Chapter 5 – Maritime Security Levels

5.1 Maritime Security Levels – Overview ................................................................. 5-2
  5.1.2 Application .................................................................................................. 5-2
  5.1.3 Responsibilities ........................................................................................... 5-3
5.2 How security levels are set and communicated in Australia ........................................ 5-5
5.3 Security Directions ............................................................................................ 5-7
5.4 Impact of maritime security levels on ship’s security measures ........................................ 5-8

Chapter 6 – Contingency Planning

6.1 Overview ........................................................................................................... 6-2
6.2 Security risk assessment .................................................................................... 6-4
6.3 Security plans ..................................................................................................... 6-6
6.4 Security Controls ............................................................................................... 6-9
6.5 Piracy contingency planning and security controls ................................................ 6-11

Chapter 7 – Techniques to Circumvent Maritime Security Measures

7.0 Overview ......................................................................................................... 7-2
7.1 Common measures used to circumvent port and vessel security .................................. 7-2
7.2 Techniques to circumvent cargo security measures ............................................... 7-7
7.3 Techniques used to circumvent searches for illegal items ......................................... 7-9
7.4 Corruption of port security/ ship personnel ......................................................... 7-11
Chapter 8 – Recognition of weapons, dangerous substances

8.1 Overview .............................................................................................................................. 8-2
8.2 Weapons used in terrorist attacks ......................................................................................... 8-2
8.3 Weapons of mass destruction ............................................................................................... 8-7
8.4 Weapons used in Piracy ........................................................................................................ 8-9

Chapter 9 – Handling security-related information and comms

9.1 Overview ............................................................................................................................. 9-2
9.2 Responsibilities communicating security-related information .............................................. 9-2
9.3 Security Plans ....................................................................................................................... 9-2
9.4 Handling security-related information .................................................................................. 9-3
9.5 Maritime security information – key sources .......................................................................9-4

Chapter 10 – Security Reporting Procedures

10.1 Introduction ...................................................................................................................... 10-2
10.2 The difference between security incidents and security events ........................................ 10-2
10.3 Persons responsible for reporting maritime security incidents and events ...................... 10-3
10.4 Record keeping on Regulated Australian Ships ................................................................. 10-3
10.5 Reporting of maritime security incidents and events ........................................................ 10-4
10.6 Handy References ............................................................................................................ 10-9
10.7 Event grade examples ...................................................................................................... 10-9

Chapter 11- Maritime Security Training, Drills and Exercises

11.1 Training of key security personnel and other personnel on ships and in ports .................. 11-2
11.2 Drills and Exercises ........................................................................................................ 11-6
1.1 The importance of maritime security

The concept of maritime security has changed significantly over the last 30 years. The world’s oceans and waterways are very difficult to control from a security perspective. This is because vast stretches of international waters are not under the control of any particular nation and waterways that are controlled by different countries are often poorly monitored. As a consequence, our oceans and waterways have proved to be an ideal environment for transnational crimes such as piracy and terrorism.

The shipping industry carries more than 90% of the world’s trade and in Australia that figure rises to 99%. The events of September 11 highlighted the vulnerability of the world’s transport system to attack and triggered international action that resulted in many new codes, laws and procedures being designed to enhance maritime security.

It is important that all participants in the maritime industry understand the basic concepts of maritime security so each individual can contribute to the security of their ship, port facility or offshore facility. Today, the implications of maritime security impact on the daily work environment of most mariners in any area of the maritime industry. For example this can include: transiting through a secure port facility to join a ship; understanding the security requirements when joining a ship; or participating in ship security exercises when onboard a ship. Anyone can come face to face with a security threat at any time and by being able to correctly recognise and respond to the threat they might stop a serious situation from developing.
The IMO recognised the importance of Maritime Security Training by making it a requirement for Maritime Security Awareness Training to be a compulsory element in the Certificate of Safety Training 2014.

1.2 Timeline of events shaping the current maritime security environment - an Australian context

Maritime security issues first appeared on the radar in 1985 following the hijacking of the Italian cruise ship Achille Lauro. The IMO (the United Nations Agency involved with safety of shipping and protection of the marine environment) adopted a resolution to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews. In 1988 the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation was adopted. Piracy has plagued the world’s waters for centuries and was recognised as a significant issue in 2000 when 469 actual and attempted attacks were recorded. In 2000 the USS Cole was attacked introducing a new form of maritime terrorism when a small craft laden with explosives crashed into her hull while she was alongside in port. In 2002 the MV Limburg was attacked in a similar manner which left little doubt that Al –Qaeda had developed the capability to carry out attacks in the maritime domain.

The single biggest event that saw a shift in global thinking towards security was the September 11 attack on America in 2001. This changed global attitudes towards security and led to the development of many new laws, codes and conventions to enhance maritime security by increasing the level of security of a specific location or vessel and by identifying key areas of the maritime industry that were weak and could be exploited by criminals.

Possibly the most significant development in maritime security legislation was the introduction of the International Ship and Port Facility Security (ISPS) code by the International Maritime Organisation (IMO) in 2002. This code included several amendments to the 1974 Safety of Life at Sea (SOLAS) convention. It was the fastest ever convention to be adopted in the IMO. The aim is to provide a standardised, consistent framework for assessing and applying security measures by all countries who have signed the SOLAS convention. The code requires Governments to undertake risk assessments in order to establish the level of security threat in their ports. It also requires that ships and ports appoint dedicated security officers who oversee formal security plans that are approved by their Governments. The ISPS code has had wide-ranging implications for governments, shipping companies and port facilities. Much of this security awareness course will be based on and directly refers to the Code.

In Australia, the Maritime Transport and Offshore Facilities Security Act (MTOFSA or ‘the Act’) was developed as the key piece of legislation to implement the ISPS code. The Act provides a regulatory framework that assists the development and implementation of maritime security plans for ships, ports and offshore facilities. It is the Act which details the security requirements to be employed by Australian registered vessels and not the ISPS code. Having said this, compliance with The Act will naturally imply compliance with the ISPS code.
The Office of Transport Security (OTS) was established as an agency of the Australian Department of Infrastructure and Transport. The purpose of the OTS is to regulate transport security and advise the federal government on transport security matters. Its direct focus is the development of effective security policy and planning. The OTS has no capability to respond to a security incident as this responsibility is given to the Police, customs or relevant response agencies in each state and territory. The head of the OTS is the First Assistant Secretary (the Secretary).

1.3 Maritime security awareness course objectives and overview

This course aims to give you the following proficiencies as identified in IMO table A-V1_61 (2)

- Basic working knowledge of maritime security terms and definitions, including elements that may relate to piracy and armed robbery
- Basic knowledge of international maritime security policy and responsibilities of Governments, companies and persons
- Basic knowledge of maritime security levels and their impact on security measures and procedures aboard ship and in port facilities
- Basic knowledge of security reporting procedures
- Basic knowledge of security-related contingency plans
- Basic knowledge of techniques used to circumvent security measures
- Basic knowledge enabling recognition of potential security threats, including elements that may relate to piracy and armed robbery
- Basic knowledge enabling recognition of weapons, dangerous substances and devices and awareness of the damage they can cause
- Basic knowledge in handling security-related information and security-related communications
- Basic knowledge of training, drill and exercise requirements under relevant conventions, codes and IMO circulars, including those relevant for anti-piracy and anti-armed robbery

It has been structured into 10 chapters after the Introduction that directly reflects the proficiencies listed above.

1.4 Assessment and Certification

Maritime Career Training’s Security Awareness Course is conducted with the approval of the Australian Maritime Safety Authority. We will provide a Statement of Attainment to successful applicants upon completion of the course.

A final written assessment will be conducted. The pass mark will be 70% or higher. Multiple choice questions will make up no more than 40% of the marks. The remainder of the assessment questions will involve short written answers.
Interesting maritime security case studies

1.5 MV Limburg Bombing 2002

**Name:** MV Limburg, 157,000-ton crude oil tanker

**Date:** Oct 6 2002

**Location:** Arabian sea

**Description of attack:** The MV Limburg was carrying around 39,700 barrels of crude oil from Iran to Malaysia on 6 October 2002.

While in the Gulf of Aden to pick up another load, an explosives-laden dinghy rammed the starboard side of the tanker.

The explosives detonated on impact and the vessel caught fire, killing one crew member and injuring 12 others. 90,000 barrels of oil leaked into the Gulf of Aden, the fire was put out and the vessel was towed to Dubai. The damage caused was around $45 Million US.

**Organisation:** Al Qaeda

**Ramifications:** Extensive damage, environmental pollution, 1 dead, 4 injured

**Significance for global maritime security:** The attack is significant because it marks Al-Qaeda's first successful strike against an oil target.
1.6 USS Coal Bombing 2000

**Name:** USS Cole

**Date:** 12 Oct 2000

**Location:** Aden Harbour, Yemen

**Description of attack:** A 35-foot boat laden with the explosives RDX and TNT with two bombers on board rammed the USS Cole port amidships while it was refuelling in Aden harbor, ripping a 32-foot by 36-foot hole in the hull and causing extensive internal damage.

A U.S. Navy investigation found that the ship's officers and crew failed to take a number of security measures that would have possibly prevented the attack. At the time, Yemen was rated at a "high" threat level, the fourth-highest of a five-level threat alert system.

The vessel was moored at a refuelling platform when the attack occurred. The two suicide bombers waved to some of the ship’s crew who were topside, many of whom later said they assumed the approaching craft was a garbage boat. Many of the crew were below decks for lunch.

The damage from the blast took 18 months and $250 million to repair.

**Organisation:** Al Qaeda and Islamic army of Aden

**Ramifications:** 17 dead, 47 injured, significant damage to the vessel, 2 attacker deaths.

**Significance for global maritime security:** First time a suicide boat laden with explosives had caused a maritime terror incident.
1.7 Boarding and Hijacking of the Maersk Alabamba, 2009

**Name:** MV Maersk Alabamba  

**Date:** April 2009  

**Description of attack:** Somali piracy reached such levels that in 2009 the US Maritime Administration recommended ships stay 600 nm out to sea. On 8 April 2009, four Somali pirates boarded the Maersk Alabamba 240nm off the coast when she was enroute to Kenya. At the time the ship was carrying 20 crew and 17,000 metric tons of cargo.

During the boarding, the captain stayed on the bridge with two other crew members while the rest of the crew locked themselves in the engine room. The ship’s engineers were able to sink the pirate speed boat shortly after the boarding by continuously swinging the ship’s rudder. They then took control of the ship from within the engine room and with it the Pirate’s ability to control the ship.

