
	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>



# **SHIP SECURITY OFFICER**

## **IMO MODEL 3.19**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### **SCOPE**

This course to provide knowledge to those who be designated to perform the duties and responsibilities of a Ship Security Officer (SSO), as defined in Section A/2.1.6 (and section A/12) of the ISPS Code and in section A-VI/5 of the STCW Code, as amended, and in particular the duties and responsibilities with respect to the security of a ship, for implementing and maintaining a Ship Security Plan and for liaising with Company Security Officers (CSO) and with Port Facility Security Officers (PFSOs).

### **OBJECTIVES**

Those who successfully complete this course should be able to undertake the duties and responsibilities as Ship Security Officer, as defined in section A/12.2 of the ISPS Code and in section A-VI/5 of the STCW Code, as amended, which include, but are not limited to:


- .1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- .2 maintaining and supervising the implementation of the Ship Security Plan, including any amendments to the plan;
- .3 coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant Port Facility Security Officer;
- .4 proposing modifications to the Ship Security Plan
- .5 reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and Verifications of compliance and implementing any corrective action;
- .6 enhancing security awareness and vigilance on board;
- .7 ensuring that adequate training has been provided to shipboard personnel; as appropriate;
- .8 reporting all security incidents;
- .9 coordinating implementation of the Ship Security Plan with the Company Security Officer and the relevant Port Facility Security Officer;
- .10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

### **ENTRY STANDARD**

No specific entry requirements are contemplated. However, to obtain a Certificate of Proficiency as Ship Security Officer, the trainee shall have obtained approved seagoing service as mentioned in STCW Regulation VI/5 as amended.

### **COURSE CERTIFICATE, DIPLOMA OR DOCUMENT**

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

**COURSE INTAKE LIMITATION**

The maximum numbers of trainees are 25

**STAFF REQUIREMENTS**

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

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

**TEACHING FACILITIES AND EQUIPMENT**

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

**TEACHING AIDS**

Instructor Manual

Audiovisual aids: video player, TV, slide projector, overhead projector, etc.

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

Videos(s)

**BIBLIOGRAPHY**

ISPS Code Part A

ISPS Code Part B

SOLAS Chapter XI-1

SOLAS Chapter XI-2



**TIMETABLE**


➤ **COURSE OUTLINE**

SUBJECT AREA	HOURS
<p><b>1. INTRODUCTION</b></p> <p>1.1.Course overview 1.2.Competences to be achieved 1.3.Historical perspective 1.4.Current security threats and patterns 1.5.Ship and port operations and conditions</p>	1.5
<p><b>2. MARITIME SECURITY POLICY</b></p> <p>2.1.Relevant international conventions, codes and recommendations 2.2.Relevant government legislations and regulations 2.3.Definitions 2.4.Legal implications of action or non-action by security personnel 2.5.Handling sensitive security-related information and communications</p>	1.0
<p><b>3. SECURITY RESPONSIBILITIES</b></p> <p>3.1.Contracting governments 3.2.Recognized Security Organization 3.3. The company 3.4.The ship 3.5.The port facility 3.6.Ship Security Officer 3.7. Company Security Officer 3.8. Port Facility Security Officer 3.9.Seafarers with designated security duties 3.10. Port Facility personnel with designated security duties</p>	1.5
<p><b>4. SHIP SECURITY ASSESSMENT</b></p> <p>4.1.Risk assessment methodology 4.2.Assessment tools 4.3.On-scene security surveys 4.4.Security assessment documentation</p>	1.25
<p><b>5. SECURITY EQUIPMENT</b></p> <p>5.1.Security equipment and systems 5.2.Operational limitations of security equipment and systems 5.3.Testing, calibration and maintenance of security equipment and systems</p>	1.5
<p><b>6. SHIP SECURITY PLAN</b></p> <p>6.1.Purpose of the Ship Security Plan 6.2.Contents of the ship Security Plan 6.3.Confidentiality issues 6.4.Implementation of the Ship Security Plan 6.5.Maintenance and modification of the Ship Security Plan</p>	2.0




<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

SUBJECT AREA	HOURS
<b>7. THREAT IDENTIFICATION, RECOGNITION AND RESPONSE</b> 7.1. Recognition and detection of weapons, dangerous substances and devices 7.2. Methods of physical searches and non-intrusive inspection 7.3. Implementing and coordinating searches 7.4. Recognition, on a non-discriminatory basis, of persons posing potential security risk 7.5. Techniques used to circumvent security measure 7.6. Crowd management and control techniques	3.0
<b>8. SHIP SECURITY ACTIONS</b> 8.1. Actions required by different security levels 8.2. Maintaining security of the ship/port interface 8.3. Usage of the Declaration of Security 8.4. Reporting security incidents 8.5. Implementation of security procedures	1.5
<b>9. EMERGENCY PREPAREDNESS, DRILLS AND EXERCISES</b> 9.1. Contingency planning 9.2. Security drills and exercise 9.3. Assessment of security drills and exercise	1.25
<b>10. SECURITY ADMINISTRATION</b> 10.1. Documentation and records 10.2. Monitoring and control 10.3. Security audits and inspections 10.4. Reporting nonconformities	1.0
<b>11. SECURITY TRAINING</b> 11.1. Training requirements	0.5
<b>TOTAL:</b>	<b>16.0</b>

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### COURSE TIMETABLE

<b>DAY/ PERIOD</b>	<b>1<sup>st</sup> PERIOD (2.0 HOURS)</b>	<b>2<sup>nd</sup> PERIOD (2.0 HOURS)</b>	<b>3<sup>rd</sup> PERIOD (2.0 HOURS)</b>	<b>4<sup>th</sup> PERIOD (2.0HOURS)</b>
Day 1 (8hours)	1. INTRODUCTION 1.1 Course overview 1.2 Competences to be achieved 1.3 Historical perspective 1.4 Current security threats and patterns 1.5 Ship and port operations and conditions  2. MARITIME SECURITY POLICY 2.1 Relevant international conventions, codes and recommendations 2.2 Relevant government legislation and regulation 2.3 Definitions	2.4 legal implications of action or non-action by security personnel 2.5 handling sensitive security-related information and communications  3. SECURITY RESPONSIBILITIES 3.1 Contracting governments 3.2 Recognized Security Organization 3.3 The company 3.4 The ship 3.5 The port facility 3.6 Ship Security Officer 3.7 Company Security Officer	3.8 Port Facility Security Officer 3.9 Seafarers designated security duties 3.10 Port facility personnel with designated security duties 3.11 Other personnel  4. SHIP SECURITY ASSESSMENT 4.1 Risk assessment methodology 4.2 Assessment tools 4.3 On – scenes security surveys 4.4 Security assessment documentation	5. SECURITY EQUIPMENT 5.1 Security equipment and system 5.2 Operational limitations of security equipment and systems 5.3 Testing calibration and maintenance of security equipment and systems  6. SHIP SECURITY PLAN 6.1 Purpose of the Ship Security plan 6.2 Contents of the ship security plan

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

<b>DAY/ PERIOD</b>	<b>1<sup>st</sup> PERIOD (2.0 HOURS)</b>	<b>2<sup>nd</sup> PERIOD (2.0 HOURS)</b>	<b>3<sup>rd</sup> PERIOD (2.0 HOURS)</b>	<b>4<sup>th</sup> PERIOD (2.0HOURS)</b>
Day 2 (8 hours)	6.3 Confidentiality issues 6.4 Implementation of the ship security plan 6.5 Maintenance and modification of the ship security plan 7. THREAT IDENTIFICATION, RECOGNITION AND RESPONSE 7.1 Recognition and detection of weapons, dangerous substances and devices 7.2 Methods of physical searches and non-intrusive inspections	7.3 Implementing and coordinating searches 7.4 Recognition a non-discriminatory basis, of persons posing potential security risk 7.5 Techniques used to circumvent security measures 7.6 Crowd management and control techniques	8. SHIP SECURITY ACTIONS 8.1 Actions required by different security levels 8.2 Maintaining security of the ship/port interface 8.3 Usage of the declaration of security 8.4 Reporting security incidents 8.5 Implementation of security procedures 9. EMERGENCY PREPAREDNESS, DRILLS AND EXERCISE 9.1 contingency planning 9.2 security drills and exercise 9.3 assessment of security drills and exercise	10. SECURITY ADMINISTRATION 10.1 documentation and records 10.2 Monitoring and control 10.3 Security audits and inspection 10.4 Reporting nonconformities 11. SECURITY TRAINING 11.1 Training requirements

**MANUAL****1. Introduction****1.1. Course overview**

The threat of attack from pirates and terrorists is a very real one for vessels passing through global waters that are designated as high risk areas.

This course is specifically designed for crew who may encounter a security or safety problem as they transit hostile environments and adverse conditions.

It includes an introduction to the background of the International Ship and Port Facility Security Code (ISPS), the roles of the company security officer (CSO) and ship security officer (SSO), security requirements and security administration.

The programme covers security drills, security exercises, crowd management techniques, security protection and emergency preparedness.

Students will become proficient in:

- Ship security assessments and audits
- Creating ship security plans
- Ship and port facility security measures
- Recognition of behavioural patterns of people likely to threaten security
- Detection of weapons
- Testing and calibration of security equipment and systems.


**1.2. Competencies to be achieved**

Completed the course will have knowledge of methods and criteria in maritime security:

**Methods**

- Assessment of evidence obtained from approved training or examination
- Assessment of evidence obtained from approved training, or approved experience and examination, including practical demonstration of competence to:
  1. conduct physical searches
  2. conduct non-intrusive inspections



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

**Criteria**

- Procedures and actions are in accordance with the principles established by the ISPS Code and the SOLAS, 1974, as amended.  
Legislative requirements relating to security are correctly identified.
- Procedures achieve a state of readiness to respond to changes in maritime security levels.
- Communications within the ship security officer's area of responsibility are clear and understood.
- Procedures achieve a state of readiness to respond to changes in the maritime security levels.

**1.3. Historical perspective**

Most legislation in the maritime world is initiated by some kind of maritime disaster or accident. The Titanic catastrophe, where many passengers and crew members perished due to the fact that there were not enough lifeboats, gave birth to international safety regulations. The MARPOL-convention came in to force a few years after serious oil pollution, caused by the grounding of the tanker Torrey Canyon on rocks near the Isles of Scilly. Further, despite proper rules and regulations, a very high number of accidents caused the IMO to implement the International Safety Management Code (ISM).

Contrary to previous conventions and codes, the creation of the ISPS Code was caused by a disaster that happened ashore, when hijacked aircrafts on the 11th of September 2001 flew into the twin towers of the World Trade Center, destroyed part of Pentagon and crashed on a field in Pennsylvania.


In peace time, to facilitate trade, merchant ships have traditionally been entering territorial waters and ports without much hindrance. The embarkation of port authorities, with clearance and free pratique granted has occurred once the ship was alongside a berth or at a customary anchorage.

With such an easy access to seaports, security experts were of the opinion that merchant ships could be used as a tool by terrorists. Different scenarios were developed, where merchant ships were means of transportation of terrorists and their weapons, or that the ship in its own right was a weapon. An example given was the risk of gas ships being hijacked and blown up in busy seaports.

Urgently, legislation was needed to protect both merchant ships and seaports.

**Maritime terrorism before ISPS Code (before 1 July 2004)**

The Council for Security Cooperation in the Asia Pacific has offered an extensive definition for maritime terrorism:

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

“...the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities.”

Similar to the ISPS Code, not only are ships considered as objects for maritime terrorism, but also port facilities.

Maritime terrorism is not rampant. Nevertheless there has been a steady flow of incidents during the last 50 years. The Global Terrorism Database (GTD) at the University of Maryland is an open-source database on global terrorist incidents (including maritime), covering events from 1970 through 2012.

From 11<sup>th</sup> June 1970 to 1<sup>st</sup> July 2004, there were 212 maritime terrorism incidents. However, most of those incidents were on rather low level, like the incident with GTD ID: 200112120005: “12/12/2001: Members of People’s Revolutionary Army (ERP) set up an illegal checkpoint along the Cauca River near Magangue, Sucre, Colombia. The rebels stopped a canoe traveling along the river and abducted nine of the passengers. Three people were released the next day. Specific motive is unknown.”

Still there are some significant incidents that got an extensive media coverage.



- Santa Maria: The hijacking of the Portuguese passenger ship Santa Maria is considered to be first case of maritime terrorism. On January 22, 1961, 24 leftist




Portuguese terrorists hijacked the luxury cruise liner. The ship was carrying 600 passengers and a crew of 300. The would-be hijackers embarked the vessel as passengers at the port of La Guairá in Venezuela and on the Dutch island of Curacao, with weapons hidden in their suitcases. The terrorists took over command of the vessel, but eventually surrendered when they were given political asylum in Brazil.

- Sounion: A few years prior to the outbreak of the civil war in Lebanon, in March 1973 the Greek passenger ship Sounion sunk in the port of Beirut. A limpet mine was attached to the ship's hull by Palestinian terrorists while the ship was in dock, with the aim of blowing up the ship once at sea. Due to the interference of a Swedish undercover agent based in Lebanon, the departure was delayed, passengers could disembark and the ship sunk while still alongside the berth.
- Shadow V: A fishing boat owned by the former First Sealord and last Viceroy of India, Lord Mountbatten. In September 1979, while onboard the boat in waters near his summer home on Ireland, a bomb planted by the Irish Republican Army exploded and killed him.
- Rainbow Warrior; A Greenpeace ship sunk by the French foreign intelligence service in the port of Auckland, New Zealand, July 1985. Not an act of terrorism as such, but two French secret service agents were found guilty and sentenced to ten years in prison by the New Zealand court of law.
- Achille Lauro; In October 1985, the passenger ship while on a cruise in the Mediterranean, was hijacked by four terrorists from Palestine Liberation Front, off the coast of Egypt. After only two days of negotiation, but after they had killed an elderly American passenger, the hijackers gave up when they were promised political asylum in Tunisia. However, justice was swift, as US warplanes forced the Egyptian airliner carrying the hijackers to land in Italy.

As a result of the hijacking, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) was developed and adopted.

- The Tanker War: With something that can be referred to as state terrorism, both sides attacked shipping in the Persian Gulf, mainly tankers, during the Iran-Iraq war between 1980 and 1988. According to sources more than 400 seamen were killed and 340 ships were attacked, during the conflict.
- The Tamil Tigers: During the civil war between the Sri Lankan government and the Liberation Tigers of Tamil Eelam, the latter was involved in maritime terrorism with its Sea Tigers brigade. The brigade was accused of hijacking several vessels in waters off the coast of Sri Lanka, including Irish Mona (in August 1995), Princess Wave (in August 1996), Athena (in May 1997), Misen (in

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

July 1997), Morong Bong (in July 1997), MV Cordiality (in Sept 1997) and Princess Kash (in August 1998). One spectacular act of maritime terrorism was the suicide attack on the tanker Silk Pride.

- USS Cole: Although a warship, the modus operandi used by the attackers was kind of a harbinger, when in October 2000, a small craft laden with explosive commanded by Al Qaeda suicide bombers hit the US Navy destroyer. The attack killed 17 sailors and wounded another 42.
- M/T Limburg: In October 2002, the French owned crude oil carrier was attacked when approaching an offshore terminal off the coast of Yemen. An explosive-laden boat rammed the hull of the tanker, causing an explosion followed by fire.
- Superferry 14: Regrettably, the ferries of the Philippines have a very bad safety record. Also, the maritime security record has been tarnished. The February 2004 terrorist attack on Superferry 14 caused the death of 116 persons. Suicide bombers from the Al Qaeda linked Abu Sayyaf group, using a boat loaded with explosives, were the perpetrators.

**Maritime terrorism after ISPS Code (after 1st July 2004)**


Supporters of the ISPS Code may argue that the Code has been successful since there have been no serious maritime terrorist attacks since the implementation.

Detractors may argue that the code did not help much in protecting seafarers against the menace of modern day piracy.

Whatever opinion someone may have, the Code was developed to protect the international community against terrorism, and as such it has been a success. Piracy and terrorism are different crimes, needing different approaches. And, according to conventional wisdom, the link between terrorist and pirates is very weak.

Although there has been a positive impact on the security situation from the Code, there have been some serious incidents:

- Don Ramon: The second maritime terrorist attack by Abu Sayyaf took place in August 2005 onboard the passenger ship Don Ramon in Filipino waters. Terrorist had placed a timed bomb beneath gas cylinders in the ship's galley, causing the ship to sink and wounding 30 passengers.
- M. Star: In July 2010, the Japanese owned very large crude oil carrier experienced an explosion when transiting the Strait of Hormuz. Although no craft was sighted, the explosion made a large dent in the hull, parts of

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

accommodation were slightly damaged and one crewmember was injured. After two days, the terrorist group Brigades of Abdullah Azzam claimed responsibility.

- Yemen, level 3: In August 2013, due to a high level of activity by Al Qaeda affiliated groups in Yemen, the Government of United Kingdom raised the ISPS security level to level 3 for British flagged ships in Yemeni territorial waters. A serious situation indeed, since an elevation to level 3 was unprecedented since the ISPS Code was introduced in 2004.
- Cosco Asia: In September 2013, while on transit in the Suez Canal, the Chinese owned container vessel under the flag of Panama, was hit by a rocket propelled grenade. The ship sustained only minor damages, and there were no casualties. An Islamist group named Al-Furqan claimed responsibility for the attack. Although a minor attack, it was of great concern for the Egyptian government, due to the economic importance of the Canal. To increase security, a protective wall along the Canal is in the process of being constructed.

