LNG), bulk cargo, and petroleum products.

Port Facility Security Plan – 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

Port Facility Security Officer - the person designated as responsible for the development, implementation, revision, and maintenance of the port facility security plan and for liaison with ship security officers and company security officers

Designated authority - The organization or the administration identified as responsible for ensuring the implementation of Chapter XI-2 of the Safety Convention pertaining to port facility security and ship/port interface from the point of view of the port facility.

Recognized security organization - An organization with appropriate expertise in security and anti-terrorism matters recognized by the Administration and authorized by it to carry out assessment, verification, approval and certification activities, required by SOLAS Chapter XI-2 or by Part A of the ISPS Code, on its behalf

Declaration of security - is defined by the Safety of Life at Sea (SOLAS) Convention as "an agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement"

Security incident - is an event that may indicate that a ship or port facilities security have been compromised or that measures put in place to protect them have failed.

Security level - The security levels under the ISPS code describe the current scenario related to the security threat to the country and its coastal region including the ships visiting that country. The security levels are decided by the cooperation of ship and port authority, keeping the current condition of national and international security. The local government sets the security level and ensures to inform port state and ships prior to entering the port, or when berthed in the port.

1.4 Maritime security policy

1.4.1 International conventions, codes and recommendations

- Previous efforts of the International Maritime Organization (IMO)

The International Maritime Organization (IMO) has adopted a number of resolutions and conventions toward maritime security. Early efforts of the IMO include the following:

Resolution A.545 (13)--Measures to Prevent Acts of Piracy and Armed Robbery against Ships – Signed in 1983, this resolution urged action to initiate a series of measures to combat acts of piracy and armed robbery ships and small craft at sea.

Resolution A.584 (14)--Measures to Prevent Unlawful Acts Which Threaten Safety of Ships and Security of Passengers – Adopted in 1985, following the hijacking of the Italian cruise ship Achille Lauro, in October 1985, which marked **one of the first actual terrorist acts recorded in modern maritime history.** This was later reviewed in November of 2001 with IMO Resolution A.924 (22).

MSC/Circ.443--Measures to Prevent Unlawful Acts against Passengers and Crews On Board Ships – Approved in 1986, this is intended for application to passenger ships engaged on international voyages of 24 hours or more and the port facilities that serve them.

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) – Adopted in 1988, the treaty ensures 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.

The Organization has also adopted other maritime security instruments including the following:

MSC/Circs. 622 and 623, as revised, on Guidelines for administrations and industry on combating acts of piracy and armed robbery against ships;

MSC/Circ. 754 on Passenger ferry security, providing recommendations on security measures for passenger ferries on international voyages shorter than 24 hours, and ports;

Assembly resolution A.871(20) on Guidelines on the allocation of responsibilities to seek the successful resolution of stowaway cases; and

Assembly resolution A.872(20) on Guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic.

- ## Efforts of the International Maritime Organization (IMO) following 9/11

Following the tragic events of September 11, 2001, the Organization passed Assembly resolution A.924(22) which called for a review of the existing international legal and technical measures to prevent and suppress terrorist acts against ships at sea and in port, and to improve security aboard and ashore.

The adoption of resolution A.924(22) precipitated a Diplomatic Conference on Maritime Security in December 2002 attended by Contracting Governments to the 1974 SOLAS Convention. The 2002 SOLAS Conference adopted a number of amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended. This timetable of a little more than a year represents a landmark achievement for the 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.

International Maritime Organization (IMO)

By June 2004, part of the agreement under IMO is the implementation of measures under the International Ship and Port Facility Security Code (ISPS Code) and the Convention on Safety of Life at Sea (SOLAS). These measures will greatly affect both the public and private sectors. Specifically, the measures will be applied on governments, ships and maritime carrier companies; and ports facilities and operators.

Under ISPS Code, ships will be required to have the following:

(a) Security plans
(b) Security officers and
(c) Onboard Security equipment

On the other hand, port facilities will have their own

(a) Security plan
(b) Security officers and
(c) Security equipment

For ships and port facilities, the requirements also include:

a) Monitoring and controlling access;
b) Monitoring the activities of people and cargo; and
c) Ensuring security communications are readily available

To ensure implementation of the foregoing requirements, the ISPS Code also emphasizes the importance of training and drills.

World Customs Organization (WCO) Task Force on Security and Facilitation of International Trade

Upon the request of developed countries and the IMO, the WCO created a task force to promote security and trade facilitation in the supply chain. The challenge to the task force is how to harmonize the various security initiatives without affecting the international movement of goods. By June of 2003, the WCO has developed various initiatives such as:

1. Export controls (e.g. Unique Consignment Reference and WCO Data Model); and
2. Guidelines for cooperation between business and governments (e.g. Legal and Procedural infrastructure for Data Collection and Transmission / Advance Cargo Information).

▪ Amendments to SOLAS, 1974, as amended and the ISPS Code

The 2002 SOLAS Conference amended SOLAS Chapter XI to include the following special measures for maritime security:

- SOLAS Chapter XI was divided into two parts: **Chapter XI-1: Special Measures to Enhance Maritime Safety**; and **Chapter XI-2: Special Measures to Enhance Maritime Security.**
- SOLAS Chapter XI-2 incorporated new regulations regarding definitions and the requirements for ships and port facilities.
- These new regulations are supported by the **International Ship and Port Facility Security Code (ISPS Code)** which contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a non-mandatory section (Part B).

The new SOLAS Chapter XI-2 and the ISPS Code were intended to ensure the security of ships and port facilities by treating this as a risk management activity and ensuring appropriate security measures through an assessment of the risks in each particular case.

▪ Security-related provisions of the STCW Code

STCW Code Section A-VI/6.
Mandatory minimum requirements for security related training and instruction for all seafarers.

1. Security related familiarization.

Before being assigned to shipboard duties, all persons employed or engaged on a seagoing ship which is required to comply with the provisions of the ISPS Code, other than passengers, shall receive approved security-related familiarization training.

The security-related familiarization shall be conducted by the ship security officer or an equally qualified person.
Documentary evidence must be retained by the ship to show that this familiarization has been carried out.

2. Proficiency in security awareness.

Seafarers employed or engaged in any capacity on board a ship which is required to comply with the provisions of the ISPS Code on the business of that ship as part of the ship's complement without security duties shall, before being assigned to any shipboard duties, receive appropriate approved training or instruction in security awareness as set out in table A-VI/6-1.

An STCW Certificate of Proficiency in security awareness must be issued to the seafarer to show that this training has been carried out.

Transitional provisions.

Until 1 January 2014, seafarers who commenced an approved seagoing service prior to the date of entry into force of this section shall be able to establish that they meet the above requirements by previous equivalent training and/or relevant sea service, and can be issued with an STCW Certificate of Proficiency without further training.

3. Proficiency in designated security duties.

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 duties and responsibilities listed in column 1 of Table A-VI-6-2.

An STCW Certificate of Proficiency in designated security duties must be issued to the seafarer to show that this training has been carried out.

Transitional provisions

Until 1 January 2014, seafarers who commenced an approved seagoing service prior to the date of entry into force of this section shall be able to establish that they meet the above requirements by previous equivalent training and/or relevant sea service, and can be issued with an STCW Certificate of Proficiency without further training.

- IMO guidance on preventing and suppressing acts of piracy and armed robbery against ships

Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships

1 The Maritime Safety Committee, at its eighty-sixth session (27 May to 5 June 2009), approved a **revised MSC/Circ.623/Rev.3 (Guidance to shipowners and ship operators, shipmasters and crews for preventing and suppressing acts of piracy and armed robbery against ships)** as given at annex.

2 The revision was carried out on the basis of the outcome of the comprehensive review of the guidance provided by the Organization for preventing and suppressing piracy and armed robbery against ships; and took into account the work of the correspondence group on the review and updating of MSC/Circ.622/Rev.1, MSC/Circ.623/Rev.3 and resolution A.922(22), established by MSC 84.

3 Member Governments and organizations in consultative status with IMO are recommended to bring this circular to the attention of shipowners, ship operators, shipping companies, shipmasters and crews and all other parties concerned.

4 This circular revokes MSC/Circ.623/Rev.3.

It is important to bear in mind that shipowners, companies, ship operators, masters and crews can and should take measures to protect themselves and their ships from pirates and armed robbers. While security forces can often advise on these measures, and flag States are required to take such measures as are necessary to ensure that owners and masters accept their responsibility, ultimately it is the responsibility of shipowners, companies, ship operators, masters and ship operators to take seamanlike precautions when their ships navigate in areas where the threat of piracy and armed robbery exists. Planning should give consideration to the crew's welfare during and after a period of captivity by pirates or armed robbers. Before operating in waters where attacks have been known to occur, it is imperative for shipowners, companies, ship operator and masters concerned to gather accurate information on the situation in the area. To this end the information on attacks and attempted attacks gathered, analyzed and distributed by the IMO, IMB's Piracy Reporting Centre and the ReCAAP Information Sharing Centre (ReCAAP ISC), the Maritime Security Centre, Horn of Africa, Governments and others is vital information, upon which precautionary measures should be based.

Note: For contents of (msc.1-circ.1334 - guidance to shipowners and ship operators' shipmasters and crews on preventing and suppressing piracy and armed robbery)

1.4.2 Government legislation and regulations

Some governments have acted on a national level to produce legislation and/or regulations concerned with measures to enhance maritime security. For instance, the United States government has the Maritime Transport Security Act of 2002 (MTSA 2002) and the Customs-Trade Partnership Against Terrorism (C-TPAT).