The crew later used brute force to overpower the pirates and free a hostage. The frustrated pirates then decided to depart the ship in a lifeboat taking the Captain, Richard Phillips with them for bargaining power. The USS Bainbridge and USS Halyburton responded to the situation and a 4 day standoff developed that ended in US snipers taking out three of the pirates and capturing the 4th. The captain was recovered in good condition. The Maersk Alabama has been attacked another three times since then. In Nov 2009 she warded off pirates with small arms fire and acoustic weapons. In 2010 the security team onboard repelled a skiff with 5 pirates and in 2011 a skiff of 5 pirates tried to hijack the vessel from astern but was repelled by the ship’s armed security team.

**Organisation:** Somali Pirates  

**Ramifications:** Nil crew injured, hostage released.  

**Significance for global maritime security:** This event brought the issue of Somali piracy to the world press.
1.8 The Hijacking of the Cruise Liner Achille Lauro, 1985

**Name:** MV Achille Lauro

**Date:** October 1985

**Description of the Attack:** The Achille Lauro was an Italian cruise liner that was sailing off Egypt to Port Said in October 1985. She was attacked by four men representing the Palestine Liberation Front (PLF) who were seeking revenge after the Israeli bombings of the PLO headquarters in Tunis. The hijackers demanded the vessel sail to Tartus in Syria and demanded the release of 50 Palestinians who were in Israeli prisons. On arrival at Tartus, the ship was refused permission to dock and the hijackers killed a disabled Jewish-American passenger Leon Klinghoffer and ordered crew to throw his body overboard. The ship headed back towards Port Said and after two days of negotiations the hijackers abandoned the liner in exchange for safe conduct aboard an Egyptian airliner. Then President Ronald Reagan ordered that their plane be intercepted by F-14s and they were escorted to a naval air base in Sicily where the hijackers were arrested.

**Organisation:** Palestine Liberation Front (PLF)

**Ramifications:** 1 passenger killed

**Significance for Global Maritime Security:** This event was recognised as one of the first maritime terrorism events. Afterwards the IMO investigated the concept of maritime terror and in March 1988 released the Convention on the Suppression of Unlawful acts against the Safety of Maritime Navigation.
1.9 Terrorist attack on Super Ferry 14 in 2004

**Name:** Super Ferry 14  
**Date:** February 2004  
**Location:** En route from Manila to Cagayan de Oro City.  
**Organisation:** Abu Sayyaf  
**Description:** 90 minutes into a passenger ferry crossing in the Philippines a bomb exploded, killing 116 passengers. Five months after the incident, Redondo Cain Dellosa admitted to planting the bomb in the boat and six members of Abu Sayyaf were charged with murder. Investigators believed that the ship was targeted by Abu Sayyaf because the company that owned it refused to pay protection money.  

**Ramifications:** 116 killed, numerous injured. Substantial damage to the vessel and loss to the company involved.

**Significance to Global Maritime Security:** This is not only the worst terrorist attack in the Philippines, it is also the most deadly maritime attack at sea.
Chapter 2: Maritime security threats and threat recognition

Threats to Maritime security ................................................................................................................... 2

2.1 Maritime terrorism ............................................................................................................................. 2

2.1.1 Definition ................................................................................................................................... 2

2.1.2 Australia's terrorism threat ....................................................................................................... 2

2.1.3 Weapons used by terrorists ....................................................................................................... 3

2.1.4 Biological/chemical attack ........................................................................................................ 3

2.2 Piracy ............................................................................................................................................. 4

2.2.1 Somali pirates ............................................................................................................................. 6

2.2.2 West African pirates .................................................................................................................. 7

2.2.3 South East Asian Piracy ......................................................................................................... 7

2.2.4 Techniques used in piracy ....................................................................................................... 8

2.2.5 Recent Piracy Examples ......................................................................................................... 8

2.3 Organised Crime ............................................................................................................................ 10

2.3.1 Drug smuggling ....................................................................................................................... 10

2.3.2 Cargo theft ............................................................................................................................... 11

2.4 Other Security Threats .................................................................................................................. 11

2.4.1 Stowaways ................................................................................................................................. 11

2.4.2 Disaffected Individuals: .......................................................................................................... 12

2.4.3 Violent or Disruptive Protest ................................................................................................. 13

2.5 Identification of potential security threats .................................................................................... 14
Threats to Maritime security

2.1 Maritime terrorism
Terrorism has become a major concern since the September 11 attacks and has presented enormous security challenges for companies and Governments around the globe. While terrorists may target a small group of victims, the real intended audience is often much wider. For example, the terrorist attacks on twin towers sent a message to America and the rest of the world.

The attacks of 9/11 and the Bali bombings underline the general and increased threat of terrorism we now face. The attacks on the USS Cole and MV Limburg over the past five years highlight the possibilities and dangers that maritime terrorism present.

The international maritime community has become increasingly concerned about the possibility of terrorists:

- placing a terrorist device inside cargo bound for a particular destination
- using a vessel to import cargo necessary for the terrorist group to function or
- illegally smuggling members of a terrorist operation

2.1.1 Definition

Terrorism can be defined as:

the use of violence and threats to intimidate or coerce, especially for political purposes

Terrorism:

- involves the use of or violence against people or property to intimidate, coerce or to demand ransom
- is conducted by organised groups
- is politically motivated and is aimed at raising political awareness or achieving political goals
- often use threats to create public fear.

2.1.2 Australia’s terrorism threat

A terrorist attack on Australia’s maritime industry is definitely possible. Terrorists have stated a desire to create maximum economic impact and Australia relies heavily on shipping and seaborne trade. Australia is also adjacent to a region where terrorist groups have known maritime capabilities.
The Australian Government lists the following as major terrorist threats to the maritime industry:

- a direct attack on a port facility (especially a container, oil, gas or chemical terminal)
- a direct attack on a ship, particularly a high-risk vessel, such as one carrying high-consequence dangerous goods, a passenger ferry, a cruise liner, or a US Navy vessel in an Australian port
- an attack on a ship, to hijack it and use it as a weapon against something else
- the use of a ship, its cargo or a sea container for terrorist purposes to transport terrorists or terrorist material, including a possible weapon of mass destruction.

The impacts of maritime terrorism are severe and extend beyond the loss of human life. The following are real impacts of the terrorist attack on the MV Limburg:

- 1 crew member dead and 4 injured
- 90,000 barrels of oil lost
- Approximately $45 million US worth of damage
- Insurance premiums tripled for vessels transiting through ports in Yemen
- Some shipping lines cut Yemen from their destination which caused a substantial loss of business to the local ports and economy
- Over 3000 Yemeni port workers lost their jobs due to the decline in shipping.

2.1.3 Weapons used by terrorists

Chapter 8 describes weapons used by terrorists in detail including weapons of mass destruction and explosives.

2.1.4 Biological/chemical attack

Biological attacks are used by terrorists to cause wide-spread fear and economic disruption. Terrorists may taint cargo with a biological or chemical agent or poison for the purpose of causing harm to whoever handles the product and ultimately causes widespread panic. Previous cases where this has occurred has cost companies millions and changed the way food products today are packaged and shipped. If such an attack occurred in today’s environment, it could shut down the entire cargo supply chain including a port and shipping line and place many lives at risk. Chapter 8 describes this type of attack in more detail and provides examples of previous attacks such as the anthrax attacks in America and the Sarin gas attack used on a Japanese subway.
2.2 Piracy

Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS) defines piracy as:

(1) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or passengers of a private ship or private aircraft, and directed:

- On the high seas, against another ship or persons or property on board such ship.
- Against a ship, persons or property in a place outside the jurisdiction of any State.

(2) 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, and

(3) Any act of inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b).

Piracy has plagued the world’s waters for centuries but has become an increasing threat to global maritime security since 1994. In the last 10 years, the international maritime community has seen a progressive escalation in daring and violent pirate attacks that have resulted in an increasing number of crew killed. The weapons used by pirates have evolved from knives, machetes and pistols to military automatic rifles and RPGs (rocket propelled grenades).

The graph “yearly statistics of incidents which occurred since 1984” has been compiled by the IMO and shows that the numbers of pirate attacks world-wide have increased from under 100 in 1994 to approximately 540 in 2011.
The graph below shows the changing trends in piracy hotspots since 2003. Indonesia and waters through south East Asia, such as the Malacca Strait have traditionally had high levels of pirate attacks. These numbers have reduced in recent years, most likely due to efforts by the international maritime community to deter piracy attacks such as increased surveillance and security assistance by military in the region.

The African region is a different story and the number of attacks off the coast of Somalia and the Gulf of Aden has dramatically increased since 2007.

This image below has been provided by the IMB’s piracy reporting centre and shows the number and location of attempted and actual piracy attacks for the first half of 2012.
A detailed estimate provided by the Oceans Beyond Piracy Initiative has estimated the impact of piracy on the global economy to be close to $7 billion in 2011.

There are four danger areas that are highly susceptible to attack by pirates:

- Gulf of Aden, near Somalia and the southern entrance to the Red Sea
- the Gulf of Guinea, near Nigeria and the Niger River delta
- the Malacca Strait between Indonesia and Malaysia and
- off the Indian subcontinent, particularly between India and Sri Lanka (although this is not shown by attacks this year in the image above).

2.2.1 Somali pirates

The area around Somalia provides the greatest piracy threat to shipping. In 1991 commercial fishing fleets began to exploit Somalia’s coastline following the collapse of the Somali dictator, Major General Mohamed Siad Barre. Local fishermen responded by fighting for what they deemed to be their own resources and began boarding illegal trawlers armed with knives and pistols. They would charge the illegal operators a fine around $1000 US. It didn’t take long for fishermen to realise that holding up the illegal fisherman provided more income than catching the fish and by the mid 2000, many part time fisherman had turned to full-time piracy.

The tactics of Somali pirates focus on hijackings and kidnapping and in 2011 the average ransom payments to Somali pirates was above $5million. Piracy has become the second biggest generator of wealth in Somalia bringing in over $200M a year.
The international community has taken the following steps to counter Somali Piracy:

- **2008**: UN Security Council passed resolution 1851. This move allowed authorised countries with navies deployed in the Gulf of Aden to take action against pirates and armed robbers within Somali waters.
- **Resolution 1951** paved way for the Contact Group on Piracy of the Coast of Somalia to be created in 2009. Amongst other things, this group has addressed military co-ordination, shipping, self-awareness and public information related to piracy.
- In January 2009, 9 east African countries signed the Djibouti Code of Conduct to implement aspects of the 2008 UN resolutions.

### 2.2.3 West African pirates

The motivation behind Piracy off West Africa is largely social and political. Pirate tactics in the Gulf of Guinea include hijacking oil tankers and selling the oil back on the black market. Evidence has been found that Nigeria’s rebel movement has been involved in oil tanker attacks. This group has pressured the Nigerian government for more equitable allocation of oil revenues. The IMB has noted that Nigerian piracy has expanded into neighboring waters during 2011.