#### **1.4. Current security threats and patterns**

Maritime security has always been a part of commercial shipping. Piracy is as old as shipping itself and stowaways is hardly a new problem either. During wars, the merchant marine has been an integral part of the war effort, being a vital support line for warring nations in need of weapons, food, oil and other commodities.

Thus, war, piracy and stowaways are threats that the shipping industry has been dealing with for a long time. Administrations and ship owners' associations have for decades been issuing regulations and instructions in an attempt to assist seafarers to deal with the perils.

For example, during the cold war, all Swedish ships were issued with an instruction about how to act during crisis and war by the Swedish Maritime Administration.

Some 30 years ago, with the appearance of modern piracy, the IMO and the International Chamber of Shipping issued guidelines.

In 1957, an international convention relating to stowaways was adopted, although not yet in force, and there are policies issued about how to deal with stowaways.

However, any specific instructions, how to protect a ship against terrorists, prior to the ISPS Code, were never issued. The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, which was agreed upon after the spectacular hijacking of Achille Lauro, was only addressing punishment of acts that could threaten the safety of maritime navigation.





Maritime piracy and maritime terrorism are known threats to global shipping, with piracy imposing substantial human and economic costs particularly off the coast of Somalia in recent years. Drug, weapon, and human trafficking also have an increasingly well-documented maritime dimension. What may be less well understood is the extent to which each of these criminal areas may overlap or demonstrate signs of mutual cooperation. However, given the evidence that is emerging, we are becoming more aware of the impact global maritime crime can have beyond the specific geographical locations in which it occurs. Piracy, terrorism and illicit trafficking are problems that afflict all of us associated with maritime trade, and argue for a more comprehensive solution.




### **Maritime Piracy**

From data collected between 2002 through 2012 global pirate attacks have been found to be cyclical in nature, with the first high point noted in 2003 and then again in 2010, and a drop in 2006. A steep drop in 2012 indicates we are currently entering another low point in the cycle of maritime piracy.

What is not clearly evident from the numbers alone is the geographical pattern of maritime piracy in these years. Pirate attacks from 2002 through 2006 were concentrated in the Strait of Malacca region and the South China Sea. However, from 2006 through 2011 Somali pirates were responsible for the vast majority of attacks, with their geographical range extending initially from the Somali coastline then eventually east into the Indian Ocean, south down the coasts of Kenya and Tanzania, reaching the Seychelles, and finally the entrance of the Persian Gulf.

This tendency to concentrate geographically highlights a critically important point for mariners; pirate hot spots can be identified, and to some extent even predicted.

Maritime piracy has tended to concentrate in just three regions in the last five years; the Horn of Africa (exclusively Somali pirates), the Gulf of Guinea (pirates from Nigeria), and the region in and around the Strait of Malacca (committed largely by Indonesian

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

pirates). Not only did global pirate attacks drop in 2012, Somali pirate attacks dropped substantially. However, at the same time, we see a disturbing rise in attacks in the Gulf of Guinea and a resurgence of attacks in and near the Strait of Malacca, despite the overall global decline.


### **Maritime Terrorism**

The current geographical shift of maritime piracy from the Horn of Africa to Malacca and the Gulf of Guinea is important from the point of view of maritime terrorism as well, as terrorist groups with known maritime capabilities operate in these parts of the world (this is particularly the case in Nigeria and the Movement for the Emancipation of the Niger Delta – MEND). While many argue that pirate-terrorist “linkages” are unlikely to occur due to differing motivations (pirates operate for economic gain; terrorists for political gain) it must be noted in reality that there are significant “grey areas.” For example, the now-defunct Liberation Tigers of Tamil Eelam (LTTE) committed both pirate and terrorist attacks in Sri Lanka; most of the pirate attacks in Nigeria are attributed to MEND, which has been designated as a foreign terrorist organization (FTO) by the United States.

This said, activity has been remarkably quiet on the maritime terrorist front. Predictions about a “move to the sea” by groups such as al Qaeda in the Arabian Peninsula (AQAP) operating largely in Yemen, al Shabaab in Somalia, or Jemaah Islamiyah in Indonesia have yet to materialize. Abu Sayaaf in the Philippines has been active in the past, but has not been significantly active in the maritime realm – particularly against foreign interests – for some years. There has been no known direct maritime attack by al Qaeda since the 2004 USS Firebolt incident in the Persian Gulf; the most recent known maritime terrorist event by any group was the minor attack on the VLCC M/V M. Star in 2010 attributed to the al Qaeda-affiliated Abdullah Azzam Brigades.

This should not argue for a relaxing of vigilance. Terrorism, by its very nature, always contains an element of unpredictability. A former UK First Sea Lord and Chief of Naval Staff deemed maritime terrorism “a clear and present danger” that may “potentially cripple global trade and have grave knock-on effects on developed economies,” and USN Captain Jim Pelkofski (Ret.) has noted that “indications point to an acceleration of the pace of maritime terrorism, heralding a coming campaign.” Most importantly remains the threat from the “lone wolf”. Individuals or groups operating “off the radar” can be remarkably difficult to apprehend prior to an attack, as we unfortunately noted from the recent Boston Marathon bombing.

While maritime terrorist attacks against a single vessel may not impose substantial economic damage beyond that to the shipping company, attacks against ports could be much more economically crippling. And the attack need not happen in the United States to cause economic harm. Were an attack to happen against a key hub port (for example, Singapore) effects could ripple throughout the global supply chain. At the same time, a

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

2002 simulation by Booz Allen Hamilton noted that just the credible threat of an attack (in this case a radiological device in a container) shut down most major US ports for 19 days.

**The “Web of Criminality”**

What may actually be the most significant threat for the maritime industry is the emerging “web of criminality” with pirates, terrorists, and “ordinary” criminals working opportunistically in an ad hoc manner around criminal opportunities. While hard statistical evidence is difficult to obtain, anecdotal evidence does exist. Pirates in Somalia are known to have engaged from time to time in gun running on behalf of al Shabaab. Al Shabaab has been associated with the illegal charcoal and khat trades (most of which is transited by ship). And in Nigeria, MEND and the more radical Boko Haram have been associated not only with piracy and oil theft (MEND) but believed to be involved in the illegal drug trade transiting through the country as well.

Maps of the world’s key shipping routes and known patterns of illicit activity highlight the complicity of the shady elements of the shipping industry, and the vulnerability of the legally operating shipping industry, very well. For example, global trade routes used by drug traffickers overlap not only with known pirate and terrorist areas of activity, but with the world’s major transit routes for the legitimate trade in energy and commodity flows.

Maritime piracy – regardless of where it occurs – imposes economic and human costs on us all. Given the extent of maritime criminality, we should not be thinking about, planning for, or protecting against “specific” threats – piracy, terrorism, drugs, human trafficking – but rather a “web” of threats with a number of actual and coincidental overlaps and interdependencies.

**Identifies threats to the maritime transport industries, such as:**


- **Piracy**

Piracy, in contradistinction, according to article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) is defined as:

Piracy consists of any of the following acts:

- a. any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
  - i. on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
  - ii. against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- 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).

The UNCLOS definition of piracy developed into international law and the International Maritime Organization (IMO)<sup>8</sup> recognized and accepted this definition. Thus, according to international law, any illegal acts of violence and detention which are committed within State's territorial waters are not defined as piracy. However, according to the IMB, nearly all illegal acts in Southeast Asia occur within territorial waters and thus would not fall under the definition of piracy. Technically, if an attack occurs within the territorial jurisdiction of a state, the event is only classified as piracy if that nation's penal code criminalizes it as such. Moreover, the IMO defines any unlawful act of violence or detention or any act of depredation at anchor, off ports or when underway through a coastal State's territorial waters as armed robbery against ships.

In order to overcome the distinctions between high seas and territorial waters, the IMB defines piracy as:

"an act of boarding (or attempted boarding) with the intent to commit theft or any other crime and with the intent or capability to use force in furtherance of that act."

Established by the International Chamber of Commerce (ICC) in 1981, the International Maritime Bureau (IMB) came into existence with the backing of the IMO, the world's foremost agency for exchanging and collecting information on maritime crime. However, according to the IMO, it is estimated that piracy incidents are likely under-reported by a factor of two (meaning, they assume that for each attack that was announced, there were two additional attacks that were not announced). Moreover, it is likely that the statistics are subject to distortion as many smaller attacks go unreported. This mainly stems from two factors:

the increase in insurance premiums often outweigh the value of the claim for smaller attacks; and


Reporting a piracy attack is often time-consuming can lead to a delay of several days. Keeping in mind the running sunk costs of an idle ship (up to \$25,000 per day), in many, especially smaller cases, it is cheaper not to report the incident.

While this wider definition allows the IMB to produce a more comprehensive picture about maritime crime, its definition is not recognized by international law.

- **Terrorism**

The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group has offered an extensive definition for maritime terrorism:

"...the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities."

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

This definition, however, does not define what terrorism is and whether it would only include maritime attacks against civilian (merchant) vessels or also attacks against military crafts. I define maritime terrorism, therefore, as the use or threat of violence against a ship (civilian as well as military), its passengers or sailors, cargo, a port facility, or if the purpose is solely a platform for political ends. The definition can be expanded to include the use of the maritime transportation system to smuggle terrorists or terrorist materials into the targeted country. Maritime terrorism is motivated by political goals beyond the immediate act of attacking a maritime target.

- **Contraband smuggling**

Smuggling is the illegal transportation of objects, substances, information or people, such as out of a house or buildings, into a prison, or across an international border, in violation of applicable laws or other regulations.

The majority of illicit drugs destined for consumer markets in the United State, Europe, Asia, and Oceana are smuggled via maritime conveyances, with the lion's share being transport unwittingly by commercial cargo/container vessels engaged in legitimate business and plying normal trade lanes.

Maritime smuggling routes therefore shift and modify when, for commercial reasons, shipping trade lanes or seaport operations change. Additional factors impacting on smuggling routes are the expansion into new or increasing consumer markets and as a reaction to law enforcement interdiction action. The surge in opium production in Afghanistan has increased the availability of cheap heroin in the European Community, Russia, and the former Eastern European countries, and the continuing escalation in heroin consumption in the United State, which now has reached epidemic levels, is driving increased opium cultivation and heroin smuggling from Colombia and Mexico. Recent changes in the supply and demand of drug, as well as interdiction concerns, have led major transnational drug trafficking organizations to modify their smuggling routes and modes of transport.

- **Stowaways and refugees**

**Stowaways**

The Convention on Facilitation of International Maritime Traffic, 1965, as amended, (The FAL Convention), define stowaway as "A person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the shipowner or the Master or any other responsible person and who is detected on board the ship after it has departed from a port, or in the cargo while unloading it in the port of arrival, and is reported as a stowaway by the master to the appropriate authorities".



***Refugees***

The 1951 Convention relating to the Status of Refugees, defines a refugee as a person who “owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion, is outside the country of his (or her) nationality , and is unable to or, owing to such fear, is unwilling to avail himself [or herself ] of the protection of that country” (Article 1A(2))


and prohibits that refugees or asylum-seekers be expelled or returned in any way to the frontiers of territories where his [or her] life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion.” (Article 33 (1))

An asylum-seeker is an individual who is seeking international protection and whose claim has not yet been finally decided on by the country in which he or she has submitted it. Not every asylumseeker will ultimately be recognized as a refugee, but every refugee is initially an asylum-seeker.



***Cargo theft***

Cargo theft is a transportation security related issue which especially road transport, maritime transport and rail transport is frequently facing. Theft has been a common problem with freight transportation throughout its history, and it includes a wide range of occurrences such as the piracy of ships, hijacking of rail cars and trucks, and theft of small items, which is referred to as “leakage”

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### ***Collateral damage***

Collateral damage occurs when a nearby fire, explosion, or attack results in damage to a ship or facility. While the damage is sometimes unintended, the costs are nevertheless real.

### **1.5. Ship and port operations and conditions**

Transportation industry has been facing challenges due to various security-related issues such as piracy, terrorism, thefts and accidents. Intermodal transportation as a system that incorporates many players, transportation modes, interchange points as well as various technologies can also be considered as an important platform for security-related problems. Although intermodal transportation is quite vulnerable to security-related risks, recent literature heavily focused on the security problems of specific transportation modes. Since intermodal industry consists of many operations, vehicles and actors, responding to security-related issues for each transportation mode only may not be sufficient.

### ***Security Concept in Transportation***


As a main function of supply chain, transportation security has a crucial importance on national economies and the global economy. Monroe and Stewart, define transportation as; “the movement of traffic from one point to another” whereas Hayuth defines it as an organizational system which aims to transport goods and people from one place to another by balancing the economic gap between supply and demand centers.

US Research Council, has identified the dangers and threats regarding transportation security as; physical attacks (ex. Bombing), biological attacks (ex. Anthrax release), chemical attacks (ex. physical attack on railcar carrying toxics) and cyber-attacks (Ex. attack on port power and telecommunications).

Reasons of requirement of security in transportation as it;

- Is a critical element of the economy,
- Is a gathering place for groups of people, has symbolic and emotional importance,
- Provides a delivery means for people and products of terrorism,
- Includes institutions with licensing and enforcement responsibilities.

As a critical element of economy, all modes of transportation should be clean, without any gaps, in order to create a sustainable transportation market.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### ***Security Gaps in Transportation Modes***

Transportation mode is; “the method of transport for the carriage of the goods”.

Some authors classify them as; road transport, rail transport, maritime transport, air transport and pipeline transport, where some classify them as; land transport, air transport and maritime transport, by involving road transport and rail transport in the concept of land transport. As a decision variable of transport, unimodal transportation modes we classified into four main categories; land transport, rail transport, maritime transport and air transport.

Some of the common identified gaps in transportation modes;

- The lack of intergovernmental coordination, especially in regard to intelligence,
- The relationship between state action and the private sector,
- The only unit concerned with coordinating security across modes possessing by inadequate powers and resources,
- Little focus on law enforcement.

The security concern in the performance of transportation arises from “security risks” and calculates the “security risks” in transportation modes as; a product of the probability of an incident attempt times the vulnerability of the target times the damage costs of a successful breach of security


$$(Security\ Risk = Probability\ of\ Incident\ Attempt \times Vulnerability \times Damage).$$

There are several different types of safety and security-related issues / gaps related with transportation modes. Classified into three groups as; accidents / crashes, cargo theft and terrorist acts. Piracy, which mostly effects the maritime transportation, can be regarded as another type of safety and security related issue on transportation. According to the above definitions of security and safety; “accidents and crashes” should be regarded as safety related issue, accidents represent unintentional failures on the part of drivers and/or vehicles or deficiencies such as roads and rail tracks and related controls such as air traffic control and signals, whereas cargo theft, terrorist acts and piracy should be regarded as security related issues in transportation.

In this classification, it should be noted that; piracy is an unlawful act against commodity whereas terrorism act is an unlawful act against human life. As a transportation safety related issue “accidents and crashes” play a very important role, especially in road transport whereas road travel has by far the highest fatality risk per distance travelled while rail and air travel are the safest modes per distance travelled.

### ***Maritime Transport***

Shipping has been one of the key stepping stones to economic growth and prosperity throughout its history. 80 % of world trade is carried by sea whilst short-sea shipping

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

carries 40% of intra-European freight. However, “the terrorist threat shows no signs of decreasing and ships and ports alike will continue to face the threat of terrorist acts. Moreover, very serious concerns about acts of piracy and armed robbery at sea persist. A further difficulty relates to incidents involving people smuggling, trafficking and stowaways”. The emergence of the risks in maritime transportation can be grounded in three factors respectively; vulnerability, threat and consequence.

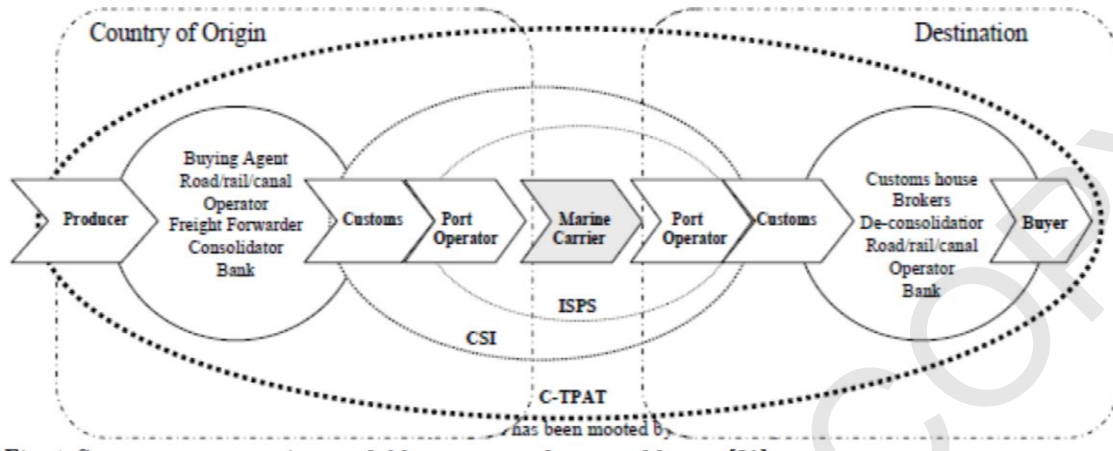
In order to ensure security in maritime transportation, article 3 of the regulation requires; the application of special measures to enhance maritime security of Convention on Safety of Life at Sea (SOLAS) and Part A of the International Ship and Port Facility Security (ISPS) Code, in accordance with the conditions and with respect to the ships, companies and port facilities.