Some of the key features of the MTSA include:

- Requirements for port, facility, and vessel vulnerability assessments
- Preparation by the Secretary of Transportation of a National Maritime Transportation Security Plan and Area Plans for each U.S. Coast Guard Captain of the Port Zone
- Development of Security Plans for certain facilities and commercial vessels
- The issuance and use of Transportation Security Cards for personnel whose responsibilities require them to access secure places aboard ships
- Establishment of a permanent program of grants to facilitate the enhancement of maritime security
- Assessment by the Secretary of Transportation of the effectiveness of anti-terrorism measures at foreign ports
- Establishment of an enhanced system of foreign seafarer identification
- Creation of Maritime Security Advisory Committees at national and area levels
- Installation and operation of Automatic Identification Systems aboard certain commercial vessels
- Establishment of a program to better secure international intermodal transportation systems, to include cargo screening, tracking, physical security, compliance monitoring, and related issues
- Provisions of civil penalties for violation of statutes or regulations
- Extension of seaward jurisdiction of the Espionage Act of 1917 to 12 nautical miles offshore of the territorial sea baseline
- Codification of the U.S. Coast Guard Sea Marshall program and consideration of utilizing merchant mariners and other personnel to assist the Coast Guard
- Requirements that shipment data be provided electronically to U.S. Customs prior to arrival or departure of cargo
- Reporting by the Secretary of Transportation to Congress on foreign-flag vessels calling at the United States ports
- Development of standards and curricula for maritime security professional training

The **Customs-Trade Partnership Against Terrorism (C-TPAT)** is a program through which the U.S. Customs provides streamlined clearance of cargo to firms that establish appropriate security procedures. The Container Security Initiative (CSI) is another program in which U.S. Customs is working with foreign ports to identify potentially dangerous shipments before they arrive in the U.S.

1.4.3 Ship and port operations and conditions

OPERATIONS

- ✓ LOADING
- ✓ VOYAGE
- ✓ DISCHARGING
- ✓ EMBARKATION
- ✓ BUNKERING

CONDITIONS

People Access to the Ship
Ship Navigation and Operation
Cargo Handling
Ship Stores Handling
Security Monitoring
Emergency Responses

Intermodal Nature of Transportation and the Interfaces between Ships and other Modes

Intermodal freight transport involves the transportation of freight in an intermodal container or vehicle, using multiple modes of transportation (e.g., rail, ship, and truck), without any handling of the freight itself when changing modes. The method reduces cargo handling, and so improves security, reduces damage and loss, and allows freight to be transported faster. Reduced costs over road trucking is the key benefit for inter-continental use. This may be offset by reduced timings for road transport over shorter distances.

An intermodal transport chain is illustrated in figure below. In this example, loaded containers leave the shipper's facilities by truck to a railyard, where they are consolidated into a train and sent to another rail yard. Trucks are again used to transport the containers from this rail yard to the sea container terminal/ this last operation may not be necessary if the sea container terminal has an interface to the rail network, in which case freight is transferred directly from one mode to the other. Containers are then transported to a port on another continent by ocean shipping, from where they leave by either trucking or rail (or both) to their destinations.

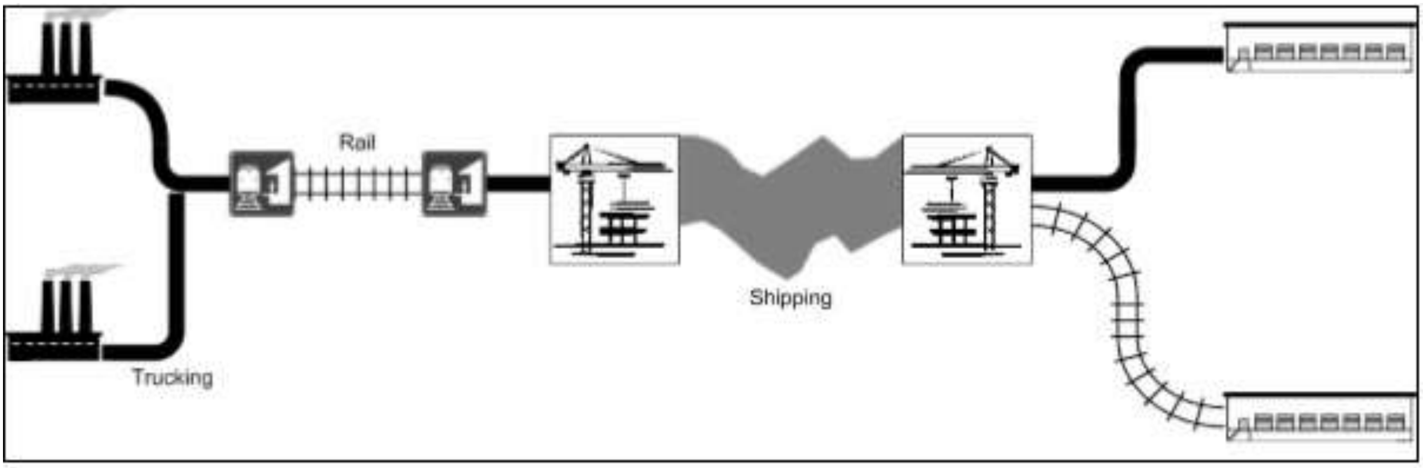


FIG. INTERMODAL TRANSPORT NETWORK

Role of a harbor as the interface between sea transport and other modes of transport

A ship will come to a harbor to do one or more of the following

- load and/or discharge cargo
- take on fuel ("to bunker")
- take on stores (food, deck stores or engine room stores)
- undergo repairs or maintenance (which may include drydocking)
- in the case of passenger ships, to land and embark passengers and to enable passengers to visit tourist sites.
- to land an injured or ill seafarer or to land survivors from a maritime accident

When in harbor during these ship/port operations, the following are the general points to be kept in mind:

- Checking the identity of all persons boarding/wanting to board the vessel
- Designated secure areas are established in liaison with the Port Facility Security Officer
- Segregate checked persons from those unchecked for ease of operation
- Segregating embarkation and disembarkation
- Identification of access points to be secured against unauthorized access
- Securing of areas that provide access to personnel
- Providing security briefings to all ship personnel on possible threats and the levels associated with the port
- Compliance with the Ship Security Plan at all times

1.4.4 Security responsibilities

1.4.4.1 Contracting Governments

- Subject to the provisions of regulation XI-2/3 and XI-2/7, 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:
  - the degree that the threat information is **credible**;
  - the degree that the threat information is **corroborated**;
  - the degree that the threat information is **specific or imminent**; and
  - the **potential consequences** of such a security incident

- When they set security level 3, issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected

- May delegate to a recognized security organization certain of their security related duties under SOLAS chapter XI-2 and Part A of the Code

- Test, to the extent they consider appropriate, the effectiveness of the Ship or 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.

1.4.4.2 Recognized Security Organizations

- Contracting Governments may authorize a Recognized Security Organization (RSO) to undertake certain security-related activities, including:
  - approval of Ship Security Plans, or any amendments, on behalf of the Administration;
  - verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of the Code on behalf of the Administration; and
  - conducting Port Facility Security Assessment required by the Contracting Government.

- May also advise or provide assistance to Companies or port facilities on security matters, including Ship Security Assessment, Ship Security Plans, Port Facility Security Assessment and Port Facility Security Plans.

1.4.4.3 Company

- Designate a Company Security Officer for the Company and a Ship Security Officer for each of its ships whose duties, responsibilities and training requirements are defined in Part A of the Code

- Shall ensure that the ship security plan contains a clear statement emphasizing the master's authority, i.e., that 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

- Shall ensure that the company security officer, the master, and the ship security officer are given the necessary support to fulfill their duties and responsibilities in accordance with SOLAS chapter XI-2 and Part A of the Code.

1.4.4.4 Ship

- Required to have, and operated in accordance with, a Ship Security Plan approved by, or on behalf of, the Administration

- Carry an International Ship Security Certificate indicating that it complies with the requirements of SOLAS chapter XI-2 and Part A of the Code

- Have onboard information, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship

1.4.4.5 Port Facility

- Port facilities shall comply with the relevant requirements of this chapter and part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

- Contracting Governments with a port facility or port facilities within their territory, to which this regulation applies, shall ensure that:

.1 port facility security assessments are carried out, reviewed and approved in accordance with the provisions of part A of the ISPS Code; and

.2 port facility security plans are developed, reviewed, approved and implemented in accordance with the provisions of part A of the ISPS Code.

- Contracting Governments shall designate and communicate the measures required to be addressed in a port facility security plan for the various security levels, including when the submission of a Declaration of Security will be required.

- Required to have, and operated in accordance with, a Port Facility Security Plan approved by the Contracting Government or the Designated Authority concerned

- Act upon the security level 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 interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

1.4.4.6 Ship Security Officer

- A Ship Security Officer shall be designated on each ship whose duties and responsibilities include, but are not limited to:
  - undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
  - maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
  - coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
  - proposing modifications to the ship security plan;
  - reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
  - enhancing security awareness and vigilance on board;
  - ensuring that adequate training has been provided to shipboard personnel, as appropriate;
  - reporting all security incidents;
  - coordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and
  - ensuring that security equipment is properly operated, tested, calibrated, and maintained.

1.4.4.7 Company Security Officer

- The Company shall designate a company security officer whose duties and responsibilities include, but are not limited to:
  - advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
  - ensuring that ship security assessments are carried out;

- ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- arranging for internal audits and reviews of security activities;
- arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;
- ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
- enhancing security awareness and vigilance;
- ensuring adequate training for personnel responsible for the security of the ship;
- ensuring effective communication and cooperation between the ship security officer and the relevant port facility security officers;
- ensuring consistency between security requirements and safety requirements;
- ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

▪ A person designated as the Company Security Officer may act as the company security officer for one or more ships provided it is clearly identified for which ships this person is responsible.

1.4.4.8 Port Facility Security Officer

▪ Designated for each port facility whose duties and responsibilities include, but are not limited to:

- conducting an initial comprehensive survey of the port facility, taking into account the relevant port facility security assessment;
- ensuring the development and maintenance of the port facility security plan;
- implementing and exercising the port facility security plan;
- undertaking regular inspections of the port facility to ensure the continuation of appropriate security measures;
- recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;
- enhancing security awareness and vigilance of the port facility personnel;
- ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- coordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- coordinating with security services, as appropriate;
- ensuring that standards for personnel responsible for security of the port facility are met;
- ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
- assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

1.4.4.9 Seafarers with Specific Security Duties

- 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, including as appropriate:
  - knowledge of current threats and patterns;
  - recognition and detection of weapons, dangerous substances and devices;
  - recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
  - techniques to circumvent security measures;
  - crowd management and control techniques;
  - security related communications;
  - knowledge of emergency procedures and contingency plans;
  - operations of security equipment;
  - testing, calibration and maintenance while at sea of security equipment and systems;
  - inspection, control and monitoring techniques; and
  - methods of physical searches of persons, personal effects, baggage, cargo and ship's stores.