### 2.2.4 South East Asian Piracy

While Southeast Asian piracy has decreased over the last 10 years, it still remains an issue. The governments of Malaysia, Singapore, Thailand and Indonesia have been active in combating the threat with Malaysia deploying two warships in the Malacca strait in 2011 and a joint operation between Malaysia, Singapore and Thailand involving air patrols above the strait. 30% of the world’s trade must pass through the Malacca Strait along with half of the world’s oil shipments.
2.2.5 Techniques used in piracy

Piracy attacks usually involve:

- Boarding a ship from one or more high-speed small boats
- Using a rope with a grappling hook or a light weight ladder (for hooking onto the ship’s side-rail)
- Climbing up the anchor chain of vessels at anchor (if the hawse cover is not secure)
- Use of weapons as a means of intimidation, to force the vessel to stop or to escape once detected.

Chapter 6 on contingency planning looks at methods to plan for and counter a pirate attack.

2.2.6 Recent Piracy Examples

The examples below have been taken from the IMB Piracy Reporting website and describe pirate attacks in May 2012.

<table>
<thead>
<tr>
<th>Attack Number</th>
<th>Narration</th>
</tr>
</thead>
<tbody>
<tr>
<td>148-12</td>
<td>23.05.2012: 1300 UTC: Posn: 12:45N – 043:18E, Bab El Mandeb Straits, Red Sea. Pirates in three skiffs approached a bulk carrier underway. Master raised alarm, informed UKMTO and alerted the armed security team onboard. Weapons sighted on the skiffs when they closed to 300 metres from the ship. The armed security team fired warning shots resulting in the pirates aborting the attempted attack and moving away.</td>
</tr>
<tr>
<td>147-12</td>
<td>23.05.2012: 0900 UTC: Posn: 25:29.6N – 057:16.8E Around 28nm WSW of Bandar-e-Jask, Iran, (Off Somalia). D/O onboard a general cargo ship underway noticed a group of 10 skiffs at a distance of 2nm from the ship on the stbd side. The forward skiff broke off from the group and approached the ship at a speed of 20-25 knots. Master and security team informed. Alarm raised, fire hoses and SSAS activated. UKMTO and navies informed. The ship increased speed and commenced manoeuvring away from the skiffs. As the skiffs closed to 500meters the armed security team fired warning shots. The skiffs ignored the warning shots and continued to approach aggressively and weapons were sighted on the skiffs. As the skiffs closed to 300meters the security team once again fired at the skiffs and it was noticed that the skiffs returned fire towards the ship. Eleven additional skiffs were sighted on the port side advancing towards the ship. As the security team fired warning shots these skiffs stopped and moved away. The skiffs on the stbd side continued to chase the ship and then after around 12 minutes from the initial approach the skiffs moved away towards a large dhow in the vicinity. No damages and no injuries to crew.</td>
</tr>
<tr>
<td>146-12</td>
<td>12.05.2012: 2100 LT: Posn: 01:14.58N – 104:08.43E, Around 4nm NNE of Pulau Batam, Indonesia. A barge under tow enroute from Singapore to Kelanis, Banjarmasin, Indonesia was boarded by robbers using a wooden tug. VTIS Singapore informed the Master that a tug was following his barge. Upon investigation Master saw a wooden tug moving away from the barge. The crew boarded the barge and found 13 containers opened. Incident reported to MPA Singapore.</td>
</tr>
</tbody>
</table>
| 145-12        | 18.05.2012: 2000 LT: Posn: 25:20.9N – 057:34.6E (Around 25nm South of Ra’s-e Jask, Iran), Off Somalia. Three skiffs chased a crude tanker underway and approached close to the stern. Alarm sounded, authorities and nearby warship contacted. Later the skiffs aborted the
<table>
<thead>
<tr>
<th>Attack Number:</th>
<th>Narration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>boarding and moved away.</td>
</tr>
<tr>
<td>144-12</td>
<td>18.05.2012: 2240 LT: Posn: 03:42.7S – 114:26.8E, Taboneo Anchorage, Banjarmasim, Indonesia. Duty A/B on roving deck patrol noticed five robbers in the forward store. Two of the robbers threatened him with a knife and the A/B escaped and informed D/O who raised alarm and alerted all crew. By the time the crew members went forward the robbers had escaped with stolen ship’s stores.</td>
</tr>
<tr>
<td>143-12</td>
<td>17.05.2012: 0740 UTC: Posn: 09:58.2N – 083:00.1W, Puerto Limon Anchorage, Costa Rica. Five robbers in a boat were noticed by alert deck watchmen alongside their container ship with boat hooks in an attempt to board. Duty officer raised alarm and reported to port authorities. Seeing the alert crew the robbers aborted the attempt and moved away.</td>
</tr>
<tr>
<td>142-12</td>
<td>15.05.2012: 0100 UTC: Suez anchorage, Egypt. Robbers boarded an anchored tanker, broke into the forecastle store, stole ship’s stores and escaped unnoticed. Upon investigation it was learnt that the robbery took place between the deck security rounds carried out by the crew.</td>
</tr>
</tbody>
</table>
2.3 Organised Crime

Organised crime can be defined as:

*Individuals engaging in unlawful activities to gain advantage or benefit for themselves such as theft, sabotage or other unlawful behaviour.*

The Australian minister for Home Affairs has stated organised crime costs the Australian economy over $15 billion per year. Organised crime can include:

- Drug and weapons smuggling
- Cargo theft
- People smuggling

2.3.1 Drug smuggling

Smuggling is a criminal activity and may result in large financial loss to the ship owner whose ship is being used by the smugglers. Often drugs are the commodity being smuggled and they may be brought onboard in a number of creative ways such as in luggage, stores, in a person’s body or in electronic equipment. Weapons are another commodity commonly smuggled.

Chapter 7 – Techniques used to circumvent security, outlines the different ways smugglers can get their illegal cargo onboard and also discusses how crime organisations can target and corrupt key players in the maritime industry to gain intelligence and access. A recent Government report (the Polaris Report) has highlighted the security threat posed to Australian ports from organised crime syndicates working with insiders from the shipping industry. Australia is attractive to smugglers for the following reasons:

- The high Australian dollar leads to increased smuggler profits
- There is a developing market in Australia for drugs and other contraband
- Australia currently has a strong economy so it is likely more people can afford a higher price for contraband.

Between mid 2010 and mid 2012, the Polaris task force had made 16 arrests, laid 77 charges and seized over 12 tonnes of illegal drugs.
2.3.2 Cargo theft

Cargo theft has been going on for centuries and continues to impact on the maritime industry. It causes significant financial losses. Although violence or political issues are not involved in most cases of cargo theft, it still remains a significant security threat. Cargo theft usually involves several individuals and can be categorised as organised crime. Crime syndicates usually target personnel on the “inside” to assist in intelligence gathering or provide access to the cargo. Corruption is dealt with further in Chapter 7 – methods used to circumvent security measures.

Common techniques used to seal cargo include:

- Opening containers stacked at a terminal or transfer facility, stealing the goods and then transporting them by car or truck
- A corrupt port driver claiming his vehicle has been hijacked and the contents stolen when he was involved with the crime, helped the criminals to steal the goods and received a cut of the profits
- Dismantling containers, removing merchandise, resealing containers
- Getaway vehicle speeding through fences and security checkpoints
- Stealing loaded trucks from storage yards

2.4 Other Security Threats

2.4.1 Stowaways

A stowaway can be defined as

*a concealed person on a vessel, or in cargo loaded on to a vessel, without the consent of the ship’s owner, master, or any other responsible person.*

The issue of stowaways ranges from a single person boarding a freighter to organised stowaway operations. Most stowaways are looking for economic opportunities and a better life for them and their families.
Methods of stowaway access include:

- Via the gangway, posing as a stevedore or contractor (with fake uniform or id)
- Via a pilot ladder that has not been fully retracted
- Climbing mooring lines and the anchor chain (especially at night)

Hiding places aboard a vessel include:

- In ventilation shafts and spaces found within cargo bays
- Inside coiled mooring lines and other equipment such as unsecured storage lockers
- Inside unsecured empty containers
- Inside lifeboats
- Inside the engine room
- In unsecured crew accommodation
- Inside linen lockers and food preparation areas.

2.4.5 Disaffected Individuals:

This is defined as:

In appropriate behaviour by disgruntled individuals (including staff) causing losses, disruptions or damage (includes sabotage).

It is possible for a staff member or insider who holds a grudge against the company or ship to cause considerable damage. For example:

- Confidential information can be accessed, altered, destroyed, stolen or leaked
- Component parts and machinery can be sabotaged, causing damage
- Food can be contaminated

Simple acts can potentially cost a company millions of dollars in lost business, damaged machinery and liability. Two examples of this include:

- When HP Foods were forced to remove cans of baked beans from super market shelves after they were discovered to have slivers of glass in them. The subsequent investigation revealed that the glass had been deliberately added by either an employee or a visitor to the factory.
- A Boeing Co. 737-400 twin-engine jet-liner in the final stages of production was discovered to have "highly irregular" wire cuts buried inside a thick bundle of wires feeding a power system. Boeing suspected the wires may have been cut by an employee.
2.4.6 Violent or Disruptive Protest

This is defined as:

*Low-level acts of violence by issue motivated groups or any activity that disrupts maritime operations.*

Issue motivated groups such as Greenpeace have been at odds with some elements of the maritime industry for years and have used maritime assets to stage demonstrations to gain public awareness of their campaigns. While these protests are largely peaceful, they can highlight weak security measures on ships and ports as protesters illegally gain access to property and assets to stage their demonstrations. Common techniques include:

- Boarding ships illegally and hanging protest signs and banners
- Political graffiti messages on vessels or other physical assets
- Illegally boarding vessels to stage a protest

Some groups employ more extreme measures of protest and the term “eco terrorism” has been used, causing sabotage and physical damage to assets.

An example of a peaceful demonstration occurred in New Zealand in February 2012 when police were called to the Shell Oil Drilling ship, the Noble Discoverer, which was alongside in a New Plymouth port. Seven Greenpeace activists had boarded the vessel including well known Xena Princess Warrior actor, Lucy Lawless. They proceeded to hang banners from the vessel “Stop Shell” and “Save the Arctic”. The vessel was due to leave for Alaska to drill five exploratory oil wells and because of the Greenpeace boarding, all work onboard had to stop.
2.5 Identification of potential security threats

The US coast guard and the US Department of Homeland Security suggest the activities below are indications of possible criminal or terrorist surveillance. Everyone has the ability to notice and report suspicious or strange behaviour.