With the aim to provide security culture, has determined the following aims to ensure security in maritime transport:

- Supporting the implementation of international security measures, cooperating closely (especially on continuous training of seafarers),
- Contributing to the international efforts to secure the international supply chain,
- Contributing to safer shipping in the afflicted piracy areas, protecting international shipping lanes against any acts that might disrupt the flow of traffic, establishing resilience plans,
- Working together to ensure adequate improvements to the ISPS Code,
- Promoting cooperation between European maritime training institutions for upgrading seafarers’ competences.
- Adapting requirements to the prerequisites of today’s shipping.

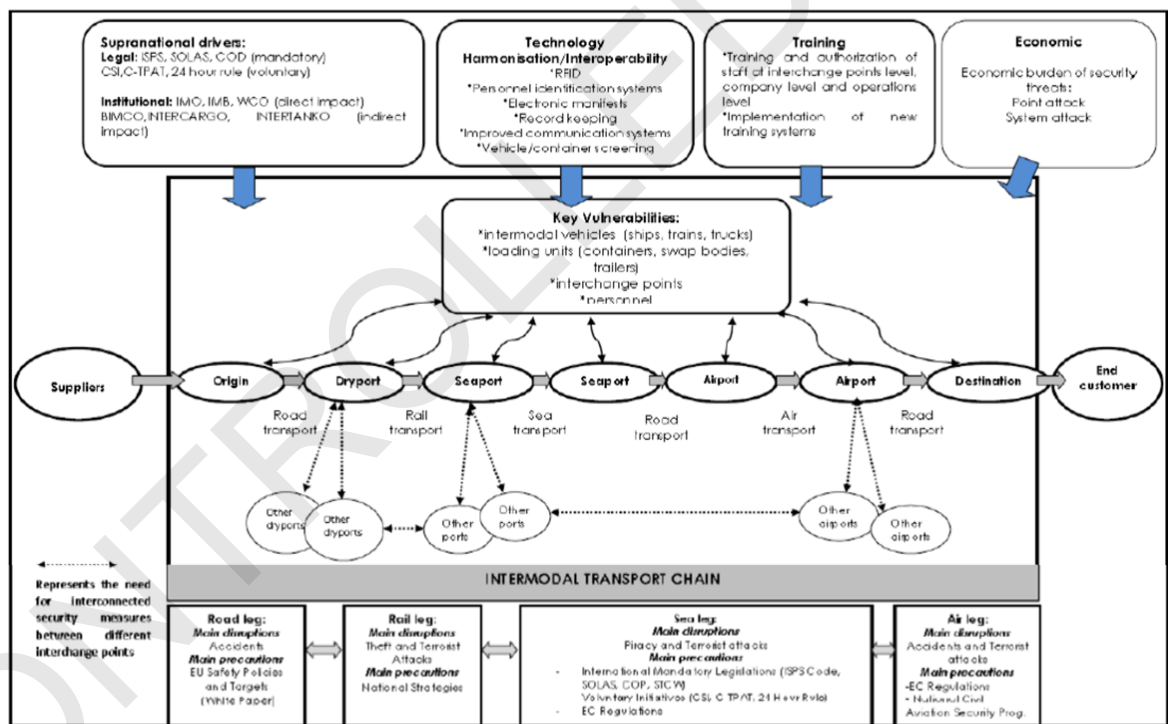
Figure shows the present secure transportation model between producer and buyer in marine transportation. ISPS and CSI applications are focused on reducing the likelihood of terrorist related incidents within application areas and not to strike a balance between efficiencies within the supply chain networks and requisite security assurances. Therefore it should be noted that other unimodal transportation modes (such as road transport, rail transport and air transport) or, in case of an integrated approach, interchange points between various modes will be out of the protection application.






Secure transportation model between producer and buyer

Framework for Intermodal Transport Chain Security



INTERMODAL TRANSPORT SECURITY CONCEPT IN SUSTAINABLE SUPPLY CHAINS

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

## 2. Maritime Security Policy

### 2.1. Relevant international conventions, codes, and recommendations

#### *IMO Maritime Security Measures - Background*

The International Maritime Organization, as the United Nations' regulatory body responsible for the safety of life at sea and environmental protection, has adopted a great number of conventions and regulations since its creation in 1959. Due to the new security challenges imposed by the devastating terrorist acts of 11 September 2001 in the United States, the Organization had to respond swiftly and firmly to any threat against the security of transport by sea. This resulted in the development of the new SOLAS chapter XI-2 on Special measures to enhance maritime security and the International Ship and Port Facility Security Code (ISPS Code).

The terrorist attacks in the United States put in doubt the vulnerability of ships and ports around the world, but they also proved that the maritime industry is determined to stand firm and to respond to one of the biggest challenges of all the times. The new regulatory regime entered into force on 1 July 2004.

These requirements represent the culmination of co-operation between Contracting Governments, Government agencies, local administrations and shipping and port industries to assess security threats and take preventive measures against security incidents affecting ships or port facilities used by international seaborne trade.


#### *History*

The hijacking of the Italian cruise ship Achille Lauro, in October 1985, marked one of the first actual terrorist acts recorded in modern maritime history. Following that incident, the International Maritime Organization adopted resolution A.584(14) on Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews. Subsequently in 1986, taking also account the request of the United Nations General Assembly to study the problem of terrorism on board ships and to make recommendations on appropriate measures, the Organization issued MSC/Circ.443 on Measures to prevent unlawful acts against passengers and crews on board ships.

Pursuant to the Achille Lauro incident the Organization continued working towards the development and adoption of conventions and security regulations and adopted, in March 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA). The Convention, which is a legal instrument, extends the provisions to unlawful acts against fixed platforms located on the Continental Shelf (Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, 1988).

The SUA Convention ensures that appropriate action is taken against persons committing unlawful acts against ships, including the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. The Convention provides for application of



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

punishment or extradition of persons who commit or have allegedly committed offences specified in the treaty.

#### ***Other Security-Related Instruments***

The Organization had adopted other maritime security instruments including:


1. MSC/Circs. 622 and 623, as revised, on Guidelines for administrations and industry on combating acts of piracy and armed robbery against ships;
2. MSC/Circ.754 on Passenger ferry security, providing recommendations on security measures for passenger ferries on international voyages shorter than 24 hours, and ports;
3. Assembly resolution A.871(20) on Guidelines on the allocation of responsibilities to seek the successful resolution of stowaway cases; and
4. 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.

#### ***Activities at the IMO since "September 11"***

In the wake of the tragic events of 11 September 2001 in the United States of America, Assembly resolution A.924(22) (November 2001) 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 aim was to reduce risks to passengers, crews and port personnel on board ships and in port areas and to the vessels and their cargoes and to enhance ship and port security and avert shipping from becoming a target of international terrorism.

The Assembly also agreed to a significant boost to the Organization's technical co-operation programme of GB £1.5 million, to help developing countries address maritime security issues. Subsequently a large number of regional and national seminars and workshops on the enhancement of maritime and port security were held around the world in 2002, 2003 and 2004, with more initiatives launched in 2005. In addition fact-finding and assessment missions and advisory services have been and will continue to be conducted upon request of the countries concerned.

As a result of the adoption of resolution A.924 (22), a Diplomatic Conference on Maritime Security, held at the London headquarters of the International Maritime Organization (IMO) from 9 to 13 December 2002 (the 2002 SOLAS Conference), was attended by 109 Contracting Governments to the 1974 SOLAS Convention, observers from two IMO Member States and observers from the two IMO Associate Members.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

United Nations specialized agencies, intergovernmental organizations and non-governmental international organizations also sent observers to the Conference.

The 2002 SOLAS Conference adopted a number of amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, the most far-reaching of which enshrined the new International Ship and Port Facility Security Code (ISPS Code). The Code 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 second, non-mandatory section (Part B). The Conference also adopted a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the Code and pave the way for future work on the subject.

## **2.2. Relevant government legislation and regulations**


### ***Interagency Government Coordination***

Individual governments delineate the roles of the Designate authority, with regard to responsibilities for port facility security, and the administration, which generally is responsible for ship security for vessels flying its flag. Some nations combine these two roles into one authority. Domestic law or regulation sets forth the division of labor and responsibility between the two entities. Typically, both entities are included in the Department or Ministry responsible for port and shipping matters, such as the Department of Transportation. Port and ship security also may be combined with security for other nodes of transportation, such as rail or aviation.

The Designated Authority may delegate maritime security responsibilities to a Recognized Security Organization (RSO) to undertake duties on its behalf for port facility security. The RSO may be authorized to approve SSPs, certify ship compliance with the measures, conduct PFSa, and provide assistance on completion of PFSAs, PFSPs, SSAs, and SSPs. If the designated Authority utilizes an RSO, it should inform the International Maritime Organization.

Governments also may delegate responsibilities to off-shore international registries, which act subject to oversight of the grating Department or Ministry of Transportation. In other cases, Flag State Administrations may delegate ship security responsibilities to RSOs. But normally, the Administration retains authority to set security levels, established requirements for a Declaration of Security, determine which port facilities should appoint a PFSO and prepare a PFSP, approve PFSAs and PFSPs and subsequent amendments, and exercise control over foreign-flagged SOLAS ships. The administration also typically retains STCW Convention STCW Code accreditation of seafarers.

Depending on the constitutional arrangement or federalist structure of governments, institution or agencies involved on maritime security may be at the


	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

National, regional or prefectural, or local level of governance. Naval and Coast Guard forces conduct maritime security operations that include visit, board, search, and seizure (VBSS) of ships. National customs and immigration forces adopt and implement practices drawn from the World Custom Organization’s Framework of Standard to secure and Facilities Global Trade (Safe Framework), which protects the global cargo supply chain. The foreign ministry is responsible for conducting international outreach and coordination. Intelligence agencies monitor maritime threats and provide information to decision markers local marine law enforcement organization and harbor police patrol internal waters and roadsteads.

Ideally, the department and ministries at the national level coordinate with organizations to develop integrated approaches to maritime security. Ensuring the cohesion of the disparate interagency community of departments, ministries, agencies and organizations is not an easy task. Institutional prerogatives, interagency politics, “stove-piped” authority, duplicate and overlapping authority (or a vacuum of authority) all impede unified action. To overcome these barriers, states may established standing or as hoc committees or officer that can serve as a fusion point for developing and implementing national maritime security policy. Often states establish a single National Maritime Security Committee that include representative from key agencies and departments, and it also may operate a maritime security operational response center to manage search and rescue (SAR), as well as the maritime interdiction of drug traffickers, migrant smugglers, and terrorist and weapons of mass destruction (WMD) at sea.

The ILO/IMO Code of Practice on Port Security suggests that states should develop a port security policy document. Generally, such a document will set forth the extent and significance of the country’s maritime industries and infrastructure, identify key maritime threats, and specify the roles and responsibilities of the various security and law enforcement organizations, the application of national security policy to ports and ships, industry responsibilities, and the delineation of governmental authority.

The ISPS Code and Maritime Security Measures ensure that government and industry are effectively linked. At the same time, coordination across and throughout the levels of government enable effective, proportionate, and sustainable security procedures. Normally these functions are fulfilled by a National Maritime Security Committee, which include representatives from the intelligence community, the merchant shipping industry, and the military. The interagency community generally has to work together to fashion a national concept of the security threats and vulnerabilities, national security priorities, developing maritime security initiatives based upon a national maritime security strategy or framework, developing coordinated position and international treaties and commitments, resolving jurisdictional issues among departments and agencies, and executing national level policy.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### 2.3. Definitions

***Ship security plan***

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

***Company security officer***

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

***Ship security officer***

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

***Port facility***

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

***Ship/port interface***

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

***Ship-to-ship activity***


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

***Port facility security officer***

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

***Designated Authority***

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

***Recognized security organization***

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

***Declaration of Security***

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

***Security incident***

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

***Security level***

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

***Security level 1***

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

***Security level 2***

Means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

***Security level 3***


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

***Pirate Attack***

A piracy attack as opposed to an approach is where a vessel has been subjected to an aggressive approach by a pirate craft AND weapons have been discharged.

***Hijack***

A hijack is where pirates have boarded and taken control of a vessel against the crew's will.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### ***Illegal Boarding***

An illegal boarding is where pirates have boarded a vessel but HAVE NOT taken control. Command remains with the Master. The most obvious example of this is the Citadel scenario.

#### **2.4. Legal implications of action or non-action by security personnel**

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 ISPS Code.

The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of ISPS Code.

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 ISPS Code.

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 part B of ISPS Code.

The company security officer shall ensure the effective co-ordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of ISPS Code.


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

Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels.

A recognized security organization may prepare the ship security plan for a specific ship.

The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations.

In such cases the recognized security organization, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

The submission of a ship security plan, or of amendments to a previously approved plan, for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, have been developed.

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

The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration.

The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment is reinstated, this documentation no longer needs to be retained by the ship.

The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

The plan shall be protected from unauthorized access or disclosure.

Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance, save if:

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

- identification of the restricted areas and measures for the prevention of unauthorized access to them;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;





- procedures for responding to any security instructions Contracting Governments may give at security level 3;
- duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
- identification of the locations where the ship security alert system activation points are provided;
- procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit

### **3. Security Responsibilities**

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

##### ***Obligations of Contracting Governments with respect to security based on SOLAS Chapter XI-2***

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


Contracting Governments shall set security levels and ensure the provision of security-level information to port facilities within their territory, and to ships prior to entering a port or whilst in a port within their territory. When changes in security level occur, security-level information shall be updated as the circumstance dictates.

##### ***Responsibilities of Contracting Governments based on ISPS Code***

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

1. the degree that the threat information is credible;
2. the degree that the threat information is corroborated;
3. the degree that the threat information is specific or imminent; and



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

4. The potential consequences of such a security incident.

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

Contracting Governments may delegate to a recognized security organization certain of their security related duties under chapter XI-2 and this Part of the Code with the exception of:


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

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

### **3.2. Recognized Security Organizations**

Contracting Governments may authorize a recognized security organization (RSO) to undertake certain security related activities, including:

1. approval of ship security plans, or amendments thereto, on behalf of the Administration;
2. verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of ISPS Code on behalf of the Administration; and


	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

3. Conducting port facility security assessments required by the Contracting Government.

An RSO may also advise or provide assistance to Companies or port facilities on security matters, including ship security assessments, ship security plans, port facility security assessments and port facility security plans. This can include completion of a SSA or SSP or PFSA or PFS. If an RSO has done so in respect of a SSA or SSP that RSO should not be authorized to approve that ship security plan.

When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

1. expertise in relevant aspects of security;
2. appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;
3. their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimize such risks;
4. their ability to maintain and improve the expertise of their personnel;
5. their ability to monitor the continuing trustworthiness of their personnel;
6. their ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material;
7. their knowledge of the requirements chapter XI-2 and part A of ISPS Code and relevant national and international legislation and security requirements;
8. their knowledge of current security threats and patterns;
9. their knowledge on recognition and detection of weapons, dangerous substances and devices;
10. their knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
11. their knowledge on techniques used to circumvent security measures; and

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

12. Their knowledge of security and surveillance equipment and systems and their operational limitations.

When delegating specific duties to a RSO, Contracting Governments, including Administrations, should ensure that the RSO has the competencies needed to undertake the task.

### **3.3. The company**

#### ***Specific responsibility of Companies***

The Company shall ensure that the master has available on board, at all times, information through which officers duly authorized by a Contracting Government can establish:

1. who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;
2. who is responsible for deciding the employment of the ship; and
3. in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

#### ***Obligations of the Company***


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

The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities.

#### ***Master's discretion for ship safety and security***

The master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgement of the master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

If, in the professional judgement of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship. In such cases,

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

the master may implement temporary security measures and shall forthwith inform the Administration and, if appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures under this regulation shall, to the highest possible degree, be commensurate with the prevailing security level. When such cases are identified, the Administration shall ensure that such conflicts are resolved and that the possibility of recurrence is minimized.

### **3.4. The ship**

#### ***Ship security***

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


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

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

At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in Level 1, taking into account the guidance given in part B of ISPS Code.

At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in Level 1, taking into account the guidance given in part B of ISPS Code.

Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

- In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.


When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

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

### **3.5. The port facility**

#### ***Port facility security***

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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

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


14.3 At security level 2, additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in level 1, taking into account the guidance given in part B of ISPS Code.

At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in Level 1, taking into account the guidance given in part B of ISPS Code.

In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.

When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security officer and ship security officer shall liaise and co-ordinate appropriate actions.

When a port facility security officer is advised that a ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### 3.6. Ship Security Officer

A ship security officer shall be designated on each ship.

Duties and responsibilities of the ship security officer shall include, but are not limited to:


- undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
- co-ordinating 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;
- co-ordinating 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, if any.

### 3.7. Company security officer

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

Duties and responsibilities of the company security officer shall include, but are not limited to:

- advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- ensuring that ship security assessments are carried out;
- ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- arranging for internal audits and reviews of security activities;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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


### **3.8. Port facility security officer**

A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

Duties and responsibilities of the port facility security officer shall include, but are not limited to:

- conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
- ensuring the development and maintenance of the port facility security plan;
- implementing and exercising the port facility security plan;
- undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
- recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
- 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;
- co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- co-ordinating 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



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

### **3.9. Seafarers with designated security duties**


Seafarers with designated security duties shall meet the standard of competence specified in section A-VI/6, paragraphs 6 to 8 of the STCW Code.

Duties and responsibilities of the Seafarers with designated security duties shall include, but are not limited to:

1. knowledge of current security threats and patterns;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who likely to threaten security;
4. techniques used to circumvent security measures
5. crowd management and control techniques;
6. security related communications;
7. knowledge of emergency procedures and contingency plans;
8. operation of security equipment and systems;
9. testing, calibration and at-sea maintenance of security equipment and systems;
10. inspection, control, and monitoring techniques; and
11. methods of physical searches of persons, personal effect, baggage, cargo, and ship stores.