1.4.4.10 Port Facility Personnel with Designated Security Duties

- Port facility personnel having specific security duties and responsibilities shall understand their responsibilities for port facility security as described in the port facility security plan and shall have sufficient knowledge and ability to perform their assigned duties, including as appropriate:

  - knowledge of current threats and patterns;
  - recognition and detection of weapons, dangerous substances and devices;
  - recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
  - techniques to circumvent security measures;
  - crowd management and control techniques;
  - security related communications;
  - knowledge of emergency procedures and contingency plans;
  - operations of security equipment;
  - testing, calibration and maintenance while at sea of security equipment and systems;
  - inspection, control and monitoring techniques; and
  - methods of physical searches of persons, personal effects, baggage, cargo and ship's stores.

1.4.4.11 Other Personnel

- Crew members of the ship and other port facility personnel who attended security training awareness and security drills in response to all security levels set under the ISPS code also have roles in ensuring that the security plans work and will help recognize areas for enhancement of maritime security.

- Use of unarmed security personnel

The use of unarmed security personnel is a matter for individual shipowners, companies, and ship operators to decide. The use of unarmed security personnel to provide security advice and an enhanced lookout capability could be considered.

- Use of privately contracted armed security personnel

If armed security personnel are allowed on board, the master, shipowner, operator and company should take into account the possible escalation of violence and other risks. However, the use of privately contracted armed security personnel on board merchant ships and fishing vessels is a matter for flag State to determine in consultation with shipowners, operators and companies. Masters, shipowners, operators and companies should contact the flag State and seek clarity of the national policy with respect to the carriage of armed security personnel. All legal requirements of flag, port and coastal States should be met.

- Role of military, industry and intergovernmental organizations in the prevention, suppression and reporting of piracy and armed robbery against ships [as indicated in MARINA outline]

Military teams or law enforcement officers duly authorized by Government

The use of military teams or law enforcement officers duly authorized by the Government of the flag State to carry firearms for the security of merchant ships or fishing vessels is a matter for the flag State to authorize in consultation with shipowners, operators and companies. The carriage of such teams may be required or recommended when the ship is transiting or operating in areas if high risk. Due to rules of engagement defined by their Government, or in coalition with other Governments, boarding conditions should be defined by the States involved, including the flag State. The shipowner, operator and company should always consult the flag State prior to embarking such teams.

1.5 Maritime security levels

The ISPS Code identifies three Maritime Security (MARSEC) levels which describe the security threat that a country and its coastal region are facing. The local government sets the security level with the help of ship and port authority.

MARSEC Level 1

The **normal level** that the ship or port facility operates on a daily basis. Level 1 ensures that security personnel maintains minimum appropriate security 24/7.

In this level, all those liable to board must be searched. The frequency of the same should be specified in the SSP. Such searches are to be carried out in coordination with the port facility. It is important to remember the human rights angle of the individual being searched and the search should not violate their dignity.

- Minimum security measures are always maintained on board and in port
- Ship and port operation is carried out as per ship and port facility security plan
- Port facility ensures to keep the ‘no access’ areas under surveillance at all times
- Ship and port authority mutually supervise loading and unloading operation of cargo and stores, ensuring access control and other minimum-security criteria.
- Minimum access in the ship is maintained at all times.

MARSEC Level 2

A **heightened level for a time period** during a security risk that has become visible to security personnel. Appropriate additional measures will be conducted at this security level.

At this level, the SSP should establish the measures to be applied to protect against the heightened risk. Higher vigilance and tighter control with regard to the security of the ship is in play here.

- Assigning additional personnel for patrolling the access areas
- Deterring waterside access to the ship
- Establishing a restricted area on the shore side of the ship
- Increasing the search frequency and detail of the persons due to board or disembark
- Escorting all visitors onboard
- Additional security briefings to the ship's personnel with emphasis in relation to the security level
- Carrying out a full or partial search of the ship

MARSEC Level 3

Will include **additional security measures** for an incident that is forthcoming or has already occurred that must be maintained for a limited time frame. The security measure must be attended to although there might not be a specific target that has yet been identified.

Again, the SSP should be adhered to and with strong liaison with the port facility. The following measures should be put in place with the highest degree of vigilance and detail:

- Limiting access to a single, controlled access point
- Granting access strictly to authorized personnel or those responding to any security incident
- Suspension of embarkation and disembarkation
- Suspension of cargo operations and stores etc.
- If needed, the evacuation of the ship
- Close monitoring of the movement of the people on board
- Preparing for a full or partial search of the ship

1.6 Security reporting procedures

The Ship Security Officer should and is responsible for reporting all security incidents to the CSO, PFSO, and the contracting governments as specified in the code.

Security incidents generally can fall into two categories:

.1 those considered to be sufficiently serious that they should be reported to relevant authorities by the CSO, including:

- Unauthorized access to restricted areas within the ship for suspected threat-related reasons
- Unauthorized carriage or discovery of stowaways, weapons or explosives
- Incidents of which the media are aware
- Bomb warnings
- Attempted or successful boardings
- Damage to the ship caused by explosive devices or arson

.2 those of a less serious nature but which require reporting to, and investigation by the SSO, including:

- Unauthorized access to the ship caused by breaches of access control points
- Inappropriate use of passes
- Damage to equipment through sabotage or vandalism
- Unauthorized disclosure of a ship security plan
- Suspicious behavior near the ship when at a port facility
- Suspicious packages near the ship when at a port facility
- Unsecured access points to the ship

Ship security plans shall address procedures for responding to security threats or breaches of security, including:

.1 Provisions for maintaining critical operations of the ship/port interface; and
.2 Procedures for reporting security incidents

Reporting requirements for ships prior to entering port

Ships intending to enter ports of [State] may be required to provide the following information prior to entry into port:

- 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 any previous port where it has conducted a ship/port interface within a specified time frame;
- any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within a specified time frame;
- that the appropriate ship security procedures were maintained during any ship-to-ship activity within a specified time frame; or
- other practical security-related information (not to include details of the ship security plan).

Examples of other practical security-related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

- information contained in the continuous synopsis record;
- location of the ship at the time the report is made;
- expected time of arrival of the ship in port;
- crew list;
- general description of cargo aboard the ship;
- passenger list; and
- information required to be carried under SOLAS regulation XI-2/5.

1.7 Security drills and exercises

Drill and exercise requirements.

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.

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 relevant circumstances, taking into account the guidance given in the ISPS Code.

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.

Exercises.

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.

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.

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

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

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.

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

Drills and Training for Rest of Ship's Crew

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.

1.8 Ship security actions

- **Security measures and procedures aboard ship**

The **Ship Security Plan (SSP)** should establish security measures that could be undertaken at each security level covering the following:

1. *Access to the ship by ship's personnel, passengers, visitors, etc.*

   – At **security level 1**, SSP should establish the security measures to control access to the ship, which may include the following:

   - Checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, e.g., joining instructions, passenger tickets, boarding passes, work orders, etc.;

- In liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage, personal effects, vehicles and their contents can take place;
- In liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro, and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;
- Segregating checked persons and their personal effects from unchecked persons and their personal effects;
- Segregating embarking from disembarking passengers;
- Identification of access points that should be secured or attended to prevent unauthorized access;
- Securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and
- Providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

- At **security level 2**, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:
  - Assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;
  - Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;
  - Deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;
  - Establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;
  - Increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;
  - Escorting visitors on the ship;
  - Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and
  - Carrying out a full or partial search of the ship.

- At **security level 3**, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:
  - Limiting access to a single, controlled, access point;
  - Granting access only to those responding to the security incident or threat thereof;
  - Directions of persons on board;
  - Suspension of embarkation or disembarkation; suspension of cargo operations, deliveries etc;
  - Evacuation of the ship;
  - Movement of the ship; and
  - Preparing for a full or partial search of the ship.

- Recommended actions in response to attacks and attempted attacks by pirates and armed robbers

Suspected piracy/armed robbery vessel detected

- Early detection of suspected attacks must be the first line of defense. If the vigilance and surveillance has been successful, a pirate/armed robbery vessel will be detected early.
- The ship's crew should be warned and, if not already in their defensive positions, they should move to them.
- Appropriate passive and active measures, such as evasive maneuvers and hoses should be vigorously employed as detailed in the preparation phase or in the ship's security plan.
- Shipowners, company, ship operator and master should be aware of any UN Security Council, IMO or any other UN resolutions on piracy and armed robbery against ships and any recommendations therein relevant to the shipowner, operator, master and crew when operating in areas where piracy or armed robbery against ships occur.

Being certain that piracy/armed robbery will be attempted

- If not already in touch with the security forces of the littoral coastal State, efforts should be made to establish contact.
- Crew preparations should be completed and, where a local rule of the road allows ships under attack to do so, a combination of sound and light signals should be made to warn other ships in the vicinity that an attack is about to take place.
- Vigorous maneuvering should be continued and maximum speed should be sustained if navigation conditions permit.
- Nothing in these guidelines should be read as limiting the master's authority to take action deemed necessary by the master to protect the lives of passengers and crew.

Pirate/armed robbery vessel in proximity to, or in contact with, own ship

- Vigorous use of hoses in the boarding area should be continued. It may be possible to cast off grappling hooks and poles, provided the ship's crews are not put to unnecessary danger.
- While giving due consideration to safety of crew, vessel and environment it is recommended that masters should not slow down and stop, as far as practicable, when pursued by or fired upon by pirates/armed robbers intending to board and hijack the vessel.
- Where the pirates/armed robbers operate from a mother ship, masters should consider steering away from the mother ship thus increasing the distance between the attacking craft and the mother ship.