Things to look out for:

- An unknown person approaching employees or their family members inquiring about the facility
- Unknown or suspicious workmen trying to gain access to the facility to repair, replace, service or install equipment
- Drop off of a suspicious package
- Unknown person photographing facilities
- Theft of standard documents detailing standard operating procedures of the port or ship,
- Theft of ID cards, vehicle passes, employee uniforms or facility/ ships vehicles,
- Prolonged interest by a suspicious person in:
  - port/ ship security measures,
  - personnel,
  - entry points or access controls
- Unusual behaviour by unknown persons such as being startled or quickly looking away from personnel or vehicles entering or leaving designated facilities
- Unauthorised persons observing security reaction drills or procedures
- Increase in anonymous telephone or email threats to facilities in conjunction with suspected surveillance incidents , indicating possible surveillance of threat reaction procedures
- Unknown persons conducting foot surveillance (two or three working together)
- Unknown persons conducting mobile surveillance, using bikes, scooters, motorcycles, cars, trucks, utes or boats
  - Suspicious general aviation aircraft operating in proximity to facilities
    - Prolonged static surveillance using operatives disguised as demonstrators, shoe shiners, flower vendors, news agents not previously seen in the area
    - Unknown persons noted to make discreet use of still cameras, video recorders, or not taking at non-tourist locations
- Use of multiple sets of clothing, identification or the use of sketching materials.
CHAPTER 3: Maritime security terms and definitions

3.1 Introduction to maritime security terms and definitions ....................................................... 3

3.2 Terms and definitions relating to legislation and Maritime Security Agencies .................. 3

3.2.1 Terms and definitions relating to legislation ................................................................... 3
   3.2.1.1 International Ship and Port Facilities Security (ISPS) code: ....................................................... 3
   3.2.1.2 Maritime Transport and Offshore Facilities Security Act and Regulations 2003 ........................ 3

3.2.2 Terms and definitions relating to agencies active in maritime security............................ 3
   3.2.2.1 Department of Infrastructure and Transport: ......................................................................... 3
   3.2.2.2 Office of Transport Security (OTS): .......................................................................................... 3
   3.2.2.3 Australian Maritime Safety Authority (AMSA): ........................................................................ 4
   3.2.2.4 International Maritime Organisation (IMO) ............................................................................. 4
   3.2.2.5 International Maritime Bureau Piracy Reporting Centre (IMB PRC) ........................................... 4

3.3 Terms relating to the ISPS code and the Maritime Transport Offshore Facilities Security Act. 5

3.3.1 Terms, definitions and acronyms relating to Security Personnel e................................... 5
   3.3.1.1 Ships Security Officer (SSO) ........................................................................................... 5
   3.3.1.2 Company Security Officer (CSO): .................................................................................... 5
   3.3.1.3 Port Facilities Security Officer (PFSO): ............................................................................ 5
   3.3.1.4 Port Service Provider Security Officer (PSPSO): .............................................................. 5
   3.3.1.5 Maritime Industry Participant (MIP): ............................................................................. 5

3.3.2 Terms relating to ports and ships ................................................................................... 5
   3.3.2.1 Security Regulated Ports: ........................................................................................................ 5
   3.3.2.2 Security Regulated Ships: ........................................................................................................ 5
   3.3.2.3 Regulated Australian Ship: ...................................................................................................... 6
   3.3.2.4 Regulated Foreign Ship: .......................................................................................................... 6

3.3.3 Terms relating to assessments, plans, audits and certification ........................................ 6
   3.3.3.1 Ship Security Assessment (SSA): .............................................................................................. 6
   3.3.3.2 Ship's Security Plan (SSP): ..................................................................................................... 6
3.3.3.3 Port Facility Security Assessment (PFSA): ................................................................. 6
3.3.3.4 Maritime Security Plan (MSP): ..................................................................................... 6
3.3.3.5 Declaration of Security: ............................................................................................... 7
3.3.3.6 Continuous Synopsis Record: ..................................................................................... 7
3.3.3.7 International Ship Security Certificate (ISSC): .......................................................... 7

3.3.4 Terms and definitions relating to security levels ............................................................ 7
3.3.5 Terms and definitions relating to maritime security zones ............................................. 7

3.6 Abbreviations used in this course ....................................................................................... 9
3.1 Introduction to maritime security terms and definitions

There are many terms, definitions and acronyms used in maritime security to the point where it is almost like learning another language. This chapter is devoted to listing these and briefly explaining some of the key terms and concepts in the world of maritime security. This chapter will also provide a handy reference throughout the course.

3.2 Terms and definitions relating to legislation and Maritime Security Agencies

3.2.1 Terms and definitions relating to legislation

3.2.1.1 International Ship and Port Facilities Security (ISPS) code: is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Having come into force in 2004, it prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to "detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade."

3.2.1.2 Maritime Transport and Offshore Facilities Security Act and Regulations 2003 (MTOFSA). This act and regulations were developed by the Australian government to implement the ISPS code in Australia. The act came into effect at the same time as the ISPS code in July 2004. It aims to safeguard maritime transport and offshore facilities against unlawful interference. The act and regulations establish a regulatory framework which centers on maritime industry participants developing security plans.

3.2.2 Terms and definitions relating to agencies active in maritime security

3.2.2.1 Department of Infrastructure and Transport: The federal Department whose role it is to provide policy advice to the Minister for Infrastructure and Transport and deliver a variety of programs on behalf of the Australian Government. The Department conducts research and analysis; provides safety information and advice; and performs regulatory functions. They have a strong policy development role, together with program administration and service delivery responsibilities. The department is not responsible for responding to a maritime security incident.

3.2.2.2 Office of Transport Security (OTS): An Agency of the Department of Infrastructure whose purpose is to regulate transport security and advise the federal government on transport security matters. The OTS implements audit, compliance and security measures; handles transport security operations and intelligence and ensures that transport security regulation, planning and policy follow government guidelines. As it is part of the Department, it has no capability to respond to any security incident.
3.2.2.3 **Australian Maritime Safety Authority (AMSA):** is responsible for maritime safety, including search and rescue. While the OTS is responsible for transport security, both maritime safety and security are linked. The Maritime Standards division within AMSA is responsible for representing Australia through the International Maritime Organization (IMO) in the development, implementation and enforcement of international standards that govern many areas, one of which is Maritime Security.

3.2.2.4 **International Maritime Organisation (IMO):** is the United Nations specialised agency with responsibility for the safety and security of shipping and the prevention of marine pollution by ships. It has promoted the adoption of some 50 conventions and protocols and adopted more than 1,000 codes and recommendations concerning maritime safety and security, the prevention of pollution and related matters. The IMO’s Maritime Security Working group developed the ISPS code which was developed in 2001 and came into effect in 2004.

3.2.2.5 **International Maritime Bureau Piracy Reporting Centre (IMB PRC):**

The IMB is a non-profit making organisation, established in 1981 to act as a focal point in the fight against all types of maritime crime and malpractice. It is a specialised division of the International Chamber Of Commerce (ICC) and has established a 24 hour IMB Piracy Reporting Centre (PRC) in Kuala Lumpur, Malaysia in response to the rapidly growing number of piracy-related incidents. The main objective of the PRC is to be the first point of contact for the shipmaster to report any incident of piracy, armed robbery or even stowaways - thus initiating the process of response. The main aim of the PRC is to raise awareness within the shipping industry.
3.3 Terms relating to the ISPS code and the Maritime Transport Offshore Facilities Security Act

3.3.1 Terms, definitions and acronyms relating to Security Personnel as defined by the ISPS code

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

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

3.3.1.3 Port Facilities Security Officer (PFSO): 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.

3.3.1.4 Port Service Provider Security Officer (PSPSO): A Security Officer who represents a Port Service Provider (PSP). A PSP is a service provider that supports the maritime industry by providing services from the water, for example tugs, lighters, bunker barges.

3.3.1.5 Maritime Industry Participant (MIP): The MTOFS Act defines MIPs as:

- port operators or
- port facility operators or
- the ship operator for a regulated Australian ship or
- the ship operator for a regulated foreign ship or
- a person (other than a maritime security inspector or a duly authorised officer) appointed by the Secretary under the Act to perform a maritime transport security function or
- a contractor who provides services or a person who conducts a maritime-related enterprise

3.3.2 Terms relating to ports and ships

3.3.2.1 Security Regulated Ports: Areas of a port that are intended for use either wholly or partially in connection with the movement, loading, unloading, maintenance or provisioning of security regulated ships, comprise a security regulated port.

3.3.2.2 Security Regulated Ships: A security regulated ship is either:

- a regulated Australian ship or
- a regulated foreign ship.
Certain government-controlled ships (both Australian and foreign) such as Navy and customs vessels are not required to comply with the act specifications for security regulated ships.

### 3.3.2.3 Regulated Australian Ship:
A regulated Australian ship is an Australian ship that is:

- a passenger ship that is used for overseas or inter-State voyages or
- a cargo ship of 500 gross tonnage or more that is used for overseas or inter-State voyages or
- a mobile offshore drilling unit that is on an overseas or inter-State voyage (other than a unit that is attached to the seabed)
- a ship of a kind prescribed in the regulations.

### 3.3.2.4 Regulated Foreign Ship:
A regulated foreign ship:

- is a foreign ship and
- is one of the following:
  - a passenger ship
  - a cargo ship of 500 gross tonnage or more
  - a mobile offshore drilling unit (other than a unit that is attached to the seabed)
  - a ship of a kind prescribed in the regulations and
- is in Australian waters and
- is in, or is intending to proceed to a port in Australia.

### 3.3.3 Terms relating to assessments, plans, audits and certification

#### 3.3.3.1 Ship Security Assessment (SSA):
A risk based analysis of security-related hazards or threats for each ship the Company operates. The SSA will address the particulars of the ship, its cargoes and crew and the locations where it will operate. It should consider the likelihood of various security-related scenarios and possible responses to those scenarios.

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

#### 3.3.3.3 Port Facility Security Assessment (PFSA):
A risk based analysis of security-related hazards or threats for the port facility. The PFSA will address the particulars of the port facility and ships, persons, cargo, cargo transport units and ship’s stores within the port facility. It should consider the likelihood of various security-related scenarios and possible responses to those scenarios.

#### 3.3.3.4 Maritime Security Plan (MSP):
MSP in Australia, also known as Port Facilities Security Plan (PFSP) in the ISPS code. A document based on the PFSA developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship’s stores within the port facility from the risks of a security incident. The maritime industry participants who must have a maritime security plan in force are:
• operators of security regulated ports
• operators of facilities at security regulated ports
• providers of services at such ports

3.3.3.5 Declaration of Security: The Declaration of Security (DOS) is a document between a ship and a port facility or another ship it is interfacing with and provides a means for ensuring that critical security concerns are properly addressed and security will remain in place throughout a vessel’s stay at the facility. A DOS will address security requirements that could be shared between a port facility and a ship or between ships and state the responsibility of each stakeholder.

3.3.3.6 Continuous Synopsis Record: The CSR provides an on-board record of the history of the ship. Any changes shall be recorded in the CSR so as to provide updated and current information together with the history of the changes.

3.3.3.7 International Ship Security Certificate (ISSC): The ISSC is issued by the ship’s flag state and its purpose is to certify that the ship complies with the regulations of Part A of the ISPS code. It is the responsibility of the shipping company to obtain the certificate and the ship to carry it.