### **3.10. Port facility personnel with designated security duties**

Port Facility personnel with designated security duties in accordance with the requirements of chapter XI-2 of SOLAS 74 as amended , the ISPS Code, the IMDG Code , the IMO/ILO Code of Practice on Security in Ports, and guidance contained in IMO MSC.1/ Circ. 1341.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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

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

#### **4. Ship Security Assessment**

In order to reach the acceptable security risk level, the company and the ship must always identify potential maritime security threats the ship is likely to be encountered, and must systematically and scientifically analyze the possibility of security damage likely to be caused by the ship and its personnel, cargoes equipment, technical system and operation, and its seriousness of the consequence, and determining the process of the actions taken to mitigate the unacceptable risk, all of which are called “risk-assessment-based decision-making”.

Risk can be shown through the probability and consequence of a given security tampering as the following equation:


$$R = PC$$

where: R — risk value of a given security tampering;

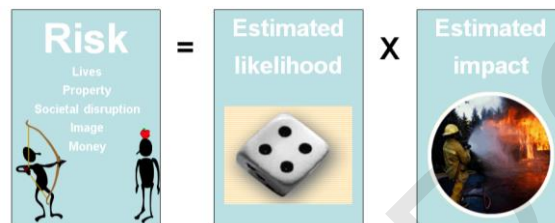
P — probability of a given security tampering. The probability of security tampering can be further defined as the product of the threat (T) and vulnerability (V), i.e.  $P = TV$ ;

C — the sum likely to be resulted from a successful security incident. The consequence can be based on life, economy, symbolized value, environmental influence etc.

In accordance with the principle of risk management, it is generally considered that risk always exists and cannot be eliminated thoroughly. However, risk can be mitigated through management so as to reduce the extent of the consequence (C), to prevent

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

the threat (T), or to mitigate the vulnerability (V). It is usually easier to mitigate vulnerability than to reduce the consequence or threat. The final objective of risk management is to reach a comparatively low risk level. The objective of maritime security is to endure that when threat level increases, the threat can be offset by means of the actions taken to reduce the consequence (C) or to reduce the vulnerability (V). For example, a ship at a port can take actions to add security check when threatened with bomb. Another example is that the ship can require cease of cargo handling, boarding control of personnel from outside, or shifting the ship far from the easily attacked location when lack of ship security officer.



#### 4.1. Risk assessment methodology

##### *General*

For development of the ship security plan, initial and overall ship security assessment is to be carried out so as to evaluate the effectiveness of security measures and procedures for preventing illegal action, and to determine the vulnerabilities of the ship against illegal action.

The result of the ship security assessment is to be used to determine the security measures needed to deal with local security threat considered onboard the ship.


Security level will change due to the changing of ships and time. In order to make full use of ship and shore resources, communication between security officers is very important.

Ship security assessment is to determine:

- need to protect goal;
- security measures having been implemented;
- additional security measures and procedures required.

Ship security assessment is to be subjected to regular review and the ship security plan is to be renewed as necessary.

Security assessment of each ship is to include the following two stages:

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- (1) The first stage is initial evaluation, determining the security threat of the ship under imitating condition of service characteristics, analyzing the risk extent of potential security threat which the ship is capable of dealing with.
- (2) The second stage is final evaluation, identifying vulnerabilities of the ship to prevent security incident, security tampering through site security survey to determine acceptable risks, and determining the risk control measures to mitigate vulnerabilities for unacceptable risks.

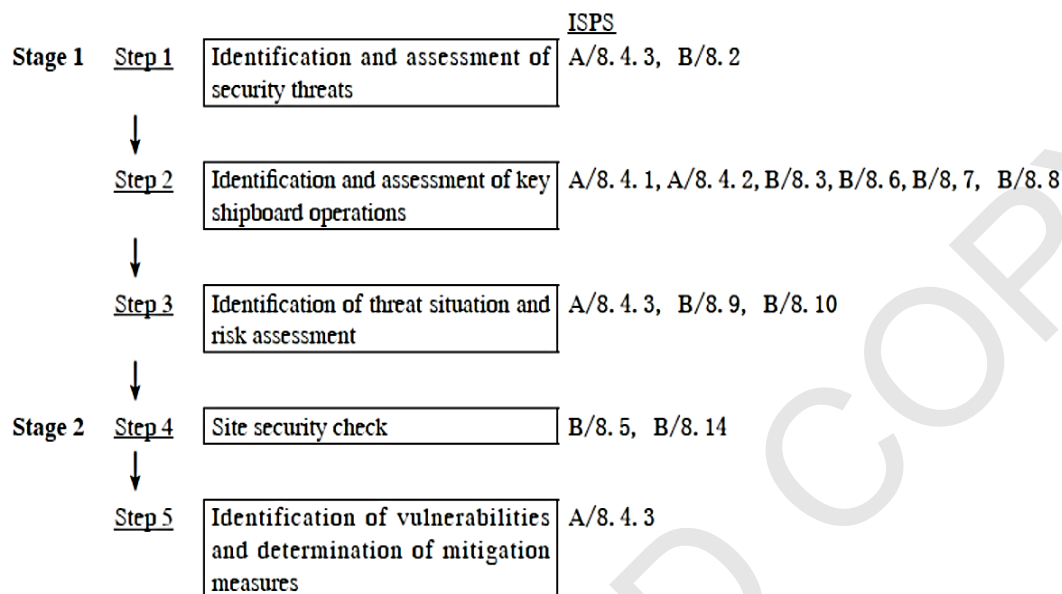
**Note:** The security assessment of a ship is to be carried out through two ways:

- a. single ship — for single ship, security assessment is to be developed including required site security survey of the ship;
- b. general-purpose ship — for general-purpose ship, security assessment is to be carried out covering the security risk assessment of the part or whole of the company's fleet, which is to provide "site security survey" for each ship. Ship security assessment reflects all the related "ship's characteristics".

The result of any ship security assessment is only applicable to specific service environment of the ship, including the structure condition of the ship, navigation areas, loaded cargoes.

When the service environment of the ship changes substantially, the result of ship security assessment is to be reviewed, and the security is to be evaluated when necessary.

The steps and processes of ship security assessment




The following to be considered in ship security assessment

Security capability of the ship is to be evaluated under different security levels against security threat identified, including:

- (1) physical security;
- (2) structure integrity;
- (3) personnel protection system;
- (4) procedure policy;
- (5) radio and radio communication system, including computer system and network; and
- (6) restricted areas.

Personnel carrying out ship security assessment are to have risk evaluation knowledge and skill, and are to have expert assistant in relation to:

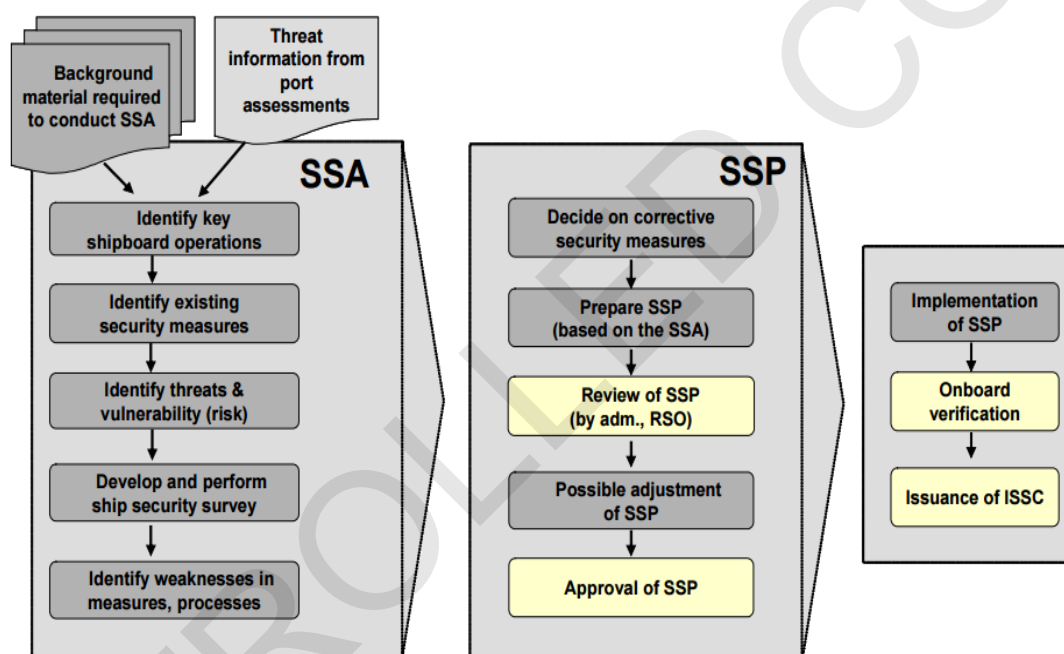
- (1) knowledge of current security threats and patterns;
- (2) recognition and detection of weapons, dangerous substances and devices;
- (3) recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
- (4) techniques used to circumvent security measures;
- (5) methods used to cause a security incident;
- (6) effects of explosives on ship's structures and equipment;
- (7) ship security;
- (8) ship/port interface business practices;
- (9) contingency planning, emergency preparedness and response;
- (10) physical security;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- (11) radio and telecommunications systems, including computer systems and networks;
- (12) marine engineering; and
- (13) ship and port operations.

Note: Expert assistance can be realized by means of a person or a group of persons with the professional knowledge related.

Example of the relation between SSA and the SSP can be illustrated in the following way:




#### 4.2. Assessment tools

The Ship Security Officer must use systematic and consistent approaches to evaluate the security conditions and vulnerabilities.

The operational aspects will be the main focus.

A checklist can/will be used and must include items like:

- General layout of the ship
- Location of areas that should have restricted access, such as the bridge, engine room, radio room etc.
- Location and function of each or potential access point to the ship
- Open deck arrangements including the height of the deck above water
- Emergency and stand-by equipment available to maintain essential services

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- Numerical strength, reliability, and security duties of the ship's crew
- Existing security and safety equipment for protecting the passengers and crew
- Existing agreements with private companies for providing ship an waterside security services
- Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems

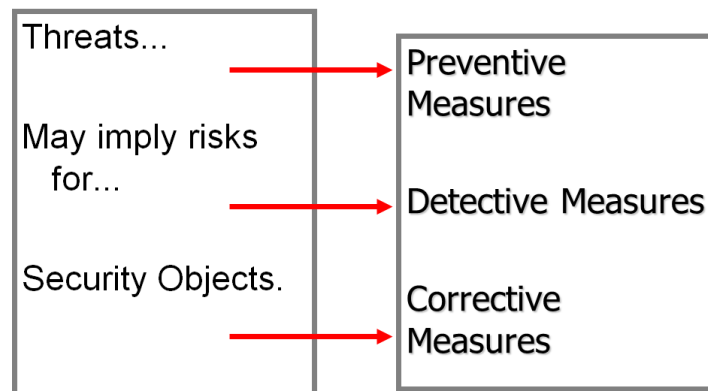
#### **4.3. On-scene security surveys**

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:


1. ensuring the performance of all ship security duties;
2. monitoring restricted areas to ensure that only authorized persons have access;
3. controlling access to the ship, including any identification systems;
4. monitoring of deck areas and areas surrounding the ship;
5. controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
6. supervising the handling of cargo and the delivery of ship's stores; and
7. ensuring that ship security communication, information, and equipment are readily available.

#### ***The survey should fulfill the following functions:***

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





	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

#### **4.4. Security assessment documentation**

The SSA should take into account all possible vulnerabilities, which may include:

1. conflicts between safety and security measures;
2. conflicts between shipboard duties and security assignments;
3. watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;
4. any identified security training deficiencies; and
5. any security equipment and systems, including communication systems.

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

Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

If the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO.

### **5. Security Equipment**

#### **5.1. Security equipment and systems**

Each ship is required to be fitted with a ship security alert system which when activated shall initiate and transmit a ship to shore security alert to a competent authority designated by the administration. Such a system is designed to be activated from the navigational bridge and from another place on a ship. The purpose of AIS is to ensure automatic transmission of ship's identity, position and other relevant data with large and quick movements of personnel and cargo. It is not possible to now rely only on physical examination as a method of ensuring security. Highly sophisticated equipment and system which include X rays, Robots, Explosive detection systems of different types, Biometrics, and cameras of various types are now in use all over the world to track down terrorist and saboteurs.

**AIS****Benefits of AIS**

Operating in the VHF maritime band, the AIS (Automatic Identification System) system enables the wireless exchange of navigation status between vessels and shore-side traffic monitoring centers. Commercial ships, ocean-going vessels and recreational boats equipped with AIS transceivers broadcast AIS messages that include the vessel's name, course, speed and current navigation status.

- Transmit your position. Fitting a Class A or Class B AIS transceiver ensures that you are seen by other AIS equipped vessels.
- Vessel Protection. As part of a suitably configured network, AIS enables owners to be alerted to unauthorized vessel movements.
- Port management. AIS can be used as a highly effective port management tool allowing easy identification, control and direction of vessels.
- Coastal surveillance. AIS and radar can be fused to create effective and efficient coastal tracking, surveillance and safety systems.

The regulation applies to ships built on or after 1 July 2002 and to ships engaged on international voyages constructed before 1 July 2002, according to the following timetable:

- passenger ships, not later than 1 July 2003;
- tankers, not later than the first survey for safety equipment on or after 1 July 2003;
- ships, other than passenger ships and tankers, of 50,000 gross tonnage and upwards, not later than 1 July 2004.

An amendment adopted by the Diplomatic Conference on Maritime Security in December 2002 states that, additionally, ships of 300 gross tonnage and upwards but less than 50,000 gross tonnage, are required to fit AIS not later than the first safety equipment survey after 1 July 2004 or by 31 December 2004, whichever occurs earlier. (The original regulation adopted in 2000 exempted these vessels.)

**Ship Security Alert System**

The ship security alert system (SSAS) allows transmission of a silent security alert to a flag state authority when the security of the ship is under threat or has been compromised.



### **Ships to be provided with a SSAS**


According to the international requirements regarding the security of ships and of port facilities (SOLAS XI-2, regulation 6) ships must be provided with a SSAS as follows

1. Ships constructed on or after 1 July 2004,
2. Passenger ships and passenger high-speed craft constructed before 1 July 2004 not later than at the first survey of their radio installation after 1 July 2004,
3. Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high-speed craft of 500 GT and above constructed before 1 July 2004 not later than at the first survey of their radio installation after 1 July 2004.
4. other cargo ships of 500 GT and above constructed before 1 July 2004 and mobile offshore drilling units not later than at the first survey of their radio installation after 1 July 2006.

### **Locks**

In accordance with the ship security plan, all doors allowing access to the bridge, engine-room, steering gear compartments, officers' cabins and crew accommodation should be secured and controlled in affected areas and should be regularly inspected. The use of surveillance equipment to monitor the areas as well as regular patrolling can be of merit. The intention should be to establish secure areas which attackers will find difficult to penetrate.

Securing by locking or other means of controlling access to unattended spaces adjoining areas could also prove useful.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

As there have been occasions when entire crews have been locked up, consideration should be given to secreting equipment within areas in which the crew could be detained to facilitate their early escape.

The Master's cabin is one of the main objectives of the assailants who are looking for money and the master keys to other living quarters, to steal the crew's personal effects of value and nautical equipment from the bridge. The cabins and other living quarters should be kept locked whenever their occupants are absent.


Open portholes can be an easy access to clever criminals: close them with the clips in place always when you leave. Try also to keep the accesses to internal areas locked, guaranteeing the entry and exit by the gangway watchman.

Try to reduce the opportunities of robbery by putting all portable equipment which is not in use to its place of storage. Valuables left exposed tempt opportunistic thieves, keep them in safe place under lock and key.

### ***Lighting***

Ships should use the maximum lighting available consistent with safe navigation, having regard in particular to the provisions of Rule 20(b) of the 1972 Collision Regulations. Bow and overside lights should be left on if it can be done without endangering navigation. Ships must not keep on deck lights when underway, as it may lead other ships to assume the ship is at anchor. Wide beam floods could illuminate the area astern of the ship. Signal projector lights can be used systematically to probe for suspect craft using the radar guidance if possible. So far as is practicable crew members on duty outside the ship's secure areas when in port or at anchor should avail themselves of shadow and avoid being silhouetted by deck lights as this may make them targets for seizure by approaching attackers.

Based on specific information on acts of piracy and armed robbery at sea in specific regions, ships may consider travelling blacked out except for mandatory navigation lights. This may prevent attackers establishing points of reference when approaching a ship. In addition, turning on the ship's lights as attackers approach could alert them that they have been seen, dazzle them and encourage them to desist. It is difficult, however, to maintain full blackout on a merchant ship. The effectiveness of this approach will ultimately depend in part on the level of moonlight, but primarily on the vigilance of the ship's crew. While suddenly turning on the ship's light may alarm or dazzle attackers, it could also place the crew at a disadvantage at a crucial point through temporary loss of their night vision.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### ***GMDSS equipment***

The system is intended to perform the following functions: alerting (including position determination of the unit in distress), search and rescue coordination, locating (homing), maritime safety information broadcasts, general communications, and bridge-to-bridge communications. Specific radio carriage requirements depend upon the ship's area of operation, rather than its tonnage. The system also provides redundant means of distress alerting, and emergency sources of power.

Recreational vessels do not need to comply with GMDSS radio carriage requirements, but will increasingly use the Digital Selective Calling (DSC) VHF radios. Offshore vessels may elect to equip themselves further. Vessels under 300 Gross tonnage (GT) are not subject to GMDSS requirements.