- Preventing Pirate Attacks

Fortunately, there are tools and techniques for avoiding, preventing and surviving pirate attacks. A satellite system allows shipping companies to monitor the location of their ships. This can be particularly useful if pirates hijack or steal a ship. Companies can also install non-lethal electrical fences around a ship's perimeter, as long as that ship does not carry flammable cargo. In addition, International Maritime Organization regulations require ships to be able to send distress signals and warnings covertly in case of pirate attack.

To prevent pirate attacks, crews should:

- Avoid discussing a ship's route or cargo while in port
- Keep constant watch in areas prone to piracy

- Avoid bottlenecks in shipping lanes
- Search the ship before leaving port to make sure no one is on board without authorization

The best defense against a pirate attack is evasion -- it's easier to keep pirates from boarding than to force them to leave. Upon detecting the approach of pirates, a crew should:

- Call for help and warn other ships in the area
- Take evasive action and attempt to out-maneuver the attackers
- Sound the alarm, use the ship's lights to illuminate the vessel, and do anything else to make the pirates aware that they have lost the element of surprise

If the pirates approach the ship, the crew should first try to throw off any grappling hooks or poles before the pirates can board. Crew can also use the ship's fire hoses to deter pirates or try to push them overboard. However, experts discourage crew members from carrying firearms, since the presence of weapons can encourage attackers to respond with violence.

Once the pirates board the ship, the crew's first priority is to ensure their own safety. The crew should also try to stay in control of the craft and encourage the pirates to depart.

1.9 Ship Security Assessment

Under the International Ship and Port Facility Security Code (ISPS), every shipping company must take certain steps into consideration to ensure security of the crew, ship and environment.

Several plans and procedures have been introduced to ensure utmost security of the ship and its crew.
A ship security plan (SSP) is a must for every ship under the ISPS Code.

Moreover, in order to ensure that every ship follows all the protective measures specified in the SSP, a Ship Security Assessment is carried out by the concerned authority.

The ship security assessment (SSA) is generally carried out before making the ship security plan (SSP).

The chief security officer (CSO) checks that the people with the necessary skills carry out the ship security assessment.

The ship security assessment (SSA) includes an on-scene security survey which includes:

1. Identification and evaluation of key shipboard operations which require additional care while carrying out

Under key shipboard operations, critical processes such as cargo handling, navigation, machinery handling etc. are taken into consideration for evaluation. Along with that, critical spaces such as stores, bridges, machinery spaces, and steering control system are also taken into consideration.

2. Identification of existing security measures and procedures

Under security measures, procedures such as response to emergency conditions, security patrol, security communication systems, handling of surveillance equipment, including door barriers and lightings are taken into account.

3. Identification of weakness in policies, procedures, and infrastructure

On the basis of identification of various other aspects, a list of objectives would be detailed such as new security measures to be implemented, determination of mitigation strategy etc.

4. Identification of human factors that can be a threat to safety and security of the ship

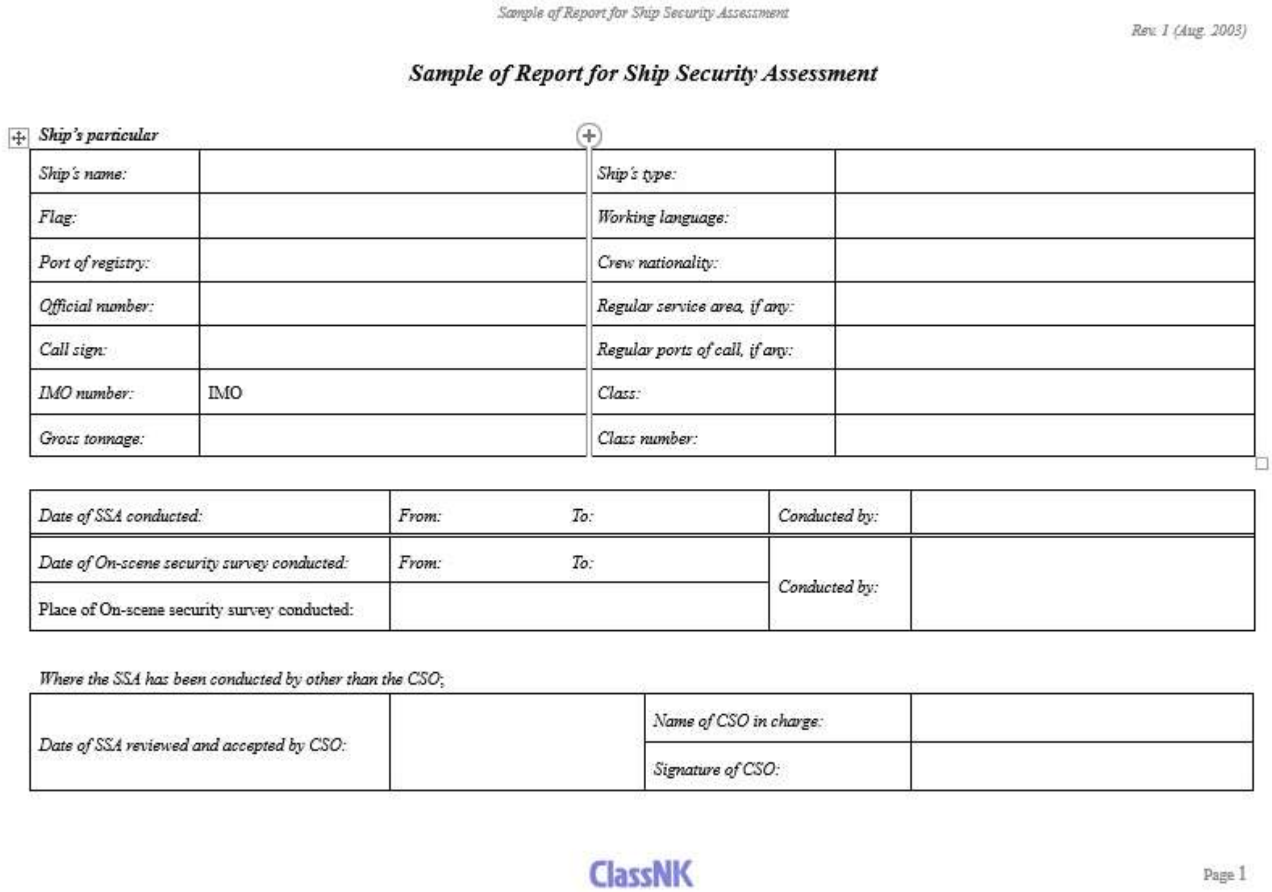
Shipboard protective measures, procedures, and operations are evaluated to identify possible weakness pertaining to human factors.

Aspects such as monitoring of restricted areas to ensure only authorized persons are allowed, ensuring performance of security duties, supervising and handling of cargo etc. are taken into consideration to identify such factors.

5. Identification of potential threads and likelihood of their occurrence

Under this, the company identifies various threat scenarios to a ship under specific circumstances. Threat scenarios would be considered keeping in mind various aspects of the ship such as types of ship, crew, type of cargo etc.

Ship Security Assessment Checklist



Sample of Report for Ship Security Assessment

Rev. 1 (Aug. 2003)

Sample of Report for Ship Security Assessment

Ship's particular

Ship's name:		*Ship's type:*	
Flag:		*Working language:*	
Port of registry:		*Crew nationality:*	
Official number:		*Regular service area, if any:*	
Call sign:		*Regular ports of call, if any:*	
IMO number:	IMO	*Class:*	
Gross tonnage:		*Class number:*	

Date of SSA conducted:	*From:* *To:*	*Conducted by:*	
Date of On-scene security survey conducted:	*From:* *To:*	*Conducted by:*	
Place of On-scene security survey conducted:			

Where the SSA has been conducted by other than the CSO;

Date of SSA reviewed and accepted by CSO:		*Name of CSO in charge:*	
		Signature of CSO:	

ClassNK

Page 1

The vessel owner and operator have the primary responsibility for ensuring the physical and safety of their vessel. Therefore, **in addition to meeting the requirements of the ISPS Code**, the SSA should also prepare a means to promote sound security practices. The SSA is an essential and integral part of the process of developing and updating the Ship Security Plan (SSP).

Appreciating that every ship is unique – in design, operations, cargo, voyage pattern, etc. – a ship owner/operator may wish to demonstrate that specific recommended security measures are not appropriate for his specific ships.

Owners/operators are to balance the security measures by evaluating his ship's:

- Key shipboard operations
- Existing security measures
- Assessed threats, and
- Consequences and/or vulnerability (risk)

It should be recalled that achieved security is highly dependent on the human element. Vigilance, prevention and response can only be as good as the crew's skills, knowledge experience and attitude related to security.

On-Scene Security Survey

The on-scene security survey is an integral part of any Ship Security Assessment.

List of preparations required prior to an on-scene security surveys are as follows:

- ✓ General Information of the ship
- ✓ Contributing Factors such as Trade patterns, route, ports, flag and cargo
- ✓ Existing security measures and equipment
- ✓ Threat evaluation and risk assessment and weaknesses

The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

- ✓ Ensuring the performance of all ship security duties;
- ✓ Monitoring restricted areas to ensure that only authorized persons have access;
- ✓ Controlling access to the ship, including any identification systems;
- ✓ Monitoring of deck areas and areas surrounding the ship;
- ✓ Controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
- ✓ Supervising the handling of cargo and the delivery of ship's stores; and
- ✓ Ensuring that ship security communication, information, and equipment are readily available
- ✓ 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 shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- ✓ Identification of weakness, including human factors in the infrastructure, policies and procedures.

Security aspects of a ship's layout are identified and the most critical operations, systems, areas and personnel to protect, with respect to a security incident, are prioritized.

The survey is divided into the following sections:

- ✓ Physical Security
  Physical security aboard ship is a part of risk management that is concerned with physical obstacles disposed in depth to frustrate attempts to penetrate the security defenses.

- ✓ Structural Integrity
  It is of vital importance to know the significance of structural integrity for ships and other structures in accessing the ship's vulnerability—that is, to know that the "why," "how," "when," and "where" factors apply to the effectiveness of such particular condition.