3.3.4 Terms and definitions relating to security levels

3.3.4.1 Maritime Security Levels 1, 2 and 3: The International Maritime Organization’s (IMO) International Ship and Port Facility Security (ISPS) Code provides for three security levels. These provide an internationally harmonised approach to maritime security levels. In Australia, the Department determines the appropriate security level, taking into account the prevailing threat environment.

The three maritime security levels set out in the ISPS Code are:

- **Security level 1**: The default level at which ships, port and offshore facilities normally operate
- **Security level 2**: The level applying for as long as there is a heightened risk of a security incident
- **Security level 3**: The level applying when there is probable or imminent risk of a security incident, even though it may not be possible to identify the specific target

3.3.5 Terms and definitions relating to maritime security zones

Maritime security zones are established to provide additional security measures in particular areas within security regulated ports, ships (in port or at sea) or offshore facilities. Reasons may include:

- controlling people’s movements
- providing cleared areas
• preventing interference with ships and offshore facilities, and restricting access to critical installations and areas

The types of security zones that may be employed are:

• Port security zones
• Offshore security zones
• Ship Security Zones
• Onboard Security zones.
3.6 Abbreviations used in this course

AIS: Automatic Identification System
AMSA: Australian Maritime Safety Authority
CSO: Company Security Officer
CSR: Continuous Synopsis Record
EEZ: Exclusive Economic Zone
IMB PRC: International Maritime Bureau Piracy Reporting Centre
IMO: International Maritime Organisation
ISPS: International Ship and Port Facilities Security (ISPS) code
ISSC: International Ship Security Certificate
MIP: Maritime Industry Participant
MSP: Maritime Security Plan
MSCHOA: The Maritime Security Centre – Horn of Africa
MSIC: Maritime Security Identification Card
MTOFSA: Maritime Transport and Offshore Facilities Security Act
PFSA: Port Facility Security Assessment
PFSP: Port Facilities Security Plan
PSPSO: Port Service Provider Security Officer
OTS: Office of Transport Security
RCC: Rescue Coordination Centre
SSA: Ship Security Assessment
SSAS: Ship Security Alert System
SSO: Ship Security Officer
SSP: Ship Security Plan
The Secretary: Head of the office of Transport Security (Department of Transport and Infrastructure)
The Act: The Maritime Transport and Offshore Facilities Security Act
UKMTO: The United Kingdom Marine Trade Operations
Chapter 4: International and National Maritime Security Policy and Responsibilities

4.1 International and National Maritime Security Policy Overview .......................................................... 2
4.2 ISPS Code ........................................................................................................................................... 3
   4.2.1 Overview .................................................................................................................................... 3
   4.2.2 ISPS Code Objectives and Functional Requirements ............................................................... 3
   4.2.3 ISPS Code Application ............................................................................................................... 4
   4.2.4 ISPS Code Contents ................................................................................................................... 4
   4.2.5 ISPS Code Key Concepts .......................................................................................................... 5
   4.2.6 ISPS Code Responsibilities ....................................................................................................... 13
   4.3.1 Overview .................................................................................................................................... 15
   4.3.2 Purpose and Maritime Security Outcomes ............................................................................... 15
   4.3.3 Contents ................................................................................................................................... 15
   4.3.4 Act Application ............................................................................................................................ 16
   4.3.5 Act Key Concepts ......................................................................................................................... 18
   4.3.6 Act Key Concepts – Security Plans ............................................................................................. 20
   4.3.7 Act Key Concepts - Maritime security zones ............................................................................. 21
   4.3.8 Act Key Concepts - Maritime Security Identification Card (MISC) ........................................ 23
   4.3.9 MTOSF Security Personnel ......................................................................................................... 24
4.1 International and National Maritime Security Policy Overview

The IMO was established in 1948 and today has 170 member states and the slogan “Safe, secure and efficient shipping on clean oceans”. Maritime security only became a significant issue in the 1980s when a growing number of incidents such as kidnappings, hijacking and deliberate grounding caused the IMO assembly to respond. The IMO adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation in 1988 and the purpose was to ensure appropriate action was taken against persons committing acts such as the seizure of ships by force, acts of violence against persons onboard ships and the placing of devices onboard a ship which are likely to destroy or damage them. The convention gave contracting governments the obligation to either extradite or prosecute alleged offenders.

The attacks of September 11 have had massive ramifications to security across the globe and changed the way security operations are managed world-wide. In 2002 the IMO adopted the International Ship and Port Facility Security Code into the Convention for the Safety of Life at Sea (SOLAS). It isn’t surprising that this became the fastest ever convention to be adopted by the IMO and to allow for these changes, SOLAS chapter XI was amended to become chapters X1-1 and XI-2. The ISPS code contains a comprehensive set of measures to enhance the security of ships and port facilities and has serious implications for contracting governments and MIPs (companies, ports, ships and individuals).

The ISPS code was brought into effect in 2004 and in 2003 Australia passed the Maritime Transport and Offshore Facilities Security Act (MTOFSA) to implement the ISPS code in Australia. The Act is implemented through the MTOFSA regulations (2003) and the government agency responsible is the Office of Transport Security (part of the Department of Infrastructure and Transport).

In this chapter we will investigate the ISPS code, examining its purpose and contents, key concepts and the responsibilities of governments, companies and persons before looking at how it is implemented in Australia through the MTOFA act and regulations.
4.2 ISPS Code

4.2.1 Overview

The International Ship and Port Facility Security Code (ISPS Code) contains a set of security measures that certain individuals, ships and port facilities of contracting governments must adhere to. The code has two parts, Part A is mandatory and Part B recommendatory and as mentioned in the introduction, the ISPS code has been included in the SOLAS Convention to which Australia is a party.

The Code considers that ensuring the security of ships and port facilities is a risk management activity and that risk assessment is an important tool to determine what security measures are appropriate in each case. The Code provides a standardised framework for evaluating risk. As the threats to maritime security change, Governments can increase or decrease security measures in place for ships and port facilities. This is done by determining the appropriate security levels and corresponding security measures.

4.2.2 ISPS Code Objectives and Functional Requirements

The objectives of the ISPS code are:

- Establish an international framework for co-operation between governments and the shipping and port industries to detect/assess security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade
- Identify the roles and responsibilities of all parties in this co-operation
- Provide a network for the collection and exchange of security related information
- Provide a system for assessing security plans of MIPs
- Identify procedures that will be followed when security levels are changed
- Provide confidence that, at an international level, adequate security measures are in place in the commercial maritime network

In order to achieve its objectives, this Code embodies a number of functional requirements. These include, but are not limited to:

- gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments
- requiring the maintenance of communication protocols for ships and port facilities
- preventing the introduction of unauthorised weapons, devices or explosives to ships or port facilities
- providing means for raising the alarm in reaction to security threats or security incidents
- requiring ship and port facility security plans based upon security assessments and
- requiring training, drills and exercises to ensure familiarity with security plans and procedures
4.2.3 ISPS Code Application

The ISPS code applies to:

1. the following types of ships engaged on international voyages:
   - passenger ships, including high-speed passenger craft
   - cargo ships, including high-speed craft, of 500 gross tonnage and upwards
   - mobile offshore drilling units
2. port facilities serving such ships engaged on international voyages

The code states that Contracting Governments such as Australia will decide how far the code applies to ports that occasionally service ships departing or arriving on international voyages. This decision shall be based on a security assessment carried out in accordance with the Code.

The code does not apply to warships, naval auxiliaries or other ships owned or operated by a contracting government and used on government non-commercial service.

4.2.4 ISPS Code Contents

The code is divided into two parts. Part A sets out the mandatory requirements and the table of contents is laid out below:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 2: Interim international ship security certificate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Part B provides guidance regarding the provisions of chapter XI-2 and part A of the Code. It is laid out using the same structure as part A and provides guidance and interpretation of the mandatory requirements. Part B is non-compulsory.
4.2.5 ISPS Code Key Concepts

This section deals with key concepts contained within the ISPS code. For record keeping and reporting procedures refer to Chapter 10 and for training, drills and exercises, Chapter 11.

4.2.5.1 Declaration of Security

The Declaration of Security (DOS) is a document between a ship and a port facility or another ship it is interacting with and provides a means to ensure that critical security concerns are properly addressed and that security will remain in place throughout a vessel’s stay at the facility. A DOS will address security requirements that could be shared between a port facility and a ship or between two ships. They state the responsibility of each stakeholder.

Contracting governments shall determine when a DOS 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 a DOS when:

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

4.2.5.2 Ship Security Plan

Ship security plans identify the security measures to be implemented by ships when different maritime security levels are in force. A ship is required to act upon the security levels set by Contracting Governments. Chapter 5 explains maritime security levels.

Every security registered ship is required to have an approved Ship Security Plan which will detail security measures for each of the three security levels as defined in Part A of the ISPS Code. Ship security plans are discussed in more detail in Chapter 6.

4.2.5.3 Ship Security Assessment

A ship security assessment is essential prior to developing or updating a ship security plan. The CSO shall ensure the ship security assessment is carried out by an appropriately skilled individual/company to evaluate the security of the ship. The ship security assessment shall be documented, reviewed, accepted and retained by the Company. Chapter 6 provides more information on security assessment.
4.2.5.4 Company security officer

A Company Security Officer is a person designated by the company who is responsible for the security of one or more ships. The company must clearly define which ships this person is responsible for and may designate several persons to operate as company security officers depending on the number and types of vessels operated by the company.

A CSO’s responsibilities include but are not limited to:

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

4.2.5.5 Ships Security Officer

The Ships Security Officer is the person on board the ship accountable to the master, designated by the Company as responsible for the security of the ship. The SSO’s duties include implementation and maintenance of the ship security plan and liaison with the company security officer and port facility security officers.

Specific responsibilities of the SSO as stated in the ISPS code are:

- 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
• ensuring that security equipment is properly operated, tested, calibrated and maintained

4.2.5.7 Port facility security assessment

The port facility security assessment is an essential and integral part of the process of developing and updating the port facility security plan. The port facility security assessment shall be carried out by the Contracting Government who may authorise a recognised security organisation to carry out the port facility security assessment. Chapter 6 provides more detail on security risk assessment.

A port facility security assessment should include the following elements:

• identification and evaluation of important assets and infrastructure it is important to protect
• identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures
• identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability and
• identification of weaknesses, including human factors in the infrastructure, policies and procedures

The Contracting Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment and design of these port facilities are similar.

4.2.5.8 Port facility security plan

A port facility security plan shall be developed and maintained for each port facility, adequate for the ship/port interface. The plan will be based on the port facility’s security assessment and make provisions for the three security levels as discussed further in Chapter 5.