### GMDSS sea areas

GMDSS sea areas serve two purposes: to describe areas where GMDSS services are available, and to define what radio equipment GMDSS ships must carry (carriage requirements). Prior to the GMDSS, the number and type of radio safety equipment ships had to carry depended upon its tonnage. With GMDSS, the number and type of radio safety equipment ships have to carry depends upon the GMDSS areas in which they travel. GMDSS sea areas are classified into four areas: area1, area2, area3 and area 4.

In addition to equipment listed below, all GMDSS-regulated ships must carry a satellite EPIRB, a NAVTEX receiver (if they travel in any areas served by NAVTEX), an Inmarsat-C SafetyNET receiver (if they travel in any areas not served by NAVTEX), a DSC-equipped VHF radiotelephone, two (if between 300 and less than 500 GRT) or three VHF handhelds (if 500 GRT or more), and two 9 GHz search and rescue radar transponders (SART).

#### Sea Area A1

An area within the radiotelephone coverage of at least one VHF coast station in which continuous digital selective calling (Ch.70/156.525 MHz) alerting and radiotelephony services are available. Such an area could extend typically 30 to 40 nautical miles (56 to 74 km) from the Coast Station.

#### Sea Area A2

An area, excluding Sea Area A1, within the radiotelephone coverage of at least one MF coast station in which continuous DSC (2187.5 kHz) alerting and radiotelephony services are available. For planning purposes, this area typically extends to up to 180 nautical miles (330 km) offshore during daylight hours, but would exclude any A1 designated areas. In practice, satisfactory coverage may often be achieved out to around 150 nautical miles (280 km) offshore during night time.





**Sea Area A3**

An area, excluding sea areas A1 and A2, within the coverage of an Inmarsat geostationary satellite. This area lies between about latitude 76 Degrees North and South, but excludes A1 and/or A2 designated areas. Inmarsat guarantees their system will work between 70 South and 70 North though it will often work to 76 degrees South or North.

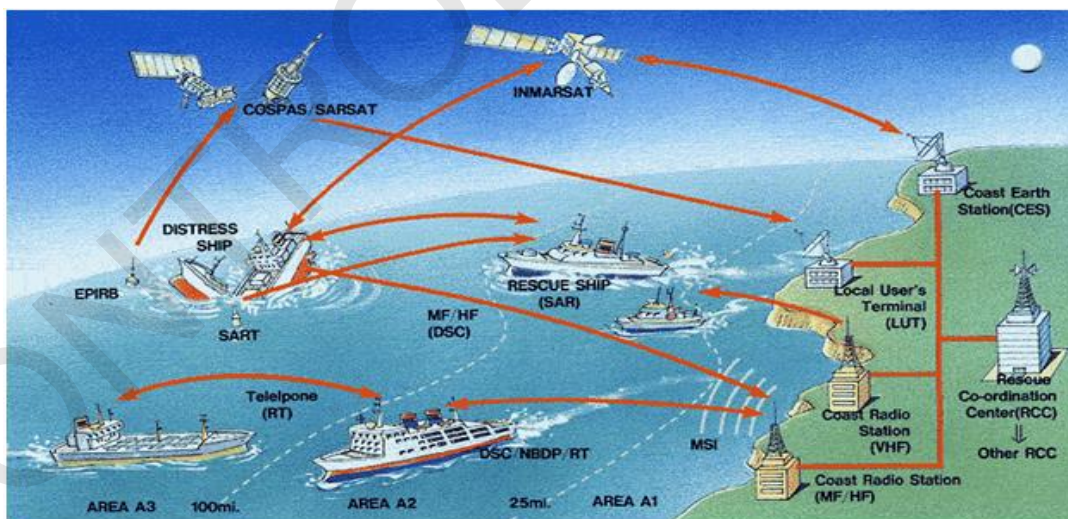
**Sea Area A4**

An area outside Sea Areas A1, A2 and A3 is called Sea Area A4. This is essentially the polar regions, north and south of about 76 degrees of latitude, excluding any A1, A2 and A3 areas.

**GMDSS radio equipment required for U.S. coastal voyages**


Presently, until an A1 or A2 Sea Area is established, GMDSS-mandated ships operating off the U.S. coast must fit to Sea Areas A3 (or A4) regardless of where they operate. U.S. ships whose voyage allows them to always remain within VHF channel 16 coverage of U.S. Coast Guard stations may apply to the Federal Communications Commission for an individual waiver to fit to Sea Area A1 requirements. Similarly, those who remain within 2182 kHz coverage of U.S. Coast Guard stations may apply for a waiver to fit to Sea Area A2 requirements.

As of August 2013, the U.S. Coast Guard provides a Sea Area A1 service through its Rescue 21 system.



**Closed Circuit Televisions**

Owners may wish to consider providing closed-circuit television (CCTV) coverage and recording of the main access points to the ship's secure areas, the corridors approaching the entrances to key areas and the bridge. The allocation of additional personnel to guarding and patrolling of restricted areas can be a useful preventive measure.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

In the event of attackers gaining temporary control of the ship, crew members should, if it is safe and practicable, leave Close Circuit Television (CCTV) records running.

Any CCTV or other recording of the incident should be secured. If practicable, areas that have been damaged or rifled should be secured and remain untouched by crew members pending possible forensic examination by the security forces of a coastal State. Crew members who came into contact with the attackers should be asked to prepare an individual report on their experience noting, in particular, any distinguishing features which could help subsequent identification of the attackers. A full inventory, including a description of any personal possessions or equipment taken, with serial numbers when known, should also be prepared.

### ***Metal detectors***

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

### ***Explosive detectors***

Any explosive material has the following characteristics


- a. It is chemically or otherwise energetically unstable.
- b. The initiation produces a sudden expansion of the material

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

#### **Classifications**

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



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### *Primary Explosives*

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

### *Secondary Explosives*

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

### *Detonation*


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

### *Baggage screening equipment*

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

### *X-ray Systems*

The most usual method of screening baggage and personal belongings is to use X-ray equipment and modern equipment are capable of producing images of good definition and penetration. However, X-ray examination can also be defeated, e.g. X-rays may not detect explosives and plastic weapons nor will they allow identification of the actual liquid in bottles or other containers. Moreover, it is possible to camouflage the image of weapons and devices by the use of other dense materials, such as lead crystal glass. The use of X-ray equipment must, therefore, also be accompanied by a percentage physical check of baggage including a proportion that does not arouse suspicion. The use of X-rays is a very effective method of screening bags and other items provided certain conditions are met, e.g. operator efficiency decreases significantly after only a relative short time, particularly at peak screening periods. For this reason, operators should only scan X-ray images for a maximum of 20 minutes and then be employed on other duties,

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

such as a physical search, for 40 minutes before returning to the console. It is also essential that the image is presented for an adequate time to permit proper examination and a minimum of 5 seconds is considered necessary for this. Screening techniques will vary depending upon whether the equipment presents a fixed or scrolling (moving) image.

### ***Alarms***

Alarm signals, including the ship's whistle, should be sounded on the approach of attackers.

Alarms and signs of response can discourage attackers. Alarm signals or announcements which provide an indication at the point at which the attacker may board, or have boarded, may help crew members in exposed locations select the most appropriate route to return to a secure area.

Announcements made by the crew should be made in the working language of the ship. The crew initial familiarization checklist should specifically state the various alarms used on board the vessel, the response and muster station to each of these alarms. The alarms and alarm signals should be standardized throughout the fleet and not be specific.


### ***Use of distress flares***

The only flares authorized for carriage on board ship are intended for use if the ship is in distress and is in need of immediate assistance. As with the unwarranted use of the distress signal on the radio, use of distress flares simply to alert shipping rather than to indicate that the ship is in grave and imminent danger may reduce their effect in the situations in which they are intended to be used and responded to. Radio transmissions should be used to alert shipping of the risk of attacks rather than distress flares. Distress flares should only be used when the master considers that the attackers' actions are putting his/her ship in imminent danger.

### ***Use of passive and non-lethal devices***

The use of passive and non-lethal measures such as netting, wire, electric fencing, and long-range acoustic devices may be appropriate preventive measures to deter attackers and delay boarding.

The use of water hoses should also be considered though they may be difficult to train if evasive manoeuvring is also taking place. Water pressures of 80 lb per square inch and above have deterred and repulsed attackers. Not only does the attacker have to fight against the jet of water but the flow may swamp his/her boat and damage engines and electrical systems. Special fittings for training hoses could be considered which would also provide protection for the hose operator.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

A number of spare fire hoses could be rigged and tied down to be pressurized at short notice if a potential attack is detected.

Employing evasive manoeuvres and hoses must rest on a determination to successfully deter attackers or to delay their boarding to allow all crew members to gain the sanctuary of secure areas.

Continued heavy wheel movements with attackers on board may lessen their confidence that they will be able to return safely to their craft and may persuade them to disembark quickly. However, responses of this kind could lead to reprisals by the attackers if they seize crew members and should not be engaged in unless the master is convinced he can use them to advantage and without risk to those on board. The following equipments should not be used if the attackers have already seized crew members:

- Handheld radios
- Automatic Intrusion Detection Device (Burglar Alarm)
- General alarm
- Long Range Acoustic Device (LRAD)
- Razor wire
- Electric fencing
- Yacht radar
- Netting

## **5.2. Operational limitations of security equipment and systems**


“Repelling pirate attacks: the measures to protect a ship”

Maintaining vigilance is essential. All too often the first indication of an attack has been when the attackers appear on the bridge or in the master’s cabin. Advance warning of a possible attack will give the opportunity to sound alarms, alert other ships and the coastal authorities, illuminate the suspect craft, undertake evasive manoeuvring or initiate other response procedures.

Signs that the ship is aware it is being approached can deter attackers.

When ships are in, or approaching areas of known risk of piracy or armed robbery, bridge watches and look-outs should be augmented, bearing in mind that many attacks are mounted from astern. Additional watches on the stern or covering radar “blind spots” should be considered.

Companies should consider investing in low-light binoculars for bridge staff and look-outs. Radar should be constantly manned but it may be difficult to detect low profile fast moving craft on ship’s radars. Yacht radar mounted on the stern may provide additional radar cover capable of detecting small craft approaching from astern when the ship is underway. Use of appropriately positioned yacht radar when the ship is at anchor may also provide warning of the close approach of small craft.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

It is particularly important to maintain a radar and visual watch for craft which may be trailing the ship when underway but which could close in quickly when mounting an attack. Small craft which appear to be matching the speed of the ship on a parallel or following course should always be treated with suspicion. When a suspect craft has been noticed, it is important that an effective all-round watch is maintained for fear the first craft is a decoy with the intention to board the ship from a second craft while attention is focused on the first.

In addition to the use of overt means of transmitting alerts, the ship security alert system could be used in the event of a piracy or armed robbery attack. It should, however, be borne in mind that certain non-disclosure issues prevail with regards to the configuration and locations of the system.

Companies owning or operating ships that frequently visit areas where attacks occur should consider the purchase and use of more sophisticated visual and electronic devices in order to augment both radar and visual watch capability against attackers' craft at night, thereby improving the prospects of obtaining an early warning of a possible attack. In particular, the provision of night vision devices, small radars to cover the blind stern arcs, closed circuit television and physical devices, such as barbed wire, may be considered. In certain circumstances non-lethal weapons such as acoustic devices, may also be appropriate. Infrared detection and alerting equipment may also be utilized.

### **5.3. Testing, calibration and maintenance of security equipment and systems**


The SSO is responsible for the storage and control of all shipboard security equipment, including the identification card system.

Security equipment must be serviced, maintained, and repaired in accordance with manufacturers' recommendations. This ensures the equipment will perform continually (including consideration of the effects of inclement weather conditions and power disruptions).

Each company should add the specific maintenance requirements.

Any equipment or system failure or malfunction shall be reported immediately.

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

## 6. Ship Security Plan

### 6.1. Purpose of the Ship Security Plan

Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in Part A of the ISPS Code.

The company security officer (CSO) has the responsibility of ensuring that a ship security plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The ship security assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

### 6.2. Contents of the ship Security Plan

Such a plan shall be developed, taking into account the guidance given in part B of ISPS Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:


- measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;
- identification of the restricted areas and measures for the prevention of unauthorized access to them;
- measures for the prevention of unauthorized access to the ship;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- procedures for responding to any security instructions Contracting Governments may give at security level 3;



- procedures for evacuation in case of security threats or breaches of security;
- duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- procedures for auditing the security activities;
- procedures for training, drills and exercises associated with the plan;
- procedures for interfacing with port facility security activities;
- procedures for the periodic review of the plan and for updating;
- procedures for reporting security incidents;
- identification of the ship security officer;
- identification of the company security officer including 24-hour contact details;
- procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
- frequency for testing or calibration of any security equipment provided on board;
- identification of the locations where the ship security alert system activation points are provided; and
- procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts. footnote

All SSPs should:

- detail the organizational structure of security for the ship;
- detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
- detail the basic security measures for security level 1, both operational and physical, that will always be in place;
- detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;
- provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and
- detail reporting procedures to the appropriate Contracting Government's contact points.

In addition the SSP should establish the following which relate to all security levels:

- the duties and responsibilities of all shipboard personnel with a security role;
- the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;
- the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;
- the procedures and practices to protect security sensitive information held in paper or electronic format;
- the type and maintenance requirements, of security and surveillance equipment and systems, if any;
- the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and
- procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

### **6.3. Confidentiality issued**





The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. The plan shall be protected from unauthorized access or disclosure.

Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9, save in circumstances specified:

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

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

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


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

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

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

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

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

#### **6.4. Implementation of the Ship Security Plan**

It is important to understand that no matter how perfect is the plan. it will be ineffective unless it is implemented properly. It is the duty of the ship's security officer to ensure that the plan is implemented on board in letter and spirit. He is to ensure that all the personnel on board the ship are conversant with their security related duties.

In order to ensure that the plan is optimally implemented onboard, the ship security officer should regularly exercise the ship's crew in security exercises and drills. Before commencement of the exercise, the personnel involved should be brief on the purpose of the exercise. On completion, a debrief should be carried out to appraise the personnel of any shortcomings.

An important aspect of the implementation of the ship's security plan is to critically examine it from the point of view of shortcomings.

#### **6.5. Maintenance and modification of the Ship Security Plan**

It needs to be appreciated that over a period of time, the plan may need to be amended to cater to any changed circumstances. The SSO must therefore, identify these changes and propose remedial measures. He can, thereafter in consultation with the ship's master, propose changes in the plan to the company security officer. As the plan is a document approved by the administration, the amendments to the plan must be approved.

Para 9.3 of Part A of ISPS Code states that amendments to a previously approved plan shall be accompanied by the security assessment on the basis of which the amendments has been developed. In a nutshell it would suffice to say that the plan is based on an assessment of various related factors. As and when any of these factors change, the assessment changes and hence the plan must be amended to cater for the changes.

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

The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5 Part A of ISPS Code, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment is reinstated, this documentation no longer needs to be retained by the ship.



## 7. Threat Identification, Recognition, and Response

### 7.1. Recognition and detection of weapons, dangerous substances and devices



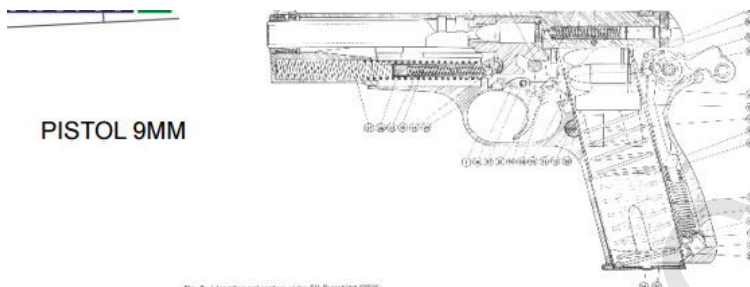
#### *Weapons*

Recognition and detection of weapons, dangerous substances and devices

- Not as easy as it sounds, within the military and civilian field there numerous cases to attend from using different weapons to identifying foreign equipment and weapons of various sizes, designs, makes , models etc. And the experience gained cannot be passed on overnight.
- It requires experts in the relevant fields to be able to recognize and detect weapons, dangerous substances and devices. What we are concerned with is the prevention of such materials entering the ports and on board vessels. To achieve this we require controls similar to airport security systems.
- X-Ray screening to detect weapons made of metal, plastic, ceramics etc.
- Low powered radar sensors to detect weapons
- Walk through detectors
- Trace detectors for dangerous substances and confirming cargos, illegal immigrants etc.
- Screening containers for chemical, biological, radioactive or nuclear cargo
- Dirty bombs - Radioactive material surrounded by explosive. Detonation spreads the radioactivity over a wide area, killing potentially hundreds of people and leaving whole areas uninhabitable for decades. As reported in the press Feb 1 2003 British Intelligence services have uncovered a plot by Al Qaeda to build a nuclear dirty bomb after discovering documents in Heart in Afghanistan indicating that the bomb had been assembled. The whereabouts are unknown and it is feared it could have been moved along the smuggling routes which spread west from Heart close to the Iranian border.

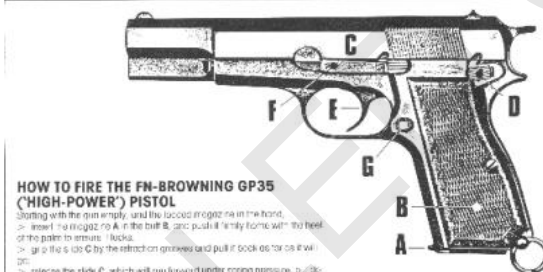


- To make ourselves less vulnerable by the use of education, awareness and the introduction of security procedures coupled with important intelligence will enable crews and personnel to identify suspicious materials and report them to the correct authorities for identification.



PISTOL 9MM

Fig. 6. A longitudinal section of the FN-Browning GP35.  
Courtesy of Fabrique Nationale.