- ✓ Personnel Protection System
  The following are the components and operations of systems to protect shipboard personnel:

  - Access Control
  - Ship Security Alert System
  - Security Equipment, if available

- ✓ Procedure Policies
  Putting in place the proper procedures and effectively implementing such will prevent and mitigate security incidents. These include assessment of the ship's vulnerability to threats, in terms of likelihood and potential consequences taking into account motives, existing measures and critical operations when assessing the likelihood and potential outcome of the scenarios.

- ✓ Radio and Telecommunication Systems
  The proper usage of GMDSS and information technology on board ship will help the contracting government and company to respond quickly in case the vessel is under threat or attack. The activation of the alert system through INMARSAT system, from Mini-M unit and on VHF and hand-held transceivers on coded messages is a typical sample.

- ✓ Other areas
  Proper training in security awareness is mandatory to all crew to be able to identify security risk areas around the ship or within a port facility. One identified area is the ship's access point.

  Establish a table for identification of vulnerabilities and criteria based on the example scenario, as well as table for counter-measures (mitigation) that will be developed to reduce risk for that scenario.

It is of paramount importance to have in place the emergency plans that deal with contingencies. When emergency plans are in place, the ship personnel function more effectively in an organized environment.

1.10 Emergency preparedness, drills and exercises

– Execution of Contingency Plans

In case of breach of security, the SSO shall evaluate, review and amend the security measures specified in the ship security plan.

Hijacking- If in case hijackers were already in control, all crew should cooperate with the Hijackers, give them whatever they want and should treat them in a “Seamanlike Manner” to prevent loss of life, ship, cargo, or environmental catastrophe.

Bomb Threat- All crew should know the drills for the response to such threat, like thorough search of the bomb around the ship or evacuation of crew if bomb has been discovered.

Unidentified Objects/Explosives on Vessel- Crew should not touch nor move the suspected objects, immediately call the PFSO to inform bomb squad and evacuate the area.

Damage to/Destruction of Port Facility- ship should immediately leave the port facility, stay in a safe area and wait for further instructions from the CSO or Contracting Government.

Piracy- Anti-piracy watch should be exercised as stated in ship’s anti-piracy guide. However, if heavily armed pirates had boarded the ship, the crew must stay calm, act in full cooperation with the pirates, which is a “Must,” and act in a “Seamanlike” manner. The safety of the crew, ship, and its cargo is the primordial concern.

Stowaways- Thorough search for stowaways will be carried out prior departure from port. However, if stowaways have been found after ship had left the port for some time, treat them fairly in accordance with IMO guidelines regarding stowaways until they are repatriated to their home country. While in port, stowaways should be confined in a secured cabin to prevent them from deserting.

2. SECURITY RISKS AND THREATS

2.1 Security documentation

Documents and records for ship security shall be kept on board at all times.

A verification of the ship’s security system and any associated equipment will be made to ensure that the ship fully complies with applicable requirements of the ISPS Code and is in satisfactory condition and fit for service for which the ship is intended. Such verification shall be endorsed on an **International Ship Security Certificate.** This certificate shall be issued for a period specified by the Administration, which shall not exceed five years. The verification of ships shall be carried out by officers of the Administration or a Recognized Security Organization (RSO).

Every ship shall be issued with a **Continuous Synopsis Record.** This record is intended to provide an on-board record of the history of the ship. This shall be issued by the Administration to each ship that is entitled to fly its flag and shall contain the following:

- ✓ Flag of the ship
- ✓ Date of registry
- ✓ Ship's identification number (Reg.3)
- ✓ Ship's name
- ✓ Port of registry
- ✓ Registered owners and their addresses
- ✓ Registered charterer(s) and their addresses
- ✓ Registered safety management company and the addresses
- ✓ All classification society(ies) with which the ship is classed
- ✓ Administration or Contracting Government or recognized organization which has issued the Document of Compliance to the Company operating the ship and the name of the body which has carried out the audit
- ✓ Administration or Contracting Government or recognized organization that has issued the Safety Management Certificate and the name of the body which has carried out the audit
- ✓ Administration or Contracting Government or the recognized security organization that has issued the International Ship Security Certificate and name of the body which has carried out the verification
- ✓ Date on which the ship ceased to be registered with the State

Records of the following activities addressed in the ship security plan shall be kept on board for the minimum period, as specified by the Administration.

Declaration of Security

The Declaration of Security is a document that may be required for a port visit when specific security requirements exist. The Declaration address the security requirements that could be shared between a port facility and a ship, or between ships, and states the responsibility for each.

What determines if a Declaration of Security is required?

A Government shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses

A ship can request completion of a Declaration of Security when:

- The ship is operating at a higher security level than the port facility or another ship it is interfacing with
- There is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages
- There has been a security threat or a security incident involving the ship or involving the port facility
- The ship is at a port which is not required to have and implement an approved port facility security plan
- The ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan

Who completes the Declaration of Security?

- The master or the ship security officer on behalf of the ship(s); and, if appropriate,
- 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

2.2 Techniques to circumvent security measures

Having a good plan, though essential to the ship's security, is not enough. Diligence of the crew in implementing the plan is just as important. The best defense against terrorists and criminals is good security awareness and observation on the part of all crew.

Ship Security Officers should be cautioned that no security equipment or measure is perfect. They should be appraised for known techniques that can be employed to penetrate and break the security systems and controls such as the disabling of alarm systems, picking of locks, jamming of radio signals, etc.

– Indicators that security measures are circumvented

- Interference or jamming and monitoring of the ship's communications system. Efforts made to broadcast over the system, damage the radio transmitter or antenna, or cut telephone lines are often the first indication that an attack is imminent.
- Damage to locks and doors such as scratches around the locks.
- Lost or stolen keys.
- Normally locked doors being found open for no reason.
- Dirty finger marks on clean doors or windows, or clean marks on dirty doors.
- False alarms on security systems. The criminal or terrorist may be testing the response time and reaction procedures, or trying to incapacitate the alarm system.
- Apparently wanton, or accidental damage to essential equipment. This may be an indicator that an attempt is about to be made to attack the ship.

- Methods used by pirates and armed robbers to attack ships

– Pirates Usually Attack at Night or Early Morning

Though armed with the most modern weaponry, the modern-day pirates still use small motorized fishing boats which are fast and too small to get detected by the ship's radar system. When these boats are used by the pirates, generally at night, they are literally invisible to the ship's crew. The pirates wait in these small boats, under the darkness of night, and speed up as soon as they see a big ship coming their way.

From piracy attacks in the past, it is said that **pirates generally attack the ship from its astern side**, using ropes attached with hooks at one end. Some of the pirates also use long bamboos to attach the ropes with hooks on the ship's side. Some pirates have also been seen using light ladders made out of wood and bamboo. The pirates are really fast with these activities and aboard the vessel way before the ship's crew realizes and raises the alarm.

Although all the huge cargo and tanker vessels are basically too high to climb, when fully loaded, these vessels move quite low with a fairly high draught. This makes it even easier for the pirates to board the ships. Moreover, **most of the piracy attacks mainly take place near to the shoreline using small speed boats.** However, some of the recent piracy attacks have even taken place at a distance of three to four hundred nautical miles from the shore. In such cases, pirates use a bigger mother ship and anchor is near the sea route. When the targeted ship arrives, they use small power boats to attack the ship.

– Use of Modern Weapons

Present day pirates are using the best of modern technology to assist them in their piracy attacks. Equipped with the most modern and automatic weapons such as AK-47 rifles and rocket propelled grenades (RPGs), the pirates mercilessly and aimlessly fire on the targeted ship.

Though huge in size, the ships are both defenseless and helpless in front of these lethal weapons. In many piracy attacks in the past, the pirates have opened fire on the cargo ships to bring them to a halt. The master of the ship has no option other than slowing down the ship or stopping it, allowing the pirates to come on board.

– Defenseless Ships, Defenseless Crew

Thus, technically, a merchant ship in Somali waters is a sitting duck, waiting to be hit by the pirates. Unless and until any substantial step is taken to fight the growing piracy activities in Somalia waters, merchant ships will always remain an easy target for the modern-day pirates.

2.3 Potential security threats

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

Suspicious patterns of behavior while emphasizing the importance of avoiding racial profiling and ethnic stereotyping. These include the following:

✓ Unknown persons photographing vessels or facilities

✓ Unknown persons attempting to gain access to vessels or facilities

✓ Suspicious individuals establishing business or roadside food stands either adjacent or in proximity to facilities

✓ Unknown persons loitering in the vicinity of ships or port facilities for extended periods of time

✓ Unknown persons telephoning facilities to ascertain security, personnel, or standard operating procedures

✓ 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

✓ Suspicious general aviation aircraft operating in proximity to vessels or facilities

✓ Suspicious 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
- ✓ Suspicious vendors attempting to sell merchandise
- ✓ Unknown or suspicious workmen trying to gain access to facilities to repair, replace, service, or install equipment
- ✓ Suspicious emails on internet, public affairs attempting to obtain information regarding the facility, personnel, or standard operating procedures
- ✓ Suspicious 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
- ✓ Repeated or suspicious out-of-ordinary phone calls
- ✓ Recreational boaters posing as mariners in distress to attract other vessels

- **Preventing Theft and Other Criminal Activities for Ships in Port**

  Individual criminal motive alone cannot turn into a crime without opportunity and the means. All (motive, opportunity and means) need to come to together for crime to happen. Individual motive cannot be controlled, means is difficult to control, but opportunity can be controlled. So the security measure must focus on the opportunity to minimize it as much as possible to affect the final result. Necessary measures must be put in place to make sure those opportunities, which will encourage crime, is reduced. If the opportunities for the attack or criminal activities are minimized considerably, then the criminal will be discouraged from focusing on the port facility, person or the vessel being protected.

2.4 Recognizing weapons, dangerous substances and devices

Various weapons, dangerous substances and devices, the damage they can cause, and appearance are as follows:

- **Handguns, Rifles, Shot Gun**

Handguns are generally small and suitable for concealed carriage. There are extremely small handguns called “Delinger” which has single loaded capacity. Some are all light-weight plastic or polymer. It is very difficult to detect using an X-ray machine or metal detector.