The port facility security plan will be approved by the Contracting Government where the port is located and will be developed in accordance with the guidance given in part B of this Code. The plan will be written in the working language of the port facility and protected from unauthorised disclosure.
4.2.5.9 **Port facility security Officer**

A PFSO is 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. A PFSO must be designated for each port facility and a person can be PFSO for more than one facility.

The duties and responsibilities of the port facility security officer shall include:

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

The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by the ISPS Code.

4.2.5.10 **International Ships Security Certificate**

An International Ships Security Certificate (ISSC) is a requirement under regulation 4 of Chapter XI-2 of SOLAS and Section 19 of Part A of the ISPS Code. It is issued by the ship’s flag state and its purpose is to certify that the ship complies with the regulations of Part A of the ISPS code. It is the responsibility of the shipping company to obtain the certificate and the ship to carry it.

On receiving the SSA and SSP, and after verifying SSAS equipment and appointment of key security personnel, familiar with their roles, the flag state can issue an interim ISSC which is valid for a period of 6 months.
A full ISSC is issued after the flag state has verified that the ship’s security system, any associated security equipment and the approved SSP meet the requirements of the regulations of Part A of the ISPS code.

The ISSC is valid for a period that cannot exceed five years, when it must be renewed. There must also be an ‘intermediate verification’ of the certificate which is conducted between the second and third year of issue. Once the ISSC has been issued, any changes made in security systems, associated security systems and the SSP must be sanctioned by the flag state.

An example of an ISSC is found below:

SOLAS/CONF.5/34
ANNEX I
Page 26

APPENDIX TO PART A

APPENDIX I

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) (State)

Certificate Number

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the Government of ________________________________ (name of State)

by ________________________________ (persons or organization authorized)

Name of ship

Distinctive number or letters

Port of registry

Type of ship

Gross tonnage

IMO Number

Name and address of the Company

THIS IS TO CERTIFY:

1. that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2. that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3. that the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based ______________________

This Certificate is valid until ________________________________ subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at ________________________________ (place of issue of the Certificate)

Date of issue ________________________________ (signature of the duly authorized official Issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)
4.2.5.11 Automatic Identification System (AIS)

The Automatic Identification System (AIS) is an automatic tracking system used on ships and by vessel traffic services. It identifies and locates vessels by electronically exchanging data with other nearby ships and AIS Base stations. AIS information supplements marine radar, which continues to be the primary method of collision avoidance for water transport.

In 2000, the IMO revised SOLAS Regulation 19 of Chapter 5 and adopted a new requirement for all ships to carry AIS capable of providing information about the ship to other ships and to coastal authorities automatically. This came into effect on 31 December 2004.

The regulation requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size.

A ship fitted with AIS is required to maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.

The regulation requires that AIS shall:

- provide information - including the ship’s identity, type, position, course, speed, navigational status and other safety related information - automatically to appropriately equipped shore stations, other ships and aircraft
- receive automatically such information from similarly fitted ships; monitor and track ships
- exchange data with shore-based facilities

![AIS Diagram](image-url)
AIS is useful for monitoring the situation over any particular sea area by the security authorities. Having said this, concern over the misuse of AIS information by pirates or terrorists in certain sea areas caused the IMO to adopt resolution A 956(23) which allows a ships master to switch off the AIS in specific areas where pirate or terrorist attack is imminent.

4.2.5.12 Ship Security Alert System (SSAS)

The Ship Security Alert System is part of the ISPS code and is a system that contributes to the IMO’s efforts to strengthen maritime security and suppress acts of terrorism and piracy against shipping. In case of attempted piracy or terrorism, the ship’s SSAS beacon can be activated. The beacon transmits a specific country code. Rescue Coordination Centres (RCCs) or SAR Points of Contact of that particular region are notified discreetly. National authorities that receive the signal can dispatch appropriate military or law-enforcement forces.

The system is a joint project between Cospas-Sarsat and the IMO and a SSAS beacon operates with similar principles to the aircraft transponder emergency code 7700.

The ship security alert system requires two activation points, one of which should be on the bridge. These will typically be fixed or portable telephone handsets, fixed or portable keypads or fixed or portable buttons. Measures should be incorporated in the activation points to avoid their inadvertent operation and the generation of false alerts.
When the SSAS is activated, recipients of the alert should be given the following information:

- Name of ship;
- IMO Ship identification number;
- Call Sign;
- Maritime Mobile Service Identity;
- GNSS position (latitude and longitude) of the ship; and
- Date and time of the GNSS position.

4.2.5.13 Continuous Synopsis Record

The CSR provides an on-board record of the history of the ship. Any change to the ship’s information is recorded in the CSR to provide updated and current information together with the history of the changes.

The requirement for CSRs on ships comes from amendments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS). The following vessels used for overseas or inter-State voyages must have a CSR:

- A passenger ship, carrying more than 12 passengers, including high speed craft or
- A cargo ship of more than 500 gross tonnes, including high speed craft or
- A mobile offshore drilling unit.

The CSR shall contain the following information:

- the name of the State whose flag the ship is entitled to fly
- the date on which the ship was registered with that State
- the ship’s identification number in accordance with regulation 3
- the name of the ship
- the port at which the ship is registered
- the name of the registered owner(s) and their registered address(es)
- the name of the registered bareboat charterer(s) and their registered address(es), if applicable
- 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
- the name of all classification society(ies) with which the ship is classed
- the name of the Administration or of the Contracting Government or of the recognised organisation which has issued:
  - the document of compliance
  - Safety management Certificate
  - International Ships Security Certificate
4.2.6 ISPS Code Responsibilities

The requirements of Contracting Governments, Companies and the Master are described below. The responsibilities of individuals such as the SSO, CSO and PFSO are described in the above section on Key elements of the ISPS Code (sections 4.2.5.4, 4.2.5.5 and 4.2.5.9).

4.2.6.1 Contracting Governments

Contracting Governments have various responsibilities, including:

- setting the applicable security level
- approving the Ship Security Plan and relevant amendments to a previously approved plan,
- verifying the compliance of ships with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code and issuing the International Ship Security Certificate,
- determining which port facilities located within their territory are required to designate a Port Facility Security Officer
- ensuring completion and approval of the Port Facility Security Assessment and the Port Facility Security Plan and any subsequent amendments
- and exercising control and compliance measures.

Contracting governments are also responsible for communicating information to the International Maritime Organization and to the shipping and port industries.

Contracting Governments can designate or establish designated authorities within Government to undertake their security duties. Recognised security organisations can carry out certain work but the final decision on the acceptance and approval of this work should be given by the Contracting Government or the Designated Authority.

4.2.6.2 Companies

Companies have several responsibilities under the ISPS code. These include the designation of a CSO for the company and a SSO for each of its ships. CSOs are required to ensure the SSA is properly carried out and that SSPs are prepared in accordance with Part A of the ISPS code and submitted for approval by or on behalf of the administration and placed on the ship.

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 in accordance with chapter XI-2 and this Part of the Code.
4.2.6.3 Master

The master has ultimate responsibility for the safety and security of the ship. SSPs are required to contain a clear statement emphasising the master’s authority and responsibility to make decisions with respect to the safety and security of the ship.

The ISPS Code states that even at the highest security level when a threat is imminent, a Master may seek clarification or amendment of instructions issued by those responding to a security incident or threat. He can do this if there are reasons to believe that compliance with any instruction may impact on the safety of the ship.

SOLAS regulation XI-2/8 provides clear guidance on the 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 the denial of access to persons (except those duly authorised by a contracting government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

4.3.1 Overview

When it comes to implementing the ISPS Code in Australia, the MTOFS Act is the key piece of legislation. It is the MTOFS Act and not the ISPS code that set the security measures for Australian registered vessels; however the inference is that compliance with the MTOFS Act is direct compliance with the code. The full title is “An Act to safeguard against unlawful interference with maritime transport and offshore facilities and for related purposes”.

The MTOFS Act is implemented through the Maritime Transport and Offshore Facilities Security Regulations (2003).

4.3.2 Purpose and Maritime Security Outcomes

The purpose of the MTOFS Act 2003 is to safeguard against unlawful interference with maritime transport or offshore facilities. To achieve this purpose, the Act establishes a regulatory framework centred on the development of security plans for ships, other maritime transport operations and offshore facilities. The implementation of a security plan should make an appropriate contribution to the achievement of the maritime security outcomes.

The maritime security outcomes are as follows:

- Australia’s obligations under Chapter XI-2 of the SOLAS Convention and the ISPS Code, including those with regard to the rights, freedoms and welfare of seafarers, are met
- the vulnerability to terrorist attack of Australian ships, ports and other ships within Australia, and offshore facilities is reduced without undue disruption to trade
- the risk that maritime transport or offshore facilities are used to facilitate terrorist or other unlawful activities is reduced
- security information is communicated effectively among maritime industry participants and government agencies with security responsibilities for maritime transport and offshore facilities

It is not the purpose of the Act to prevent lawful advocacy, protest, dissent or industrial action that does not compromise maritime security.

4.3.3 Contents

The act is divided into 13 parts.

The simplified overview contained within the act describes these parts as follows.
Part 2: provides for maritime security levels. The security measures to be implemented when different maritime security levels are in force are set out in maritime security plans, ship security plans and offshore security plans. Part 2 also provides for the Secretary to give security directions in special circumstances.

Part 3: deals with maritime security plans. Maritime industry participants who are required to have plans must comply with their plans.

Part 4: deals with ship security plans and ISSCs (International Ship Security Certificates) for regulated Australian ships. These ships must have both a ship security plan and an ISSC. They must be operated in compliance with their ship security plans and must continue to meet ISSC standards.

Part 5: puts obligations on regulated foreign ships. The Secretary can give control directions to regulated foreign ships to ensure that security standards are maintained.

Part 5A deals with offshore security plans. Offshore industry participants who are required to have plans must comply with their plans.

Part 5B deals with ISSCs for Australian ships regulated as offshore facilities.

Part 5C deals with foreign ships regulated as offshore facilities. The Secretary can give control directions to foreign ships regulated as offshore facilities to ensure that security standards are maintained.

Part 6: provides for the establishment of maritime security zones. Additional security requirements apply in these zones which can be established within ports, on and around ships and on and around offshore facilities.

Part 7: deals with screening, weapons and prohibited items.

Part 8: sets out the powers of officials under this Act. These officials are maritime security inspectors, security assessment inspectors, duly authorised officers, law enforcement officers, maritime security guards and screening officers.

Part 9: sets out reporting obligations in relation to certain maritime transport or offshore facility security incidents.

Part 10: allows the Secretary to require security compliance information from maritime industry participants.

Part 11: provides a range of enforcement mechanisms. These are infringement notices, enforcement orders, ship enforcement orders, injunctions and a demerit points system.

Part 12: provides for review of certain decisions by the Administrative Appeals Tribunal.

Part 13: deals with miscellaneous matters.