AK 47 / AKM - RUSSIA, CHINA, SOVIET BLOCK STATES



Assault Rifles




Heckler Koch - GERMANY/- Heckler Koch (Germany / UK)UK

Machine Pistols



Cal: 9mm  
Weight: 3.425kg (7.55lb)  
Length: 368mm (14.49")  
CRFire: 550rpm  
Mag: 32rnds

 Ingram - MAC 10 (USA)



INGRAM (MAC 10) - USA

Cal: .45  
Weight: 3.818kg (8.4lb)  
Length: 269mm (10.59")  
CRFire: 1.145rpm

Uzi - Israel



UZI - ISRAEL

Cal: 9mm  
Weight: 3.11kg ((6.85lb)  
Length: 360mm (14.17")  
CRFire: 950rpm  
Mag: 20,25,32rnds





SKORPION - CZECH



Favourite weapon of the PLO

Skorpion favourite weapon for the PLA

GRENADES





***Dangerous Substances***

**BANNED SUBSTANCES: COCAINE**



**BANNED SUBSTANCES: SLEEPING MEDICIN**



**BANNED SUBSTANCES: ECSTACY**



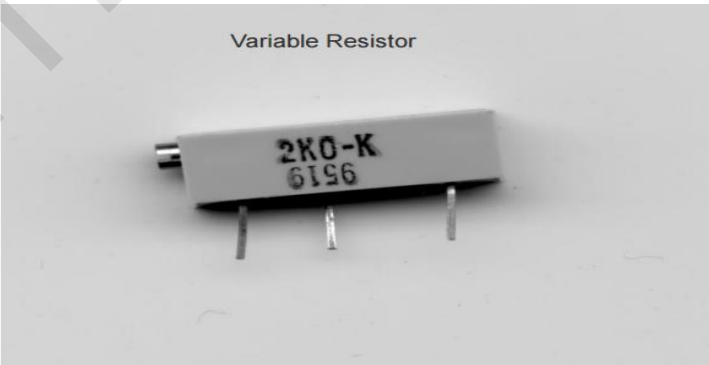
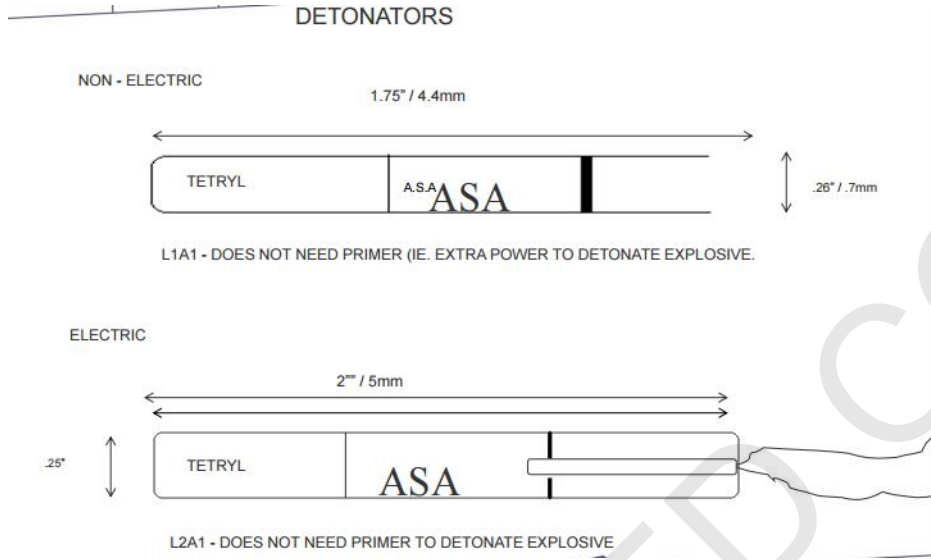
**BANNED SUBSTANCES: MARIJUANA/HASH/WEED**

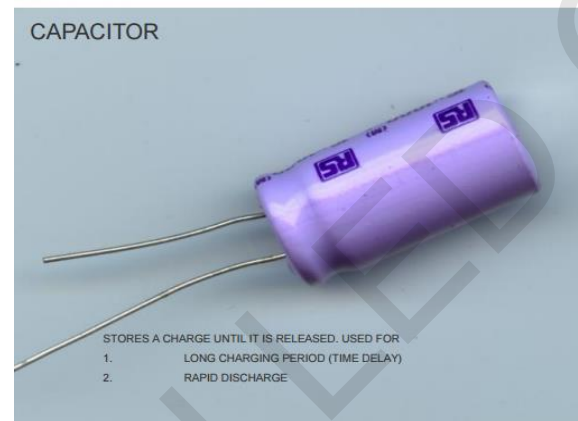
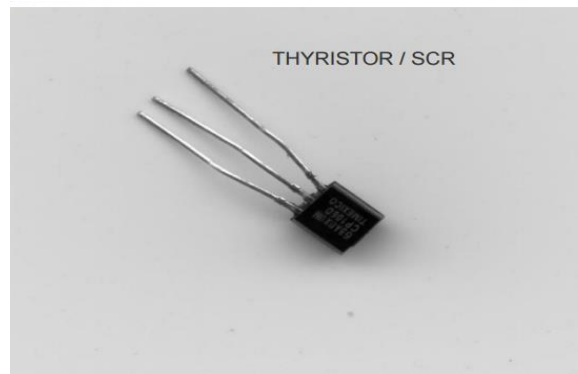




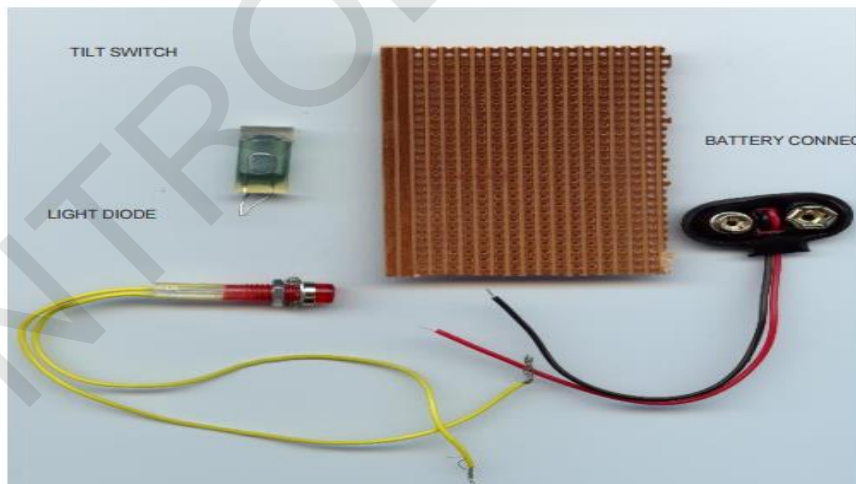


Devices






ADDITIONAL EQUIPMENT



**Recognition and detection of weapons, dangerous substances and devices**

- X-Ray screening
- Low powered radar sensors
- Walk through detectors
- Trace detectors
- Screening containers

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

***Techniques to circumvent security measures***

- Surveillance and reconnaissance
- Target reconnaissance
- Rehearsals
- Attack
- Individual
- Information Technology
- Access
- Airborne
- Subsurface

***How can we get around these security measures?***

The criminal or terrorist as an individual or as a group should be treated with the up most respect. The modern terrorist at the height of his profession in some cases is on par with military and civil forces.

He conducts surveillance and reconnaissance collating timely, accurate and critical information to contribute to the overall political objectives which their group or faith are trying to achieve.

Target reconnaissance, plans, procedures, patterns, lapses in security, lack of checks etc.

Rehearsals – support from sympathetic countries and funding

These are obviously on the large scale, to bring it down to a basic level;


Information Technology – fraud, hackers, gaining vital info on cargos and shipping movements and security plans etc.

Access – there are numerous ways to enter the ship whether it is alongside, at anchor or underway

Craft marry up together then split, losing radar signature, using local conditions

Board a ship midships or stern by the use of poles and ladders and adapted climbing equipment whilst underway

Access ladders, gangways, ramps, doors, side scuttles, windows and ports whilst at anchor or alongside.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

And of course stealing a ship by hijacking gaining access by smaller craft or even helicopter and roping down terrorists let alone flying an aircraft into the side of a vessel And lets not forget Subsurface attack whilst at anchor or in port, placement of explosives or boarding etc.

The list is endless and a terrorist or criminal will allow their imagination run wild to achieve their objectives.

## **7.2. Methods of physical searches and non-intrusive inspections**

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


### Search System and Methods

- A search of unlocked spaces
- A search locked spaces
- Personal search locations
- Physical searching
- Metal detection
- Baggage screening
- Heavy baggage
- Vehicles
- Other freight
- Deliveries to ships

### ***Methods of Search***

- Physical Searching

Physical searching is best carried out in a screened off area, as privacy minimises embarrassment and increases effectiveness. People being searched should not be given the opportunity of selecting a particular searcher. One officer should be delegated to

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

observe people waiting and note suspicious behaviour and allocate persons to available searchers to ensure no over-loading.

- **Metal Detection**

People can be screened by passing through an archway pre-set to trigger an alarm if a certain amount of metal is carried through. Hand-held metal detectors can be used for screening individuals. However, metal detectors will not pick up explosives, plastic weapons or inflammable liquids carried in glass or plastic containers. Metal detection should be augmented by a physical search of a proportion of those being screened, including some who do not alarm the detector. This would increase the chances of detection and acts as a powerful deterrent.

- **Baggage Screening**

- **Metal Detectors** - Metal detectors are of little use for screening baggage and personal belongings since most bags and brief-cases have locks, hinges and other metal components which would result in a very high alarm rate. Moreover, hand-held detectors have a limited depth of effective penetration.
- **Vapour Detection** - Air sampling systems, either static or hand-held, can be used to detect high concentrations of some explosives. However, currently no commercial system is capable of detecting all forms of explosives.
- **X-Ray Systems** - Modern equipment is capable of producing images of good definition and penetration. However, X-ray examination may not detect explosives and plastic weapons nor will it allow identification of the actual liquid in bottles or other containers. Moreover, it is possible to camouflage the image of weapons and devices by the use of other dense materials, such as lead crystal glass. The use of X-ray equipment must therefore also be accompanied by a percentage physical check of baggage, including a proportion of baggage that does not arouse suspicion. Operator efficiency decreases significantly after only a relatively short time, particularly at peak screening periods, so individual operators should only scan X-ray images for a maximum of 20 minutes and then be employed on other duties, such as a physical search, for 40 minutes before returning to the console. Each image should be presented for a minimum of 5 seconds to permit proper examination. Any baggage whose image arouses suspicion, or contains a dark area which could conceal a weapon or device, should be physically searched.
- **Physical Search** - A physical search of baggage, when considered necessary, should include a check for false compartments, often used for the smuggling of weapons and devices. Although false "bottoms" are most usual, devices have been incorporated around the sides of cases, in the lids and in the compartments of holdalls. A smell of glue, or a heavy odour to mask the smell of glue or explosives, may be an indication that a lining may have been stuck



back in position. Attention should be paid to any tampering or repair to a case, non-standard or unmatched case components, and also to greasy stains or small holes in the case exterior. If the baggage weight seems disproportionate, or the bag is unbalanced for no obvious reason, then a further check for a false compartment would be justified. Particular attention should be paid to electrical and electronic apparatus, such as radios, which have often been used as containers for devices to avoid detection under X-ray examination. Equipment may be examined for unusual characteristics: signs of tampering, excessive weight, loose objects inside (rotate, don't shake). X-ray the equipment if suspicions are aroused. Treat all new, packaged equipment in the same manner as used models.

- Use of Dogs - Specially trained dogs can be very effective in searching cars, baggage and freight. Dogs can also be used for searching in ships but will need to be trained for the seagoing environment to achieve results.

- Heavy Baggage

The screening of heavy baggage could be done by a central X-ray machine supported by physical search. It is another area where the use of dogs trained to sniff out explosives may well be beneficial. Like passenger screening, once heavy baggage has been screened it is essential it should be marked and kept under surveillance. Rules related to reconciling passengers to their baggage should be established and adhered to.

- Vehicles

At high threat levels, a high proportion of vehicles might need to be searched. The deterrent effect of this is considerable. As with baggage, dogs trained to sniff explosives can be used, but physical search is the most reliable method. Where random searching or percentage screening is in force, the advice of security services should be sought in selecting which vehicles to search. If possible, a covered shed with nearby X-ray equipment should be chosen so that suspect packages can be subjected to X-ray examination. If shore screening is non-existent, ships might spot search vehicles on board if they are unable to do this before boarding. Although difficult, this may be necessary at high threat levels and should be practised. Vehicle owners/drivers should accompany all such searches and should not be allowed to land once their vehicle is on board without the express authority of a responsible ship's officer and the notification to shore authorities. The searching of freight trailers before boarding is notoriously difficult, but measures may need to be taken to meet this problem. This will involve co-operation from shore staff. Careful examination of paperwork and screening of drivers, coupled with reaction to good intelligence, goes some way to solving this problem. Customs are closely concerned with freight and should be consulted. For the future, developments in air sampling systems may improve the ability to check freight. In the final event, trailers can be 'unstuffed' and physically searched using all methods mentioned above, including sniffer dogs.



- Other Freight

Checking freight, especially bulk aggregates and liquids, is extremely difficult and costly but might need to be done on a random basis in response to a specific threat.

- Deliveries to Ships

Terrorists may well use innocent, miscellaneous vehicles and people delivering stores to a ship. Good access control, personnel identification and random searches will help to counter this risk.

### **7.3. Implementing and coordinating searches**

In order to ensure that a thorough and efficient search can be completed in the shortest possible time, a search plan, specific of the ship could be prepared in advance.

This plan will be reviewed from time to time and modified in the light of experience. It is comprehensive and details the routes searchers should follow and all the places on the route that a device could be secreted. The plan is presented in a logical manner to cover all options and to ensure no overlap or omission. The plan allows a searcher to concentrate on the actual searching without worrying about missing something.

When searching, it should be borne in mind that a terrorist may try to match the device to the background, such as a tool box in an engine room.

The preparation of a system of check cards for individual vessels is a useful contingency, one being issued to each searcher which specifies the precise route to be followed and the areas to be searched. The cards are colour coded for different areas of responsibility, e.g. blue for deck areas, red for engine room etc. On completion of an individual search task the card is to be returned to a central control point, so that when all cards are in the search is known to be complete.


In addition to a comprehensive search plan, a plan for a fast search or 'quick look' of the more vulnerable and accessible areas has been drawn up.

Using the card system, selected cards only will be issued to cover the vulnerable and accessible areas.

Such a fast search might be carried out where:

- there is a short warning time before a potential bomb detonation
- security management judges that a received bomb threat needs investigating
- an opportunity occurs to conduct a quick search.



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### ***Types of Search***

There are two types of search:

#### **Reactive Search**

This type of search will be carried out in reaction to a specific threat or piece of hard intelligence indicating that a bomb or weapons have been placed on the ship. It can also be used as a precaution during times of heightened threat. Whenever a reactive search is ordered it will comply with the following principles:


- the searchers should be familiar with the area being searched so that out of the ordinary items are noticed
- the search should be conducted according to a specific search plan or schedule and must be carefully controlled by officers and management
- searchers must be able to recognise a potential bomb or incendiary device
- there must be a system of marking or recording searched or 'clean' areas
- a central control point should be established to which the searchers report
- searchers should be able to communicate with the search controllers
- searchers must know precisely what to do if a suspected device is found.

**Preventive Search** – This aims to deter terrorists from smuggling bombs or arms on board a ship or into a terminal or restricted area, and to enable the crew to find these devices if the terrorist tries to smuggle them in. The following principles apply to all preventive searching:

- places should be established where people and goods are checked or searched before they pass into the restricted area. Once in the area, segregation is essential and no contact must be allowed with unchecked persons or goods. The percentage of persons/goods searched will, of course, depend on the threat level.
- once in the area, no person or vehicle should be allowed to leave the area or land from a ship without the knowledge of the person controlling the search.
- car, baggage and freight reconciliation with owners/drivers is a key objective.
- restricted or sterile areas and the access to them should be searched. The frequency of such searches will be dictated by the threat level.

#### ***Search System and Search Methods***

Ship's search system will be based on the crew searching their own area of work under their normal officer or senior rating. In this way, an unusual object is more likely to be identified. Search parties will work in pairs with one searching "high" and one searching "low". If a suspicious object is found, one of the pair will remain on sentry while the other reports the find. To manage any search efficiently ship's staff will use UHF/VHF radios but operating channels should be limited to those previously worked during the voyage. The search controller (eg. SSO) will keep a record of all reports from the search

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

groups to ensure all spaces are checked and that the master always has an up to date search status. During the search routine any lifts should be turned off.

The search system can be divided into two stages:

**A search of unlocked spaces** - since most unused spaces should be locked a rapid search of vulnerable areas can be achieved by:

- checking all locked or sealed doors to ensure they have remained locked and sealed
- searching all unlocked spaces, lifts and rubbish bins
- search group leaders advising the SSO on completion of searches of their allocated spaces
- the SSO keeping a record of all reports from search group leaders to ensure that the master has an up to date status report.

**A search of locked spaces** - if warranted, a full search of locked spaces and lift shafts can follow with:

- all locked spaces and lift shafts being thoroughly searched using the necessary pass keys
- all crew accommodation, lockers, wardrobes and drawers being thoroughly searched
- search group leaders advising the bridge on completing the search of their allocated spaces
- the SSO keeping a record of all reports from search group leaders to ensure that the master has an up to date status report.

The discovery of one device should not be the end of a search as there is always the possibility that more than one has been planted.