Rifles are considered to be bulky. However, recent military assault rifles are considerably small and easy to disassemble. As for shotguns, some are with barrels cut short for concealed carriage.

Bullets

Full-metal jacket bullets have good piercing capability. However, in case the bullet hits the human body, there would be considerable energy loss (as it penetrates), and the damage to the human body may tend to be relatively small.

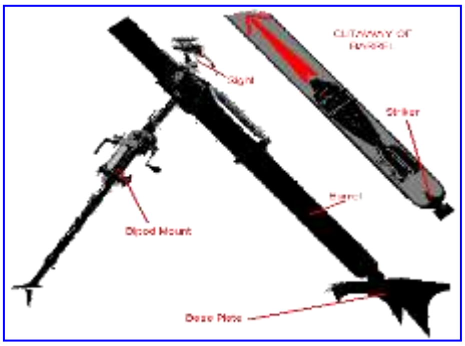
Semi-metal hollow point bullets are widely used, which once they hit the human body, the bullets are deformed in a mushroom shape expanding diameter, thus giving a bigger damage to the human body.

Spandau, Vickers and Parabellum kits include 6-inch long ammo belt. Belts available separately.

Heavy Arms

The following may be used by terrorists:

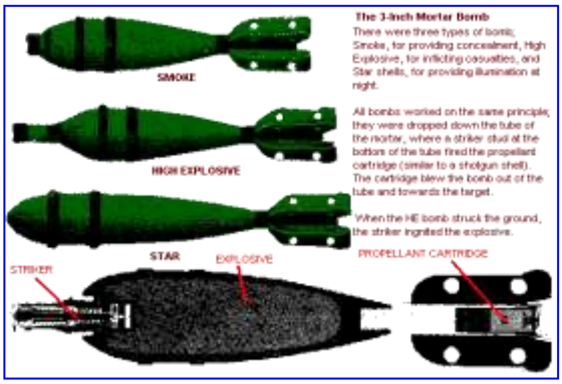
Light/ heavy machineguns
Recoiled Propelled Grenade (RPG)
Missiles
Non-recoil guns



Explosives

Military explosives such as grenades, plastic-bonded explosives, industry explosives such as dynamites or handmade explosives made of fireworks are used.

Military explosive gives strong destruction power, but even handmade explosives, if there is a mass of them, can have catastrophic destruction power.



The 3-inch Mortar Bomb

There were three types of bomb; Smoke, for providing concealment, High Explosive, for inflicting casualties, and Star shells, for providing illumination at night.

All bombs worked on the same principle; they were dropped down the tube of the mortar, where a striker stud at the bottom of the tube fired the propellant cartridge (similar to a shotgun shell). The cartridge blew the bomb out of the tube and towards the target.

When the HE bomb struck the ground, the striker ingnited the explosive.

Dynamite

Normally, one piece is 80100 g and has tendency to have stronger effect when used in an enclosed space. 3kg of dynamite (30-40 packs) is said to destroy a car totally.

Grenade

It can kill personnel within the 2m radius of its explosion

Plastic bonded explosives

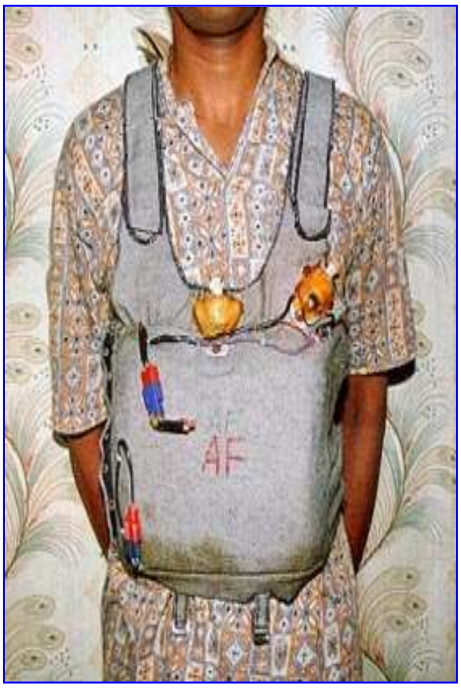
The explosive can cause a high-velocity explosion stream (8750m/sec), which is very strong. C-4 has off white color or light brown color; Semtex has dark gray color.

Vehicle bomb

If a truck/van are used with fully-loaded explosives, the whole building may have collapsed. If such devices are used in piers, considerable damage could cause to a ship alongside.

Incendiary Bombs

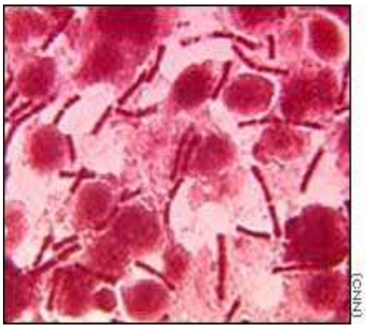
Flame bomb (filling gasoline into a bottle) for throwing to the target, or one with timing devices are reported.



NBC (Nuclear, Biological and Chemical weapons)

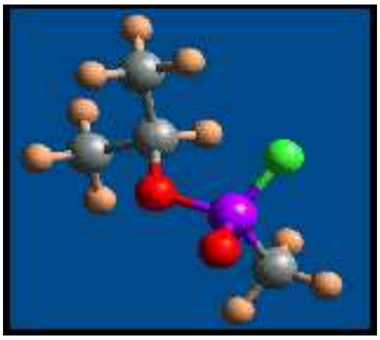
A possibility of NBC attack can't be totally eliminated. It is believed that terrorist groups have already obtained these materials.

As for biological weapons, anthrax virus, botulinos virus, and small fox virus, are possible weapons.



ANTHRAX

SARIN GAS



2.5 Crowd management and control techniques

Ship Security Officers should be familiar with the basic patterns of behavior of people in groups during time of crisis. Demonstrate to learners about the proper way to control the crowd on board in case there is a bomb threat. The critical importance of clear communication with the vessel personnel, port facility personnel, passengers, and others involved should be underscored.

A crisis refers not necessarily to a traumatic situation or event, but to a person's reaction to an event. One person might be deeply affected by an event while another individual suffers little or no ill effects. A crisis presents an obstacle, trauma, or threat.

Situational crises are sudden and unexpected, such as accidents and natural disasters.

Crowd control management is a specific training program that all individuals of a ship's crew need to learn. Crowd safety, is not just about trying to merely control the crowd, it involves using the right kind of communication and effectuating the perfect leadership skills to manage the crowd. This is why the crowd control safety program has been recommended by the STCW stipulations.

In case of any emergency, panic is the first reaction. In cruise ships, in case of complications, the element of panic will be on the higher side. This is why crowd managers in cruise ships need to have the knowledge to pacify the crowd and provide with them with the necessary information, in a manner that does not cause them to panic further.

Leadership skills, also is an aspect devoted to in the crowd control for cruise ships program. A leader is a person who is able to guide others without being rude and incoherent. In a situation of extreme exigency, the people in the cruise ship will want to listen to someone who is able to give them clear instructions and reason things in the calmest manner.

Understanding the psyche is another area where the safety program looks into. In a cruise ship, lots of people are around so the problem of communication differences and other minor conflicts arising is but natural. Crew members need to pay close attention to people so that they can prevent such conflicts from arising and thereby avoid a stressful scenario.

2.6 Handling security-related information and security-related communication

Security information and communication have certain sensitivity according to the prevailing levels of security. 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.

To safeguard maritime interests against unlawful acts which threaten the security of passengers and crews on board ships, reports on incidents and the measures taken to prevent their recurrence should be provided to the authorities as soon as possible. This information will be used in updating or revising these agreed measures, as necessary.

The individual circumstances of any particular incident may require a departure from this guidance to achieve the overall primary objective of personnel safety. Mention of the difference should be contained in any incident report in order to ensure that guidance can be continually improved and kept up to date.

2.7 Physical searches and non-intrusive inspections

It is well noted that, unless there are clear security grounds, crew members should not be required to search their colleagues or their personal effects. It should be conveyed that any search shall be undertaken in a manner that fully takes into account the human rights of the individual and preserves his/her basic human dignity.

A physical search is always conducted in the most professional and respectful manner possible. A physical search:

- Is always done by a screening officer of the same gender as the passenger. In exceptional situations, when a screening officer of the same gender is not available, alternative screening options will be offered.
- Is usually performed over clothing, though the screening officer may need to move, shift or slightly lift clothing during the search.
- Is safe and hygienic; screening officers must wear gloves during the search, and you can ask the officer to change gloves before your search.
- May be performed in a private search room. If you choose this option, one screening officer of the same gender as you will carry out the search. A witness (of the same sex as the person being searched, if possible) will also be present. Witnesses will be a screening officer or another independent third-party witness (e.g. airline representative, airport security personnel, police officer). Bring all of your personal belongings with you so they don't get lost or stolen.

All passengers need to be searched regardless of age. Physical searches may only be conducted by screening officers of the same gender as the person who is being searched.

- **Infants:** The gender of the parent or guardian is the determining factor, not the gender of the child.
- **Younger than 12 years of age:** A witness of the same gender is needed. Witnesses will be a screening officer or another independent third-party witness (e.g. airline representative, airport security personnel, police officer). A parent, guardian or airline representative must also observe the search.

- **12 to 15 years of age:** A guardian, family member or escort may observe a private physical search. Such passenger-requested observers do not replace the requirement for screening personnel or an independent third-party witness.

3. REGULAR SECURITY INSPECTIONS OF THE SHIP

3.1 Execution of security procedures

- **Regular security inspections**

It is a requirement for the SSP to carry out regular security inspections:

- ✓ Gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments,
- ✓ Requiring the maintenance of communication protocols for ships and port facilities,
- ✓ Preventing unauthorized access to ships, port facilities, and their restricted areas,
- ✓ Preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities,
- ✓ Providing means for raising the alarm in reaction to security threats or security incidents,
- ✓ Requiring ship and port facility security plans based upon security assessments, and
- ✓ Requiring training drills and exercises to ensure familiarity with security plans and procedures.