4.3.4 Act Application

4.3.4.1 Security regulated ports

Areas of a port that are intended for use either wholly or partially in connection with the movement, loading, unloading, maintenance or provisioning of security regulated ships, comprise a security regulated port.
4.3.4.2 Security regulated Ships

A security regulated ship is either:

- a regulated Australian ship or
- a regulated foreign ship

Certain government-controlled ships (both Australian and foreign) such as Navy and customs vessels are not required to comply with the act specifications for security regulated ships.

4.3.4.3 Regulated Australian Ship

A regulated Australian ship is an Australian ship that is:

- a passenger ship that is used for overseas or inter State voyages or
- a cargo ship of 500 gross tonnage or more that is used for overseas or inter State voyages or
- a mobile offshore drilling unit that is on an overseas or inter State voyage (other than a unit that is attached to the seabed) or
- a ship of a kind prescribed in the regulations

This does not include:

- an Australian ship regulated as an offshore facility
- a ship of a kind prescribed by the regulations such as a passenger ship (whether or not also a cargo ship) used for overseas or inter-State voyages if it is a pleasure craft that is not engaged in trade

4.3.4.4 Australian Ship regulated as an offshore facility

An Australian ship regulated as an offshore facility means a FPSO (floating production storage and offloading unit) or FSU (floating storage unit) that is:

- an Australian ship and
- either a security regulated offshore facility or part of a security regulated offshore facility

A FPSO or FSU is both a ship and an offshore facility. As it is an offshore facility, the Secretary may declare it to be a security regulated offshore facility. If this happens, the ship ceases to be a security regulated ship.

4.3.4.5 Regulated foreign Ship

A regulated foreign ship:

- is a foreign ship and
- is one of the following:
  - a passenger ship
  - a cargo ship of 500 gross tonnage or more
  - a mobile offshore drilling unit (other than a unit that is attached to the seabed)
4.3.4.6 Foreign Ship regulated as an offshore facility

A foreign ship regulated as an offshore facility means a FPSO (floating production storage and offloading unit) or FSU (floating storage unit) that is:

- a foreign ship and
- either a security regulated offshore facility or part of a security regulated offshore facility

A FPSO or FSU is both a ship and an offshore facility. As it is an offshore facility, the Secretary may declare it to be a security regulated offshore facility. If this happens, the ship ceases to be a security regulated ship.

4.3.5 Act Key Concepts

4.3.5.1 The Meaning of Unlawful Interference with Maritime Transport or offshore Facilities

Unlawful interference does not include lawful advocacy, protest, dissent or industrial action. The acts listed below are classed as unlawful interference with maritime transport or offshore facilities if they are done without lawful authority.

- committing an act, or causing any interference or damage, that puts the safe operation of a port, or the safety of any person or property at the port, at risk
- committing an act, or causing any interference or damage, that puts the safe operation of an offshore facility, or the safety of any person or property at the offshore facility, at risk
- taking control of a ship or offshore facility by force, or threat of force, or any other form of intimidation
- destroying a ship that is being used for maritime transport;
- destroying an offshore facility
- causing damage to a ship that is being used for maritime transport that puts the safety of the ship, or any person or property on board or off the ship, at risk
- doing anything on board a ship that is being used for maritime transport that puts the safety of the ship, or any person or property on board or off the ship, at risk
• placing, or causing to be placed, on board a ship that is being used for maritime transport anything that puts the safety of the ship, or any person or property on board or off the ship, at risk
• putting the safety of ships at risk by interfering with, damaging or destroying navigational aids, communication systems or security systems
• putting the safety of ships at risk by communicating false information

4.3.5.2 Security Directions

Security directions are issued by the Department to maritime industry participants instructing them to implement additional security measures above those approved in the security plan. This usually occurs if there is reason to believe that unlawful interference with maritime transport or offshore facilities is probable or imminent. The Department must give security directions in writing. They can be given to:

• a maritime industry participant or an employee of a maritime industry participant
• passengers
• people within the boundaries of a security regulated port and
• people within the boundaries of a security regulated offshore facility

Anyone receiving a security direction must comply with its requirements, while all other measures of the existing security level must also remain in place.

If compliance with a security direction means a person will commit an offence or contravene the Act, the person is taken not to have committed the offence or contravened the Act.

4.3.5.3 Control Directions

If a regulated foreign ship is not compliant with the Act or the ISPS Code or does not implement a higher security level when directed, it may be given a control direction to ensure security standards are maintained. Control directions may include:

• removing the ship from Australian waters
• removing the ship from a security regulated port
• moving the ship within a security regulated port
• removing the ship from an offshore security zone
• removing the ship from the vicinity of the offshore facility
• holding position for a specified period or until a specified event occurs
• taking particular actions on board the ship and
• allowing a maritime security inspector to inspect the ship or its security records

If a regulated foreign ship does not adhere to a control direction the ship’s operator or master may be subject to an injunction issued by the Federal Court.

If compliance with a control direction means a person will commit an offence or contravene the Act, the person is taken not to have committed the offence or contravened the Act.
4.3.6 Act Key Concepts – Security Plans

4.3.6.1 Maritime Security Plans

Maritime security plans set out the security measures and procedures to be implemented at each maritime security level to safeguard against acts of unlawful interference with maritime transport or offshore facilities.

MIPs who must have and comply with a maritime security plan are:

- operators of security regulated ports
- operators of facilities at security regulated ports and
- providers of services at such ports.

Maritime Security plans are referred to as Port Facility Security Plans or Port Service Provider Security plans under the ISPS code. More detail is provided in Chapter 6.

4.3.6.2 Ship Security Plans

Regulated Australian ships are required to have and comply with ship security plans. Various other ships and people are also required to comply with ship security plans and must not hinder or obstruct compliance with another ship’s security plan.

Ship security plans identify the security measures that ships must implement when different maritime security levels are in force. More detail on SSPs is provided in Chapter 6.

All regulated Australian ships are required to have a ship security plan and an International Ship Security Certificate (ISSC). It is an offence for an operator of a regulated Australian ship not to have a ship security plan in force, unless the operator has a reasonable excuse.

4.3.6.3 Offshore Security Plans

Offshore security plans set out security measures and procedures to be implemented at the different maritime security levels to safeguard against unlawful interference with an offshore facility. More detail is provided in Chapter 6.
4.3.7 Act Key Concepts - Maritime security zones

Maritime security zones are established to provide additional security measures in particular areas within security regulated ports, ships (in port or at sea) or offshore facilities. Reasons may include:

- controlling people’s movements
- providing cleared areas
- preventing interference with ships and offshore facilities and
- restricting access to critical installations and areas

The types of security zones that may be employed are:

- Port security zones
- Offshore security zones
- Ship Security Zones
- Onboard Security zones

Only personnel who have a valid Maritime Security Identification Card (MISC) have access to security zones. The MISC scheme is explained further in section 4.3.8.

4.3.7.1 Port Security Zones

The Department can establish one or more port security zones within a security regulated port. Ports, port facility operators or port service providers set out the required details of the port security zone in their security plan. The Department then decides whether to establish the zones.

Port security zones can include:

- Land side restricted zones
- cleared zones and
- water-side restricted zones

The Regulations prescribe that all port security zones must have security barriers which can range from a fence or building to trees, booms or marker buoys, as long as they clearly define the boundary and deter unauthorised access. Barriers for land-side restricted and cleared zones also need to have measures to detect and deny unauthorised access.

The MTOFS Regulations outline the duties of maritime industry participants responsible for the port security zones and offences for unauthorised entry.
4.3.7.2 Ship Security Zones

The Department can declare ship security zones around ships within a port or near an offshore facility, subject to certain requirements. This is to protect ships within these zones from unlawful interference with maritime transport. The Regulations include an ‘exclusion zone’ as a type of ship security zone. The purpose of a SSZ is as follows:

- limiting contact with security regulated ships
- controlling the movement of ships and other things in the vicinity of a security regulated ship
- providing cleared areas around security regulated ships
- preventing interference with security regulated ships
- preventing interference with people or goods that have been, or are to be, transported by security regulated ships

Where a port or port facility is expecting a ship considered to be a higher security risk, the port operator may ask the Department to declare a ship security zone for that ship.

The Regulations require clearly identifiable boundaries for ship security zones. This can be done by water-based means (such as buoys, picket boats and booms), land-side signs, or by posting, publishing or broadcasting notices. Port operators may use any means that inform nearby people about the zone and its boundaries.

The Regulations outline the duties of the port operator responsible for the ship security zone. Unauthorised entry into a ship security zone is an offence.

4.3.7.3 On-Board Security Zones

The Department can establish one or more onboard security zones on a regulated Australian ship to create additional security measures within the zones. Ship operators who want the Department to establish onboard security zones set out the required details in their security plans. The Department considers this when deciding whether to establish the zones. The Regulations include an ‘onboard restricted area’ as a type of onboard security zone.

The reasons for establishing an onboard security zone may include:

- controlling access to areas or parts of regulated Australian ships
- maintaining the security of areas or parts of regulated Australian ships
- providing cleared areas on regulated Australian ships
- preventing interference with the operation of regulated Australian ships
- preventing interference with people or goods that are being, have been, or are to be, transported by regulated Australian ships

The Regulations require clearly identifiable boundaries around onboard security zones. Zones must be permanently and sufficiently marked with signs to inform people that access is restricted and that unauthorised access is an offence under the Regulations.

The Regulations outline the duties of ship operators responsible for the onboard security zones and offences for unauthorised entry. Operators of ships with onboard security zones must monitor and
control access to the zones. They must also ensure that the security measures and procedures used to control access to the zone can detect and deter unauthorised access. It is an offence for a person to enter or remain in, or take goods or other things into, an onboard security zone unless they are authorised to do so by the ship operator.

4.3.7.4 Offshore Security Zones

The Department can establish one or more security zones in and around a security regulated offshore facility to create additional security measures within the zones. The Regulations prescribe ‘offshore facility zone’ and ‘offshore water side zone’ as types of offshore security zones. Reasons for establishing an offshore security zone include:

- limiting contact with security regulated offshore facilities
- controlling the movement of people within a security regulated offshore facility
- controlling the movement of ships and other things within and around a security regulated offshore facility
- providing cleared areas within and around security regulated offshore facilities
- preventing interference with security regulated offshore facilities
- preventing interference with people or goods (including petroleum) that have been, or are to be, transported to or from security regulated offshore facilities

4.3.8 Act Key Concepts - Maritime Security Identification Card (MISC)

A MSIC is a nationally recognised security identification card. It shows that the card holder is background checked and cleared to enter and work in the secure areas (or maritime security zones) of our ports, ships and offshore oil and gas facilities.

MSICs reduce the risk that someone planning to unlawfully interfere with maritime infrastructure will gain access to facilities. Anyone working unescorted within secure areas of a port, ship or offshore oil and gas facility must display an MSIC. If not they can be fined.

Having an MSIC does not allow automatic entry to security zones. Access to particular secure areas remains a matter for each maritime industry participant to decide.