The owners of any unattended baggage, unclaimed luggage or abandoned packages found during a search should be sought while clearing the area adjacent to the suspect item.

#### **Personnel Search Locations**

A centralised search point ashore is generally most economical in terms of equipment, personnel and space and it allows control services such as police, customs and immigration to integrate more easily. If necessary, the Port Facility Security Officer should be asked to make suitable arrangements.

However, keeping the "clean passengers" segregated after search may present problems of organisation and surveillance. A search at the gangway head has the disadvantage of allowing potential terrorists to get close to their target. Also space in ships is at a premium compared with ashore, and long queues of passengers, or other visitors to the



ship, waiting on an open gangway to pass the search control may cause irritation. However, this option may be necessary when there is no on shore screening or when, during a high level of threat, a double check is necessary.

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

***Cabins***

- Back sides and underneath drawers
- Between bottom drawer and deck
- Beneath bunks, e.g. taped to bunk frame under mattress
- Under wash basin
- Behind removable medicine chest
- Inside radios, recorders etc
- Ventilator ducts
- Inside heater units
- Above or behind light fixtures ☐Above ceiling and wall panels
- Cutouts behind bulkheads, pictures, etc.
- False bottom clothes closets-hanging clothes
- Inside wooden clothes hangers
- Inside rolled socks, spare socks
- Hollowed-out molding

***Companionways***

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

***Toilet and Showers***

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

***Deck***

- Ledges on deck housing, electrical switch rooms, winch control panels
- Lifeboat storage compartments, under coiled rope, in deck storage rooms



- Paint cans, cargo holds, battery rooms, chain lockers.

***Engine room***

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

***Galleys and Stewards' Stores***

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




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

***Behavioural characteristics of persons who are likely to threaten security***

- Individuals:
  - Criminal seeking to extort money
  - Refugees seeking political asylum
  - Mentally disturbed
- Groups

What type of people carry out such crimes and what type of character are they?

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- **Individual pirates/hijackers**

- Criminal seeking to extort money
- Refugees seeking political asylum
- Mentally disturbed – the mentally abnormal have a marked inferiority complex, nervousness, hijacking provides an opportunity for the insecure to prove themselves and achieve personal publicity. They could be armed with a hoax weapon or have a bomb in a contained package or wired to devices as suicide bombers, they do not have to be mentally disturbed just a believer in their faith!


- **Groups**

- The politically motivated groups of terrorists operate in groups of 2-5, but can be larger dependent on the task in hand, It will possibly be only the leader who will know the overall plan
- They will possibly know the layout of the vessel, the security and crew procedures and have a fundamental understanding of navigation. They will be well equipped with communications, modern weapons and explosives, which could have been prepositioned on board in advance. They will primarily attempt to access the bridge and using the shock of an armed assault as part of their technique will inevitable gain control of the ship. They will then try to locate the crew/passengers into one part of the ship to ease guarding and control. Initially ruthless, irrational and heavy handed, the elation of their success may ebb away and concern for their own safety and security will be of concern. Unless suicide bombers etc. their aggressive tendencies will reappear as the vessel approaches land or set deadlines.

***Examples of suspicious behaviors include:***

- PERSON(S) SEEN IN AREA FOR NO OBVIOUS REASON
- PERSON(S) NOT DRESSED FOR THAT PARTICULAR AREA OR FUNCTION
- PERSON(S) SEEN IN AREA MORE THAN ONCE OR IS NECESSARY
- PERSON(S) BEING NERVOUS, SWEATY WHEN COMING ABOARD SHIP
- PERSON(S) HAVING LITRITATURE OR PAPERWORK THAT SEEM TO BE OF A
- SUSPICIOUS NATURE
- PERSON(S) BEING IN POSSESSION OF LARGE SUMS OF MONEY
- PERSON(S) MEETING OTHER PERSONNEL NOT ASSOCIATED WITH THAT PARTY OR CREW
- PERSON(S) BEING IN AREAS OF THE SHIP THAT THEY HAVE NO REASON TO BE THERE OR ARE TAKING A PARTICULAR INTEREST IN A PART

**7.5. Techniques used to circumvent security measures**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

Methods of attack on ships vary considerably depending on the circumstances and the position in which the vessel finds herself. Ships at anchor are extremely vulnerable and can be easily boarded from small boats under cover of darkness. Combined attacks on vessels that are tied up alongside are also common, for example, seemingly innocent parties engaged on board the ship as stevedores are in fact found to be dropping stolen goods over side into waiting, motorized canoes a method employed extensively in Central American regions, where the culprits can make a speedy getaway up or down a river, away from the ship's berth.

In the area of Indonesia, Thailand, the Malacca Straits and the South China Sea a common practice is where fast launches pace the target vessel, which is often underway and making way at quite a fast speed. During the hours of darkness the craft close the ship to within grapple range while both craft are at speed, at which point the ship is boarded. Boarding in this way is not without considerable risk to the individual and is made easier with vessels having a low freeboard.

One of the main objectives of a boarding party is to obtain control of the ship's main operational areas such as the bridge and the engine room. By intimidation of crew, and especially the Master, boarders can then engage in the theft of cash, ship's equipment, parcels of cargo and personnel effects. On occasions, it has also been the practice for boarding to take place with stealth in mind, to force the Master to open the safe without the alarm being raised and make an equally discreet escape without raising the attention of the crew. This method may possibly reflect some inside knowledge of the ship's internal arrangement.


### ***Typical Pirate attacks***

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

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

- Skiffs only – usually two.
- Open whalers carrying significant quantities of fuel often towing 2 or more attack skiffs.
- Motherships which have included the very largest of merchant ships, fishing vessels and dhows.

These Motherships have been taken by the pirates and usually have their own crew onboard as hostages. Motherships are used to carry pirates, stores, fuel and attack skiffs to enable pirates to operate over a much larger area and are significantly less affected by the weather. Attack skiffs are often towed behind the Motherships. Where the size of

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

the Mothership allows it, skiffs are increasingly being carried onboard and camouflaged to reduce chances of interdiction by Naval/ Military forces.

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

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

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

#### **7.6. Crowd management and control techniques**

Crowd Management is not only about controlling the crowd, but also managing the crowd with confidence, knowledge, effective communication and leadership. While all crew need to become familiar with crowd management, it is mandated by STCW for masters, officers and other personnel who are designated on Muster Lists to assist passengers in emergency situations on passenger vessels.

The human behavior under stress is very difficult to predict. With the term stress we express, “psychological stress designating unpleasant emotional states evoked by the threatening environmental events or stimuli”.

There are situations where this behavior becomes irrational. This is usually described by the term ‘panic’. This has been observed during egress situations where crowd crushes and people show an element of competitiveness.

Lives may be lost, for example, through fear of using staircases in which there is some smoke but which would actually give safe passage out of a ship”.

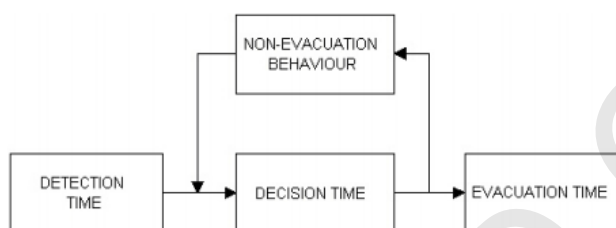
It is obvious that there is a period of situation assessment between the acoustical signal and the decision to act and evacuate. Other possible actions before the initialization of the evacuation process is the assembly of a family or the decision of the preferred exit from the particular room.



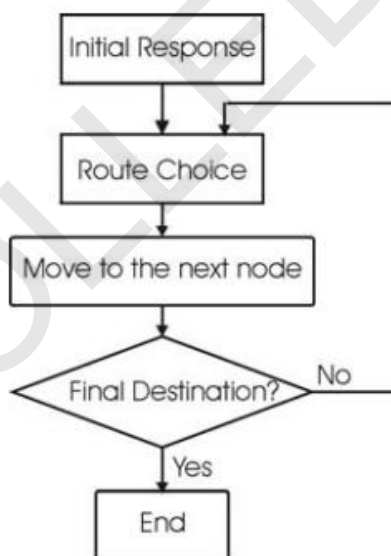


Therefore the time for a crowd to escape from a situation of potential entrapment is a function of T (time to escape) = t1 (time to start to move) + t2 (time to move to and pass through exits), rather than T = t2.

Of course competitive behavior that affects the crowd in case of panic, as they attempt to acquire something that they believe will lead them to safety, makes them irrational and results in jamming the exits and causes injuries that all result in large time delays.



*Simplifies approximation of the human behavior in case of an evacuation signal*



*The evacuation process for each person*

## 8. Ship Security Actions

### 8.1. Actions required by different security levels

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

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




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

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

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

At **security level 3**, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in Part A section 7.2 of ISPS Code, taking into account the guidance given in part B of ISPS Code. The ship should comply with the instructions issued by those responding to the security incident or

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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:

1. limiting access to a single, controlled, access point;
2. granting access only to those responding to the security incident or threat thereof;
3. directions of persons on board;
4. suspension of embarkation or disembarkation;
5. suspension of cargo handling operations, deliveries etc;
6. evacuation of the ship;
7. movement of the ship; and
8. preparing for a full or partial search of the ship.

Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.


Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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

## **8.2. Maintaining security of the ship/port interface**

### ***Reporting requirements for the ship prior to entering port***

- **Delivery of ship's stores**

The security measures relating to the delivery of ship's stores should:

1. ensure checking of ship's stores and package integrity;
2. prevent ship's stores from being accepted without inspection;
3. prevent tampering; and
4. prevent ship's stores from being accepted unless ordered.


For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

#### Security level 1

At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:

1. checking to ensure stores match the order prior to being loaded on board; and
2. ensuring immediate secure stowage of ship's stores.

#### Security level 2

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

### Security level 3

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

1. subjecting ship's stores to more extensive checking;
2. preparation for restriction or suspension of handling of ship's stores; and
3. refusal to accept ship's stores on board the ship.


- **Handling unaccompanied baggage**

The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship. It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

### Security level 1

At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 %, which may include use of x-ray screening.

### Security level 2

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 % x-ray screening of all unaccompanied baggage.

### Security level 3

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

1. subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
2. preparation for restriction or suspension of handling of unaccompanied baggage; and
3. refusal to accept unaccompanied baggage on board the ship.

- **Monitoring the Security of the Ship**


The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

1. lighting;
2. watchkeepers, security guards and deck watches, including patrols; and
3. automatic intrusion–detection devices and surveillance equipment.

When used, automatic intrusion–detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

### Security level 1

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watchkeepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary. While under way, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulations for the Prevention of Collisions at Sea in force. The following should be considered when establishing the appropriate level and location of lighting:

1. the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;
2. coverage should include the area on and around the ship;
3. coverage should facilitate personnel identification at access points; and
4. coverage may be provided through coordinating with the port facility.

#### Security level 2

At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

1. increasing the frequency and detail of security patrols;
2. increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;
3. assigning additional personnel as security look-outs; and
4. ensuring co-ordination with water-side boat patrols, and foot or vehicle patrols on the shore-side, when provided.

Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by co-ordinating with the port facility to provide additional shoreside lighting.

#### Security level 3





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


1. switching on of all lighting on, or illuminating the vicinity of, the ship;
2. switching on of all on-board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;
3. maximising the length of time such surveillance equipment can continue to record;
4. preparation for underwater inspection of the hull of the ship; and
5. initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

### **8.3. Usage of the Declaration of Security**

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

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

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

5.4 The Declaration of Security shall be completed by:

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

The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

#### **8.4. Reporting security incidents**

***Model of message in case reporting attacks and attempted attacks by pirates and armed robbers.***

- SHIPS' MESSAGE FORMATS

**Report 1:** Initial message - Piracy/armed robbery attack alert

1. Ship's name and, callsign, IMO number, INMARSAT IDs (plus ocean region code) and MMSI

MAYDAY/DISTRESS ALERT (see note)

URGENCY SIGNAL

PIRACY/ARMED ROBBERY ATTACK

2. Ship's position (and time of position UTC)

Latitude Longitude

Course Speed KTS

3. Nature of event



**Note:** It is expected that this message will be a Distress Message because the ship or persons will be in grave or imminent danger when under attack. Where this is not the case, the word MAYDAY/DISTRESS ALERT is to be omitted.

Use of distress priority (3) in the INMARSAT system will not require MAYDAY/DISTRESS ALERT to be included.

**Report 2:** Follow-up report - Piracy/armed robbery attack alert

- Ship's name and, callsign, IMO number
- Reference initial PIRACY/ARMED ROBBERY ALERT
- Position of incident

Latitude      Longitude

Name of the area

- Details of incident, e.g.:

While sailing, at anchor or at berth?

Method of attack

Description/number of suspect craft

Number and brief description of pirates/robbers

What kind of weapons did the pirates/robbers carry ?

Any other information (e.g., language spoken)

Injuries to crew and passengers

Damage to ship (Which part of the ship was attacked?)

Brief details of stolen property/cargo

Action taken by the master and crew

Was incident reported to the coastal authority and to whom?

Action taken by the Coastal State

- Last observed movements of pirate/suspect craft, e.g.:

Date/time/course/position/speed

- Assistance required

- Preferred communications with reporting ship, e.g.:

Appropriate Coast Radio Station

HF/MF/VHF

INMARSAT IDs (plus ocean region code)

MMSI

- Date/time of report (UTC)

**8.5. Implementation of security procedures**



The security measures must be scalable to provide protection at three security levels. The major elements of these requirements are:

- Designating facility, ship and company security officers
- Conducting ship and facility security assessments
- Developing ship and facility security plans
- Providing security training commensurate with job function
- Instituting access control
- Designating restricted areas
- Implementing facility/ ship interface
- Conducting security monitoring

## 9. Emergency Preparedness, Drills, and Exercises

### 9.1. Contingency planning

#### *Example of action to take in case of breach of security*

- **Response to hijack cases**

#### Action to follow when ship is hijacked

Behave as follow when hijacker or terrorist came on board the ship.

- a. Keep calm and advise all officers and members of crew to keep calm. Do not try to resist armed terrorists unless as a last resort in a clear life threatening situation.
- b. Ensure the safety of the ship
- c. Activate the ship security alert system
- d. (when ship is not fitted with the ship security alert system) Broadcast a distress message, if possible. Procedures to transmit alert signals to shore authority or to the company under distress or threatened situation should be prepared beforehand.
- e. Offer reasonable co-operation. Terrorists are very nervous and aggressive at the incident. Calm behavior of the master and officers may mitigate the strain of terrorists.
- f. There is danger that a terrorist gets excited. Among the terrorist there exists who has abnormal character, and seeking an excuse for murder. This excuse is intentionally built up by misunderstanding. Abuse of a special privilege or aggression should not be returned.
- g. Hijackers are unlikely to understand how a particular ship works, its capabilities and limitations and may be suspicious about routing operations. They need be relieved through trust of ship's personnel who respond without deception.
- h. Try to establish what group of terrorists is involved as early as possible.
- i. Try to increase the number of access point to the vessel. Without risk.
- j. Without suggesting what they may be, seek to establish the hijackers' demands and what deadlines have been set for meeting them.



- k. Assume that the incident will be prolonged. The longer incident drags on, the more likely they are to end without injury to the hostages.
- l. Recognize that hostages will feel isolated during the incident, as they will be unaware of steps being taken by the company and/or government authorities on their behalf. This can lead to antagonism against the authorities and sympathy for the terrorists. Every effort will be being made to end the incident with the utmost emphasis on the preservation of life and personal safety of all innocent parties involved.
- m. Understand that establishment of a reasonably rapport between hostages and captors are likely to reduce the chances of the terrorists acting violently against their hostages.
- n. Be aware that at some stage in the incident a confrontation between the terrorists and outside authorities may occur. Before this confrontation, an opportunity may arise or may be created to pass information about the hijackers, such as their number, descriptions, sex, how they are armed, how they deploy themselves, how they communicate with each other, their cause, nationality, language(s) spoken and understood, their standard of competence and their level of vigilance, and whether any of the hostages have been separately unidentified as to nationality, religion or occupation (e.g. forces personnel).
- o. Wherever and whenever possible, the hijackers should be encouraged to surrender peacefully and should be discouraged from mistreating either passengers or crew.

In the event or in anticipation of military action:

- a. Do not react to strangely dressed newcomers.
- b. Do not attract attention to any unusual activity.
- c. If shooting, or the loud command "GET DOWN", is heard immediately lie face down, cover ears, close eyes and slightly open mouth. Do not move until an "all clear" is given.
- d. If the loud command "STAND STILL" is heard, then freeze immediately.
- e. If the location of terrorist bombs or weapons is known, inform a member of the military assault force as soon as possible.
- f. Do not shelter or hide terrorists.
- g. Do not take photographs of the military assault force.

Following the incident, the master and his crew should avoid talking to the press and other media persons about the methods used to resolve the incidents.

- **Bomb threat (Intimidation)**

Initial Action

- When there is threatening of bomb, a person who received telephonic menace shall ask the following questions.
  - When does the bomb explode?



- Where is the bomb?
- What shape does it have?
- What type of bomb?
- What measure causes it to explode?
- Have you placed the bomb?
- By what reason?
- Where are you calling from?
- Where is your address?
- What is your name?
- Take notes of characteristics of voice you heard
  - Calm            Slow            Crying            Obscure
  - Stammer      Deep            Loud            Smattering (broken)
  - Giggle        Accent        Angry            Fast
  - Stressed      Nasal voice    Exiting with a slip
- Disguised      Sincere      Screaming      Normal
- Have you ever heard of the voice, or it resembles somebody?
- Have you heard a background noise?
- Take note of the wording spoken correctly
- When ship is in port, report this telephone to the shore authority. (harbor master, police, fire, fighter, etc.)