- **Security measures and procedures per security level**

The following security procedures are implemented when conducting a security assessment with new measures in place:

- ✓ Review and ensuring the performance of all security duties
- ✓ Monitoring controlled/restricted areas
- ✓ Controlling access to the vessel and to deck areas
- ✓ Controlling embarkation of persons and their effects
- ✓ Supervising the handling of cargo and delivery of stores
- ✓ Ensuring that ship security communication, information and equipment are readily available
- ✓ After performing above items and observing that vulnerabilities were reduced, there will be no further mitigating measures to apply.

Note: There may be other kinds of security procedures to follow that are not included in the list.

a. Controlling access to the ship

Access to the Ship

The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include the following:

.1 Access ladders,
.2 Access gangways,
.3 Access ramps,
.4 Access doors, side scuttle, windows and ports,
.5 Mooring lines and anchor chains, and
.6 Deck Cranes and hoisting gears

For each of these, the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security levels the SSP should establish the type of restrictions or prohibitions to be applied and the means of enforcing them.

Security Level 1: Access to the Ship

- ✓ Checking the identity of all persons seeking to board the ship and confirm their reason for doing so by checking their boarding permit, crew embarkation order, work orders, and passenger ticket,
- ✓ In liaison with the port facility officer, the ship should ensure that the designated access points are provided with security staff or personnel,
- ✓ Locking or securing access points,
- ✓ Using surveillance equipment to monitor the areas,
- ✓ Using guards or patrols, and
- ✓ Using automatic intrusion-detection devices to alert the ship's personnel of unauthorized access.

Security Level 2: Access to the Ship

- ✓ Assigned additional personnel to patrol deck areas to deter unauthorized access,
- ✓ Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them,
- ✓ Deterring waterside access to the ship (sea-side), in liaison with the port facility officer,
- ✓ Establishing a restricted area on the shore side of the ship, in closed co-operation with the port facility officer,
- ✓ increasing the frequency and details of searches of persons, personnel effects, and vehicles being loaded on to the ship,
- ✓ Escorting visitors onto the ship,
- ✓ Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance,
- ✓ Carrying out full or partial search of the ship.

Security Level 3: Access to the Ship

- ✓ Limiting access to a single, controlled access point,
- ✓ Granting access only to those responding to the security incident or threat thereof,
- ✓ Directing persons on board,
- ✓ Suspension of embarkation/disembarkation,
- ✓ Suspension of cargo operation, store deliveries and bunkering operation,
- ✓ Evacuation of the ship,
- ✓ Movement of the ship,
- ✓ Preparing for a full or partial search of the ship.

b. Controlling embarkation of persons and their effects

The Company Security Officer has established the following procedures to describe what the ship security officer shall do:

Security Level 1: Embarkation of Persons and their Effects

- ✓ Segregate embarking and disembarking passengers,
- ✓ Verify the reason personnel are embarking from the Ship by using tickets, boarding passes, and work orders.
- ✓ Inspect persons and their belongings before being allowed onboard (crew is not required to engage in inspection/screening of other crewmembers).
- ✓ Ensure checked persons and their personal effects are segregated from unchecked persons.
- ✓ Positively identify crewmembers prior to boarding using their Seafarers Identification record, passport or other positive means of identification and verify their authority to serve aboard the Ship.

Security Level 2: Embarkation of Persons and their Effects

- ✓ Provide security briefings to all crew and passengers prior to departing on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.
- ✓ Increase the frequency and detail of inspecting persons, carry-on items for prohibited weapons, explosives, etc.
- ✓ Positively identify personnel prior to each embarkation.

Security Level 3: Embarkation of Persons and their Effects

- ✓ Inspect all persons, carry-on items for prohibited weapons, explosives, etc.
- ✓ Provide security briefings to all crew and passengers, prior to each embarkation and disembarkation, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.
- ✓ Escort all service providers or other personnel who need to board.
- ✓ Assign additional personnel to guard designated areas.
- ✓ Assign personnel to continuously patrol designated areas.
- ✓ Increase the detail and frequency of controls used for people boarding the ship.
- ✓ Suspend embarkation or disembarkation.

c. Monitoring restricted areas

The SSP should identify the restricted areas to be established on the vessel, specify their extent, time of application, the security measures to be taken to control access to them, and those to be taken to control activities within them. The purposes of restricted areas are to provide security in the following manner:

- Prevent or deter unauthorized access;
- Protect persons authorized to be onboard;
- Protect the vessel;
- Protect sensitive security areas within the vessel;
- Protect security and surveillance equipment and systems; and
- Protect cargo and vessels stores from tampering

Designation of Restricted Areas - The vessel owner or operator must ensure restricted areas are designated on board the vessel, as specified in the approved plan. Restricted areas must include, as appropriate:

- Navigation bridge, machinery spaces and other control stations;
- Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;
- Ventilation and air-conditioning systems and other similar spaces;
- Spaces with access to potable water tanks, pumps, or manifolds;
- Spaces containing dangerous goods or hazardous substances;
- Spaces containing cargo pumps and their controls;
- Cargo spaces and spaces containing vessel stores;
- Crew accommodations; and
- Any other spaces or areas vital to the security of the vessel.

Security Level 1: Restricted Areas on the Ship

- ✓ Locking and securing access points,
- ✓ Using surveillance equipment to monitor the areas,
- ✓ Using guards or patrols, and
- ✓ Using automatic intrusion-detection devices to alert the vessel personnel of unauthorized access.

Security Level 2: Restricted Areas on the Ship

- ✓ Increased the frequency and intensify monitoring the control and access to restricted areas,
- ✓ Establishing restricted areas adjacent to the access point,
- ✓ Continuously monitoring surveillance equipment,
- ✓ Dedicating additional personnel to guard and patrol restricted areas.

Security Level 3: Restricted Areas on the Ship

- ✓ Setting up additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied, and
- ✓ Searching restricted areas as part of a search of the ship.

d. Monitoring deck areas and areas surrounding ship

Ship Security Monitoring Areas

The monitored areas mainly include the restricted areas, vulnerable areas and the surrounding of the ship including likely boarding access.

Measures for security monitoring

Security Lighting:

- While the ship is at sea, on the premise of securing the safe navigation, the lights are to be switched on as many as possible, and sufficient lights are to be provided for both sides and stern of the ship. The searchlight is to be added to enhance the visibility over the water surface surrounding the ship. Marker light is also to be switched on. The person on duty is often to use Morse code light and strong light torch for the sea surface to show that the ship is capable of defending itself. The light for the cargo area is to be switched on and the stern light is also to be added when necessary.
- While the ship is at mooring or anchorage, all the lightings on the deck and inside the ship are to be kept in good condition. At night, the lights are to be switched on to ensure the lighting for the deck, stern areas and access points of the ship, so that the crew can see the conditions of the areas over the hip and of the areas surrounding the ship. At higher security level, the lighting is to be cooperatively used for dock facility. The additional lights include strong spot light to be used for both sides and the stern of the ship to enhance the visibility of the deck and the water surface surrounding the ship
- Security persons are to be arranged for as watch-keepers on the deck including patrol.
- While the ship is at sea, the equipment such as radar, binoculars etc. can be used for detailed search for the suspected target over the sea.
- Audible and/or visual alarm is to be activated, such as siren warning and search lighting warning for suspected target.
- Or all the means mentioned above can be combined in use.

Requirements for deck lighting or lighting inside the ship

- At dark night or under poor visibility condition, when the ship/port facility interface activities, mooring or anchoring operations are carried out, the lighting for the deck, the area of the stern and access points of the ship are to be ensured.
- While the ship is at dock, at anchorage or is at sea, the deck and the ship sides in darkness or in poor visibility are to be provided with appropriate lighting upon the security level and the judgment of the master. But it is not to affect the navigating light or the safety of navigation.

e. Coordinating the security aspects of handling cargo and ship stores

- ✓ The master and the chief officer are responsible for checking the conformity of the cargoes to be loaded and cargoes listed, and for ensuring that only permitted cargoes can be loaded on the ship. If they are not in conformity, they can refuse the cargoes to be loaded on the ship.

- ✓ The ship security officer is responsible for the monitoring of the cargo handling. If a suspected case is detected, he is to contact the port facility officer, shipper or other relevant party to arrange detailed inspection of the cargoes.

- ✓ The officer on duty is responsible for the monitoring during cargo handling and normal inspection of cargo unit upon the handling instructions given by the chief officer, and for ensuring the loading cargo complete and without damage.

- ✓ If the items in the contract signed with the shipper or other responsible party cover the contents of allopatric inspection, box sealing, date arrangement and bill providing etc., the company security officer and the ship security officer are to notify the port facility security officer of the contract and have him agree on it.

Requirements for Cargo Handling Control

Control of the cargo areas

- All the cargo areas are to be inspected before commencement of the operation.
- The cargo areas are permitted to enter while the ship is at sea.
- During cargo handling, unauthorized persons are not allowed to enter the cargo areas.
- Entrance to the dangerous cargo areas are to be strictly controlled.
- The cargo handling equipment is to be fastened when it is not in use.

Control of Cargo Handling

- Before the loading, the master is to check the written cargo information submitted by the shipper or the charterer, so as to ensure the safety of the cargo to be loaded on the ship or to be unloaded to the harbor. If there is any suspected case, he is to report to the company and the relevant party of the cargo.
- The officer on duty is to carry out the normal check of the cargo, cargo carriage unit and cargo areas before or during cargo loading to ensure the cargoes being loaded on the ship matches the cargo documentation.
- Check the proper strip seal or other means to prevent being damaged, so as to ensure the cargoes were not changed.
- Before the commencement of the operation of the cargo handling, all the cargoes and cargo hauling equipment are to be checked to see whether there are weapons, ammunition, flammable or explosive substance, drugs and contraband. The check of the cargoes may be carried out by means of the following:
  - ⇨ Visual and physical examination
  - ⇨ Sample examination of the loaded cargoes (at least 25%) is to be carried out with scanning/detection equipment, mechanical devices or dogs.

- Sample check of the identification number of the empty containers and the non-container carried cargoes is to be carried out upon the cargo documentation (where applicable)
  - ⇨ Keep close contact with the port facility department to ensure that the transportation tools of with designated percentage are to be loaded on the vehicle carrier and the roro ship and passenger ship. Check is to be carried out before loading. (The company is to determine the appropriate percentage)

Dealing with Suspected Cargo

Once the suspected cargo is detected on board, the operation of the cargo handling is to be ceased, which is to be reported to the chief officer, ship security officer and company security officer.

The Ship Security Officer is to contact the port facility security officer requiring cooperation in full and more detailed inspection.

Cooperate with the emergency responding body and the port facility security officer in full check of the dangerous goods loaded on board and their locations, and cooperate with the emergency responding body in handling of the suspected goods in accordance with the relevant instructions given by the emergency responding body.

It is to be reported as the “report of illegal actions”.

The following measures for cargo handling, depending on the security level, can be used:

Security Level 1: Cargo Handling

- ✓ Routine checks on cargo, transport units, cargo spaces
- ✓ Matching cargo with the documentation
- ✓ Loading vehicles subjected to search in liaison with the PFSO
- ✓ Checking seals to prevent tampering

Security Level 2: Cargo Handling

- ✓ Detailed checking of cargo, transport units, cargo spaces
- ✓ Intense checks to ensure only intended cargo is loaded
- ✓ Intense check on loading vehicles
- ✓ Increased frequency of checking seals

Security Level 3: Cargo Handling

- ✓ Suspension of loading or discharging
- ✓ Verify inventory of DG and hazardous substances onboard

Source: https://www.marineinsight.com/marine-safety/security-levels-under-isps/

Control of Suppliers

The company is to make requirements for control of suppliers of ship's stores, including the requirements for inquiring about the security backgrounds.

Delivery of Ship's Stores

Before delivery of the ship's stores, the company is to provide the ship in time with the list of the stores ordered including name of the supplier, address, liaison, telephone and fax, etc.

Before delivery of the stores, the supplier is to notify the ship, indicating the date and time they are to be delivered.

Ensure the stores mentioned in the list provided by the company to match the spare stores on board. Only after satisfactory examination, can they be loaded on board; otherwise, they are to be refused.

At an appropriate security level, the packages of the stores integrity are to be checked before they are loaded so as to ensure the stores are not damaged or accompanied by other articles.

At an appropriate security level, visual and physical inspections are to be given to all the stores including using scanning/detection equipment, mechanical devices or dogs to sample the loaded cargo to see whether there are weapons, ammunition, flammable or explosive substance, drugs and contraband.

After being accepted, the ship's stores are to be stockpiled and fastened in time. This is avoid tampering of the stores.

The ship's stores are to be stored in restricted area after delivery.

The following measures for ship's store delivery, depending on the security level, can be used:

Security Level 1: Delivery of Ship's Stores

- ✓ Match orders with documents prior to loading
- ✓ Stow the stores securely

Security Level 2: Delivery of Ship's Stores

- ✓ Thorough checks prior to loading stores and intensifying inspections of the same

Security Level 3: Delivery of Ship's Stores

- ✓ Delivery of stores to be taken only in case of emergency

Source: https://www.marineinsight.com/marine-safety/security-levels-under-isps/

3.2 Execution and coordination of searches

- Planning a search using a system of check cards
  - Check card
    - issued to each searcher specifying the route to follow and the areas to be searched
    - can be color-coded for different areas of responsibility
    - returned to a central control point upon completion of individual search tasks
    - When all cards are returned, the search is known to be complete. The findings of the search can then be discussed

- Basic items or equipment that may be employed in conducting searches include the following:

  - ✓ 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

- Procedures to be followed to ensure effective and efficient searches include the following:

  - ✓ Crew members and facility personnel should not be allowed to search their own areas in recognition of the possibility that they might conceal 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 findings.
  - ✓ Searchers should be able to recognize suspicious items.
  - ✓ There should be a system for marking or recording "clean" areas.
  - ✓ Searches should maintain contact with the search controllers, perhaps by UHF/VHF radio.
  - ✓ Searchers should have clear guidance on what to do if a suspected package, device, or situation is found.
  - ✓ Searchers should bear in mind that weapons and other dangerous devices may be intentionally placed in disguise such as toolbox in an engine room.

- Tips for Conducting a Thorough Security Search

  The following tips should be used in conjunction with your employers and state guidelines for conducting a security search on a person.

  - **Search Preparation –** Prior to starting a search, the person should be given an opportunity to assist with the process by emptying the contents of their pockets and any bags, as well as removing specific clothing items, such as their jacket.

- **Gender Specific Searches –** When possible, it's important to have same-sex searched conducted. While this may not always be a possibility, it should be striven for to help make the person being searched more comfortable to potentially prevent any claims against harassment.

- **Don't Search Alone –** When possible, you should always have a co-worker or supervisor with you during a search process. This is important as a colleague can serve as a witness throughout the search should the person accuse you of any type of misconduct. If not possible, clearly gain consent to perform the search and inform the person what you plan on doing as part of the search and if they are uncomfortable with any portion. Clear communication is imperative to prevent any misunderstandings between you or the person.

- **Remain Sensitive to Persons –** There will be cases where the person who requires a search features religious garments or has mobility issues. When this is the case, it's important to ensure the person feels comfortable executing the search in the current location. If the person has religious issues with the search, or is not comfortable being searched in a crowded room, do what you can to accommodate their needs. If you are unable to satisfy the needs of the person, call your supervisor to have them make the final judgment call about moving forward.

- **Contact Management –** Should any illegal or forbidden items be found during the search, it's important to immediately contact your manager or supervisor. Do not simply place the forbidden items in your pocket and move forward. Doing so could result in serious legal issues for you and your security company. Once your manager/supervisor arrives, he or she will determine if calling law enforcement officers is necessary.

- **Confiscate Illegal/Forbidden Items –** While waiting for your manager or supervisor to arrive, you should immediately confiscate the illegal or forbidden items. Many times, the person will simply take the item and leave; however, depending on what was found, this may be a serious legal issue.

- There are many places on board a ship where weapons, dangerous substances, and devices can be concealed. Some of these are the following:

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 sock
- ✓ Hollowed-out molding

Companionways

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

Toilet and Showers

- ✓ Behind and under washbasins
- ✓ Behind toilets
- ✓ In ventilation ducts and heaters
- ✓ Toilet tissue rollers, towel dispensers, supply lockers
- ✓ Taped to showers 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 rope, in deck storage rooms
- ✓ Paint cans, cargo holds, battery rooms, chain lockers

Engine Room

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

Galleys and Steward's 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

4. SECURITY EQUIPMENT AND SYSTEMS

4.1. Security Equipment and Systems

- Types of Security Equipment and Systems:

Equipment for Access Control

- ✓ Locks, seals
- ✓ Monitoring equipment, automatic intruder detector
- ✓ Light, ID system for passenger, ID system for vehicle
- ✓ Ship Security Alert System

Searching/Screening Equipment

- ✓ Archway metal detector, hand-held metal detector,
- ✓ X-ray scanning machine, Explosive Vapor Detector (EVD)
- ✓ Port Equipment

Port Security Equipment

- ✓ Cargo X-ray drive-by; Cargo X-ray mobile, cargo X-ray drive-through

Baggage Inspection	
CCTV Camera	
CCTV Monitoring Station	

Finger Print Access Control	
Combination Lock	
Hand Wand	

Fire Alarm Loud Speaker	
Panel Kit	
Metal Detector	

Proximity Card System	
Panoramic Automatic Intruder Detection Alarm	
Scanmail	

Sabre 2000 Explosive Handheld Detection	

- Limitations of Security Equipment and Systems

Individual Items of Equipment and Security Systems

Locks and Seals are applied to access control areas and cargo in order to restrict its opening and closing. Locks/Seals are inexpensive and can perform unauthorized access/opening.

Surveillance/Monitoring Device (CCTV) is a devise used for monitoring and maintaining surveillance to remote areas. It is widely used in shore; however, certain precautions are to be applied:

Consider cameras' fitness for the purpose (resolution, black/white or colored, night vision capacity, field of vision, magnifying capacity) and number should be adequate for the areas to be monitored. Cameras on weather decks should be provided with weatherproof coverings.

Automatic Intrusion Detection System is a device wherein a motion active sensor function is added to the said surveillance device (CCTV).

-Activate by infrared rays or by sensor

-Alarm activated by opening/closing of doors (mechanical switch on door). It is effective to combine alarm system with surveillance system. Caution should be paid in installing such equipment, most especially as it is surveillance equipment.

Lights - strong light identifies intruders and deters intrusion. There are two types: 1) continuously switch on and 2) switch on only when a sensor detects presence of the intruder. Bear in mind that this light should not conflict with requirements of COLREG Convention.

Hand-Held Metal Detector is used for a person's reaction at gate prior entering the ship/premises. Comparatively inexpensive and easy to handle, but caution is to be exercised against running out of battery. It is necessary to confirm the function of the equipment by test piece (coin) before using the device.

Baggage X-ray Machine (Box Scatter) is used for baggage and it is known for its effectiveness compared to older models. However, the operators need to be trained as the cost of the machine is very high.

Walk-through Metal Detector - is used in the screening of individuals prior boarding the ship. Like the Baggage X-ray machine, the operators must be trained because the cost of the unit is high.

Identification System for Passenger and Crew – a system of identification for passengers and crew. It should be noted that in case of visiting a port in the USA, ID cards with a photograph is required. It should be noted that a magnetic card could be forged easily.

Vehicle Identification system– a system of scanning vehicle's registration plate automatically and alarms automatically for a subject vehicle registered in advance to exercise caution.

- **Testing, Calibration and Maintenance of Security Equipment and Systems**

Testing, calibration, and maintenance of security equipment and systems should be carried out to ensure **accuracy, efficiency, and operational readiness** of selected items of security equipment.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated and maintained according to the manufacturer's recommendation.

(b) The results of testing completed under paragraph (a) of this section shall be recorded and any deficiencies shall be promptly corrected.

(c) The Ship Security Plan (SSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.