Subsequent action

- Activate the ship security alert system
- Ring emergency bell. All members of crew stand on emergency station.
- Organize the search group, and explain them on the bomb threat.
- Fire hoses set at fire station, and prepare for emergency measure against hull damage.
- Prepare the unloading plan
- Prepare the stability calculation

- **Unidentified Object/Explosive on Shipboard**

Initial Action

Activate the ship security alert system, and report to company and agent of nearest port about the description and others of the object accurately

- appearance, size, color, fittings
- location found on shipboard
- Do not put it in water or play water on it as this could short a control circuit and denote it
- Do not run in the vicinity of the device
- Do not use VHF/UHF radios in the vicinity, within 3m, of the device.



- Do not handle, touch, shake, open or move suspected explosives or suspected devices.
- Do not cut, pull or touch wires, switches, fuses or fastenings.
- Do not step on fuses.
- Do not pass metallic tools near the suspected device
- Do not move switches, open hooks or fastenings.
- Do not smoke near by.
- Do not get too near the device to inspect.
- Do not move the device away from people – move people away from the device.
- Do not come close to the device

#### Subsequent Action

- Put sandbags or mattress around the suspected device.
- Clear neighborhood including above and below of the device. ( 6 planes)
- Identify restricted area, and instruct the crew to keep away.
- Keep the doors and openings open, so as to minimize primary damage.
- Obey instructions given by the company and shore authorities.

If a bomb explodes without warning, onboard or near the ship, the master should,

- Ensure watertight integrity and stability.
- Render first aid where/if necessary
- Take fire-fighting precautions
- Muster personnel to establish number and names of casualties.
- Inform company, local authorities (in port), and make distress call (at sea) if necessary.
- In port, be prepared to handle inquiries from press and next-of-kin.

- **Bomb Threat/Damage and Destruction to Port Facility**

- Activate the ship security alert system.
- Issue order to stand on emergency station.
- Report to the Contracting Government of the port facility.
- Obey instructions given by personnel responding to the threat (PFSO)
- Prepare to evacuate from the ship/ prepare departure of ship from the port.

- **Procedure for responding to pirates attack**

#### Action when encountered with Attackers/Pirates

- Blow whistle to alert the crew and other ships.
- Increase ship's speed, and change the course to seaside, if possible.
- Light up the upper deck and ship's side, when appropriate, and hit the light to possible attackers, using searchlight, to dazzle them.





- If pirates/attackers try to endanger the ship, shoot rocket flares.
- If intruders try to get onboard using a hook, cut the rope of the hook.
- Activate the ship security alert system.
- (when ship is not fitted with this system) Give alert to shore authority and other ships in the vicinity. (When the pirate/armed robbers assaulted the ship, transmit the distress signal using the DSC device. GMDSS of INMARSAT is transmitting the pirate information via INMARSAT-C)

Action to take when Attackers/Pirates get on shipboard

Once the pirate gets on board, the action to take by the master and crew differs depending on the degree how much the attackers take command of the ship. However, the objectives of the master and crew are:

- to ensure safety of persons on board with the greatest possible effort;
- to ensure operation of ship by the member of crew;
- to ensure leaving of attackers from ship as soon as possible.

In any case, never expose human life to danger by challenging against violence to protect the properties on board.

Evacuate in pre-determined safe place, as appropriate, and ensure that all personnel are staying there. Members of crew should pay effort to stay together.

Report the circumstances using radio equipment and seek to get help, if possible. When intruder forbids use of radio, crew should pay attention on their ability to monitor the use of radio equipment


Crew should not stay in between the intruders and their boat. Because this would increase the risk of injury or violence. Priority should be given that the intruders may easily leave off a alongside the ship.

As a rule, not try to arrest the attackers. This action works to induce violence.

When the ship is hijacked by the intruders, liaise with them, if possible, to take command of ship's operation and seek to return hostages. However, in many cases, only one option to ensure safety is to accept the requirement of the attackers.

Action to take after assault is over

- Issue pre-determined signal to announce the finish of assault.
- Ensure safety of personnel and the ship.
- Call the roll to confirm all members of crew are on board.
- Inspect if anyone injured.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

- Report to RCC.
- Ask for medical advice over radio, if needed.

- **Procedures for responding to stowaway cases**

When a stowaway is found, the master shall immediately inspect this person. In order to identify this person, the ship shall collect as much document as possible pertaining to him such as passport, seamen's not, ID card, physical check record, letters, etc.

In general, a stowaway denies his possession of document, and uses a false name and false nationality. However, in many cases, the stowaways hold their identity paper in secret, near the compartment where they were found. Therefore, the ship should perform a systematic search of document.

Most important action at finding of stowaway is to report to the company, immediately, of this fact together with all information available.

Also report to the authority and agent where the stowaway came onboard, and to the same of next port.

Refrain from raising uproar for the stowaway, But give him a room and meal. During navigation along coastal water and in port, keep him in calm in locked room, and avoids unnecessary contact of crewmember with him, until further instruction is issued.


In general, ship's deviation just for disembarkation of the stowaway is not permitted in the charter party. He shall be disembarked only after approval of the company.

## **9.2. Security drills and exercises**

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 part B of ISPS Code.

The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security-related deficiencies, which need to be addressed.

To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25% of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship, within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as those security threats listed in Part B paragraph 8.9 of ISPS Code.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>


Should consider all possible threats, which may include the following types of security incidents:

- damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the ship or of persons on board;
- tampering with cargo, essential ship equipment or systems or ship's stores;
- unauthorized access or use, including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the ship to carry those intending to cause a security incident and/or their equipment;
- use of the ship itself as a weapon or as a means to cause damage or destruction;
- attacks from seaward whilst at berth or at anchor; and
- attacks whilst at sea.

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, co-ordination, resource availability, and response. These exercises may be:

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

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

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### 9.3. Assessment of security drills and exercises

Purpose of carrying out an assessment at the end of each drill


- verify if the crew understood the procedures and duties, based in the respond rapidly and effectively in an emergency situation
- evaluate if the new crew be familiar with the vessel, her equipment and her procedures
- help to identify how your procedures might be improved
- Analyze if you and your crew are prepared to make decisions under pressure
- help check that your safety gear is working and fix it if necessary
- Crew could identified the mistakes made or deficiencies during the drill

## 10. Security Administration

### 10.1. Documentation and records

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

1. training, drills and exercises;
2. security threats and security incidents;
3. breaches of security;
4. changes in security level;
5. communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
6. internal audits and reviews of security activities;
7. periodic review of the ship security assessment;

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

8. periodic review of the ship security plan;
9. implementation of any amendments to the plan; and
10. maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment.

The records shall be protected from unauthorized access or disclosure.

***Duration and validity of Certificate***


An International Ship Security Certificate shall be issued for a period specified by the Administration which shall not exceed five years.

When the renewal verification is completed within three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing Certificate.

When the renewal verification is completed after the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing Certificate.

When the renewal verification is completed more than three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

If a Certificate is issued for a period of less than five years, the Administration may extend the validity of the Certificate beyond the expiry date to the maximum period specified in Part A section 19.3.1 of ISPS Code, provided that the verifications referred to in section Part A 19.1.1 of ISPS Code applicable when a Certificate is issued for a period of five years are carried out as appropriate.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

If a renewal verification has been completed and a new Certificate cannot be issued or placed on board the ship before the expiry date of the existing Certificate, the Administration or recognized security organization acting on behalf of the Administration may endorse the existing Certificate and such a Certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

If a ship at the time when a Certificate expires is not in a port in which it is to be verified, the Administration may extend the period of validity of the Certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and then only in cases where it appears proper and reasonable to do so. No Certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new Certificate. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the expiry date of the existing Certificate before the extension was granted.

A Certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the date of expiry of the existing Certificate before the extension was granted.

If an intermediate verification is completed before the period specified in Part A section 19.1.1 ISPS Code, then:

1. the expiry date shown on the Certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;
2. the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by section 19.1.1 are not exceeded.

A Certificate issued shall cease to be valid in any of the following cases:

1. if the relevant verifications are not completed within the periods specified under Part A section 19.1.1 ISPS Code;
2. if the Certificate is not endorsed in accordance with Part A section 19.1.1.3 and 19.3.7.1 ISPS Code, if applicable;



3. when a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and
4. upon transfer of the ship to the flag of another State.

In the case of:

1. a transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports, or
2. a Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in Part A section 19.4.2 ISPS Code.

#### ***Continuous Synopsis Record***

Every ship to which SOLAS chapter I applies shall be issued with a Continuous Synopsis Record.


The Continuous Synopsis Record is intended to provide an on-board record of the history of the ship with respect to the information recorded therein.

For ships constructed before 1 July 2004, the Continuous Synopsis Record shall, at least, provide the history of the ship as from 1 July 2004.

The Continuous Synopsis Record shall be issued by the Administration to each ship that is entitled to fly its flag and it shall contain, at least, the following information:


1. the name of the State whose flag the ship is entitled to fly;
2. the date on which the ship was registered with that State;
3. the ship's identification number in accordance with regulation 3;
4. the name of the ship;
5. the port at which the ship is registered;



	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

6. the name of the registered owner(s) and their registered address(es);
7. the registered owner identification number;
8. the name of the registered bareboat charterer(s) and their registered address(es), if applicable;
9. the name of the Company, as defined in regulation IX/1, its registered address and the address(es) from where it carries out the safety-management activities;
10. the Company identification number;
11. the name of all classification society(ies) with which the ship is classed;
12. the name of the Administration or of the Contracting Government or of the recognized organization which has issued the Document of Compliance (or the Interim Document of Compliance), specified in the ISM Code as defined in regulation IX/1, to the Company operating the ship and the name of the body which has carried out the audit on the basis of which the Document was issued, if other than that issuing the Document;
13. the name of the Administration or of the Contracting Government or of the recognized organization that has issued the Safety Management Certificate (or the Interim Safety Management Certificate), specified in the ISM Code as defined in regulation IX/1, to the ship and the name of the body which has carried out the audit on the basis of which the Certificate was issued, if other than that issuing the Certificate;
14. the name of the Administration or of the Contracting Government or of the recognized security organization that has issued the International Ship Security Certificate (or the Interim International Ship Security Certificate), specified in part A of the ISPS Code as defined in regulation XI-2/1, to the ship and the name of the body which has carried out the verification on the basis of which the Certificate was issued, if other than that issuing the Certificate; and
15. the date on which the ship ceased to be registered with that State.

**Note:** Any changes relating to the entries referred to item 4 to 12 shall be recorded in the Continuous Synopsis Record so as to provide updated and current information together with the history of the changes.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

In case of any changes relating to the entries referred to in note, the Administration shall issue, as soon as is practically possible but not later than three months from the date of the change, to the ships entitled to fly its flag either a revised and updated version of the Continuous Synopsis Record or appropriate amendments thereto.

In case of any changes relating to the entries referred to note, the Administration, pending the issue of a revised and updated version of the Continuous Synopsis Record, shall authorize and require either the Company as defined in regulation IX/1 or the master of the ship to amend the Continuous Synopsis Record to reflect the changes. In such cases, after the Continuous Synopsis Record has been amended the Company shall, without delay, inform the Administration accordingly.

The Continuous Synopsis Record shall be in English, French or Spanish language. Additionally, a translation of the Continuous Synopsis Record into the official language or languages of the Administration may be provided.


The Continuous Synopsis Record shall be in the format developed by the Organization and shall be maintained in accordance with guidelines developed by the Organization footnote. Any previous entries in the Continuous Synopsis Record shall not be modified, deleted or, in any way, erased or defaced.

6 Whenever a ship is transferred to the flag of another State or the ship is sold to another owner (or is taken over by another bareboat charterer) or another Company assumes the responsibility for the operation of the ship, the Continuous Synopsis Record shall be left on board.

7 When a ship is to be transferred to the flag of another State, the Company shall notify the Administration of the name of the State under whose flag the ship is to be transferred so as to enable the Administration to forward to that State a copy of the Continuous Synopsis Record covering the period during which the ship was under their jurisdiction.

When a ship is transferred to the flag of another State the Government of which is a Contracting Government, the Contracting Government of the State whose flag the ship was flying hitherto shall transmit to the Administration as soon as possible after the transfer takes place a copy of the relevant Continuous Synopsis Record covering the period during which the ship was under their jurisdiction together with any Continuous Synopsis Records previously issued to the ship by other States.

When a ship is transferred to the flag of another State, the Administration shall append the previous Continuous Synopsis Records to the Continuous Synopsis Record the Administration will issue to the ship so to provide the continuous history record intended by this regulation.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

The Continuous Synopsis Record shall be kept on board the ship and shall be available for inspection at all times.

### ***10.2 Monitoring the Security of the Ship***

The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

- .1 lighting;
- .2 watchkeepers, security guards and deck watches, including patrols; and
- .3 automatic intrusion–detection devices and surveillance equipment.

When used, automatic intrusion–detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.


The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

#### *Security level 1*

At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watchkeepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary. While under way, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulations for the Prevention of Collisions at Sea in force. The following should be considered when establishing the appropriate level and location of lighting:

- .1 the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;
- .2 coverage should include the area on and around the ship;
- .3 coverage should facilitate personnel identification at access points; and
- .4 coverage may be provided through coordinating with the port facility.

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

### *Security level 2*

At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

- .1 increasing the frequency and detail of security patrols;
- .2 increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;
- .3 assigning additional personnel as security look-outs; and
- .4 ensuring co-ordination with water-side boat patrols, and foot or vehicle patrols on the shore-side, when provided.

Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by co-ordinating with the port facility to provide additional shoreside lighting.

### *Security level 3*

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


- .1 switching on of all lighting on, or illuminating the vicinity of, the ship;
- .2 switching on of all on-board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;
- .3 maximising the length of time such surveillance equipment can continue to record;
- .4 preparation for underwater inspection of the hull of the ship; and
- .5 initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

## **10.3 Security audits and inspections**

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

The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

## **10.2. Reporting nonconformities**

	<b>SEAFARERS TRAINING CENTER</b>	<b>M-SSO (I)-17</b>
	<b>SHIP SECURITY OFFICER</b>	<b>REV. 5-2016</b>

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

SSO 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.

## **11. Security Training**

### **11.1. Training requirements**

The company security officer (CSO) and appropriate shore-based Company personnel, and the ship security officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

1. security administration;
2. relevant international conventions, codes and recommendations;
3. relevant Government legislation and regulations;
4. responsibilities and functions of other security organizations;
5. methodology of ship security assessment;
6. methods of ship security surveys and inspections;
7. ship and port operations and conditions;
8. ship and port facility security measures;
9. emergency preparedness and response and contingency planning;
10. instruction techniques for security training and education, including security measures and procedures;
11. handling sensitive security-related information and security-related communications;
12. knowledge of current security threats and patterns;
13. recognition and detection of weapons, dangerous substances and devices;
14. recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
15. techniques used to circumvent security measures;
16. security equipment and systems and their operational limitations;
17. methods of conducting audits, inspection, control and monitoring;
18. methods of physical searches and non-intrusive inspections;
19. security drills and exercises, including drills and exercises with port facilities; and
20. assessment of security drills and exercises.



- ***In addition, the SSO should have adequate knowledge of, and receive training, in some or all of the following, as appropriate:***

1. the layout of the ship;
2. the ship security plan (SSP) and related procedures (including scenario-based training on how to respond);
3. crowd management and control techniques;
4. operations of security equipment and systems; and
5. testing, calibration and whilst at-sea maintenance of security equipment and systems.

- ***Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:***

1. knowledge of current security threats and patterns;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
4. techniques used to circumvent security measures;
5. crowd management and control techniques;
6. security-related communications;
7. knowledge of the emergency procedures and contingency plans;
8. operations of security equipment and systems;
9. testing, calibration and whilst at-sea maintenance of security equipment and systems;
10. inspection, control, and monitoring techniques; and
11. methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

- ***All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:***

1. the meaning and the consequential requirements of the different security levels;
2. knowledge of the emergency procedures and contingency plans;
3. recognition and detection of weapons, dangerous substances and devices;
4. recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and
5. techniques used to circumvent security measures.

- ***The port facility security officer should have knowledge and receive training, in some or all of the following, as appropriate:***

1. security administration;
2. relevant international conventions, codes and recommendations;



3. relevant Government legislation and regulations;
4. responsibilities and functions of other security organizations;
5. methodology of port facility security assessment;
6. methods of ship and port facility security surveys and inspections;
7. ship and port operations and conditions;
8. ship and port facility security measures;
9. emergency preparedness and response and contingency planning;
10. instruction techniques for security training and education, including security measures and procedures;
11. handling sensitive security-related information and security-related communications;
12. knowledge of current security threats and patterns;
13. recognition and detection of weapons, dangerous substances and devices;
14. recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;
15. techniques used to circumvent security measures;
16. security equipment and systems, and their operational limitations;
17. methods of conducting audits, inspection, control and monitoring;
18. methods of physical searches and non-intrusive inspections;
19. security drills and exercises, including drills and exercises with ships; and
20. assessment of security drills and exercises.





- ***Port facility personnel having specific security duties should have knowledge and receive training, in some or all of the following, as appropriate:***

1. knowledge of current security threats and patterns;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
4. techniques used to circumvent security measures;
5. crowd management and control techniques;
6. security-related communications;
7. operations of security equipment and systems;
8. testing, calibration and maintenance of security equipment and systems;
9. inspection, control, and monitoring techniques; and
10. methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

- **All other port facility personnel should have knowledge of and be familiar with relevant provisions of the PFSP**

1. the meaning and the consequential requirements of the different security levels;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and
4. techniques used to circumvent security measures.