People who may be affected by the MSIC scheme are:

- port, port facility and port service workers
- all waterfront workers
- offshore industry participants
- seafarers on Australian regulated ships
- maritime industry participants or employees of a maritime industry participant such as:
• contract workers and labour hire firms
• agents (including freight forwarders and cargo agents)
• security contractors
• maintenance staff
• people working on or providing services to ships and offshore oil and gas facilities, including catering and maintenance companies
• supply ships and maritime rescue services
• helicopter and amphibious pilots transporting personnel to ships and offshore facilities and
• transport operators such as train and truck drivers

Anyone working unescorted in a maritime security zone needs an MSIC. Those working on a wharf, ship or offshore oil and gas facility need an MSIC to work unescorted in maritime security zones.

People who visit an Australian regulated port, ship or offshore facility more than once a year to deliver or drop off goods, provide services or conduct maintenance may also need an MSIC.

4.3.9 MTOSF Security Personnel

4.3.9.1 Maritime security inspectors

Maritime security inspectors are able to conduct ISSC inspections. They can also inspect ships, offshore facilities and the premises and operations of maritime industry participants, to ensure compliance with the Act.

Employees within the Department and law enforcement officers can be appointed as maritime security inspectors. Other persons who meet criteria prescribed in the regulations may also be appointed as maritime security inspectors.

4.3.9.2 Security assessment inspectors

Security assessment inspectors can conduct security assessments of areas, facilities, buildings (other than residences), vessels and vehicles under the control of maritime industry participants.

4.3.9.3 Duly authorised officers

The powers of duly authorised officers extend only to inspecting the operational areas of a security regulated ship or security regulated offshore facility.

The following may be appointed as duly authorised officers:

• customs officers
• members of the Australian Defence Force
• immigration officers
• AMSA surveyors
• quarantine officers
4.3.9.4 Law enforcement officers

Under the Act, police and certain customs officers have special authority to:

- stop and search people, vehicles and vessels in maritime security zones and to stop and search people on security regulated ships and on ships regulated as offshore facilities
- remove people from ships or maritime security zones if they do not leave when requested to do so
- remove vehicles and vessels from maritime security zones if an officer is unable to have the vehicles or vessels removed by persons in control of them

The Act establishes restrictions on this authority, such as requiring an officer to explain why a search is to be made and limiting the amount of force that may be used.

A person who does not leave when requested to do so by a law enforcement officer commits an offence, as does a person who hinders or obstructs an officer exercising powers under this Division.

4.3.9.4 Maritime security guards

Under the Act, maritime security guards have limited powers to:

- request people to produce identification and state reasons for being in maritime security zones and
- restrain and detain people and
- remove unauthorised people from maritime security zones if they do not leave when requested to do so and
- remove unauthorised vehicles and vessels from maritime security zones if a guard is unable to have the vehicles or vessels removed by persons in control of them

The Act establishes restrictions on these powers, such as limiting the amount of force that may be used. The power to detain a person is also restricted to the period before the person can be dealt with by a law enforcement officer.
Chapter 5: Maritime Security Levels

5.1 Maritime Security Levels – Overview

5.1.1 Security level 1

5.1.2 Security level 2

5.1.3 Security level 3

5.1.2 Application

5.1.3 Responsibilities

5.1.3.1 Contracting Governments

5.1.3.2 Ships

5.1.3.3 Port facilities

5.1.3.4 Masters

5.1.3.5 CSO, SSO, PFSO

5.2 How security levels are set and communicated in Australia

5.2.1 Notifying Maritime Security Levels for a Security Regulated Port

5.2.2 Notifying Maritime Security Levels for a Security Regulated Ship

5.2.3 Notifying Maritime security levels for a Security Regulated Offshore Facility

5.2.4 Notifying Maritime security levels for a specific MIP or area within a Security Regulated Port

5.2.5 Revoking a notification

5.2.6 When ports and ships have different levels in force

5.3 Security Directions

5.4 Impact of maritime security levels on ship’s security measures

5.4.1 Access to the ship

5.4.2 Restricted areas on the ship

5.4.3 Handling of cargo

5.4.4 Delivery of ship’s stores

5.4.5 Handling unaccompanied baggage

5.4.6 Monitoring the Security of the Ship
5.1 Maritime Security Levels – Overview

As part of the ISPS code, the IMO have introduced three security levels that are recognised globally and provide a standardised approach to maritime security. These three levels impact security measures in ports and on ships. The default security level is level 1 and once a higher level is declared, all maritime industry participants must comply with the requirements identified in their appropriate security plan. These security plans (e.g. ships security plan, maritime security plan) outline what steps are to be taken at each level. In Australia, the MTOFS Act provides clear direction on how security levels are to be set and communicated. Security levels are set by the Department of Infrastructure and Transport and the Department may also provide additional security directions in certain circumstances.

5.1.1 Security Level definitions

Security levels 1, 2 and 3 are defined as:

5.1.1.1 Security level 1 The default level at which ships, port and offshore facilities normally operate. Security level 1 means the minimum level protective security measures must be applied.

5.1.1.2 Security level 2 The level where there is a heightened risk of a security incident. On upgrading to security level 2, appropriate additional protective security measures are put in force for a period of time due to the heightened security risk.

5.1.1.3 Security level 3 The level where there is probable or imminent risk of a security incident, even though it may not be possible to identify the specific target. On upgrading to security level 3, additional protective security measures are put in force that are appropriate for an imminent or probable security threat. This is the highest security level and should apply only when there is credible information about a probable or imminent threat.

While it is likely security levels will change from 1 to 2 and 3, it is possible for these levels to escalate directly from 1 to 3.

5.1.2 Application

Unless the Department advises otherwise maritime security level 1 applies at all times to each:

- security regulated port
- regulated Australian ship
• regulated foreign ship
• security regulated offshore facility
• area within a security regulated port
• maritime industry participant

The Secretary may declare that maritime security level 2 or maritime security level 3 is in force for one or more of the following as specified in the declaration:

• a security regulated port
• a regulated Australian ship
• a security regulated offshore facility
• an area within a security regulated port
• a maritime industry participant
• operations conducted by a maritime industry participant within, or in connection with, a security regulated port or a security regulated offshore facility
• a regulated foreign ship

5.1.3 Responsibilities

5.1.3.1 Contracting Governments

It is the responsibility of contracting governments to set security levels and provide guidance for protection from security incidents. Factors that should be considered when setting the appropriate security level include:

• the degree that the threat information is credible
• the degree that the threat information is corroborated
• the degree that the threat information is specific or imminent
• the potential consequences of such a security incident

Contracting Governments are required to issue all appropriate instructions when they set security level 3. This includes providing all security-related information to the ships and port facilities affected.

5.1.3.2 Ships

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 need to be carried out on all ships to identify and take preventive measures against security incidents:

• ensuring the performance of all ship security duties
• controlling access to the ship
• controlling the embarkation of persons and their effects
• monitoring restricted areas to ensure that only authorised persons have access
• monitoring of deck areas and areas surrounding the ship
• supervising the handling of cargo and ship’s stores and
• ensuring that security communication is readily available
At security levels 2 and 3, the additional protective measures specified in the ship security plan shall be implemented for each activity detailed above.

Whenever security level 2 or 3 is set, the ship needs to acknowledge receipt of the instructions on the change of the security level. When entering a port where the contracting government has set security level 2 or 3, the ship needs to confirm with the port facility security officer that they have implemented the appropriate measures identified in the SSP.

5.1.3.3 Port facilities

A port facility is required to act on the security levels set by the contracting Government. Security measures and procedures shall be applied at the port facility to cause a minimum of interference with, or delay to passengers, ship’s personnel and visitors, goods and services.

At security level 1, the following activities need to be carried out in all port facilities, to identify and take preventive measures against security incidents:

- ensuring the performance of all port facility security duties
- controlling access to the port facility
- monitoring of the port facility, including anchoring and berthing area(s)
- monitoring restricted areas to ensure that only authorised persons have access
- supervising the handling of cargo
- supervising the handling of ship’s stores and
- ensuring that security communication is readily available

At security level 2 and 3 the additional protective measures specified in the port facility security plan shall be implemented for each above activity.

5.1.3.4 Masters

At all times the Master of a ship has ultimate responsibility for the safety and security of the ship. Even when at security level 3 a Master may seek clarification or alteration of instructions issued by those responding to a security incident or threat if there are reasons to believe that compliance with any instruction may negatively impact the safety of the ship.

5.1.3.5 CSO, SSO, PFSO

The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liaise at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intending to visit in order to establish the security level in force for that ship at the port facility.

Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility’s security level and should provide the ship with any relevant security information.
5.2 How security levels are set and communicated in Australia

In Australia, the Department of Transport and Infrastructure (the Department) sets the security levels taking into consideration the latest information relating to the current threat environment. To upgrade the security level from level 1 (the default level) the Department must make a declaration either orally (telephone or radio), in writing or by electronic transmission (email or fax) and all maritime industry participants notified must upgrade their security measures as required.

A declaration may apply to one or more of the following:

- a security regulated port
- a regulated Australian ship
- a regulated foreign ship
- a security regulated offshore facility
- an area within a security regulated port
- a maritime industry participant.

When a security regulated port receives a declaration to upgrade the security level, the new level will apply to all port operations within the boundaries of the port. Within the boundaries of the port, the security level will be in force for:

- every area
- every security regulated ship
- every ship regulated as an offshore facility
- every security regulated offshore facility
- any operations conducted by a maritime industry participant.

For a security regulated offshore facility a declaration applies to all security regulated ships and operations in the vicinity of the facility.

Once a declaration has been made the stated security level remains in force until it is revoked by the Secretary or the timeframe specified in the declaration expires. A declaration does not need to specify an expiry date. A declaration for a regulated Australian ship may limit the waters for which the security level is in force and in this case the designated security level only applies while the ship is in those waters.

5.2.1 Notifying Maritime Security Levels for a Security Regulated Port

If the Secretary declares that a maritime security level is in force for a security regulated port, the secretary must notify:

- the Port operator
• each MIP who is required to have a maritime security plan and who either controls an area or operates within the boundaries of the port
• each offshore industry participant who is required to have an offshore security plan who operates within the port boundaries

Once the port operator is notified, they have an obligation under the Act to notify:

• Every MIP who is covered by their plan and either controls an area or operates within the boundaries of the port
• The master of every security regulated ship that is within port boundaries or about to enter the port

5.2.2 Notifying Maritime Security Levels for a Security Regulated Ship
If the secretary declares a maritime security level is in force for either a regulated Australian Ship or a regulated foreign ship, they must notify the ship’s operator or the ship’s master as soon as practicable of the change. This includes if a security level changes for a regulated Australian ship while it is in specified waters.

5.2.3 Notifying Maritime security levels for a Security Regulated Offshore Facility
If the Secretary declares that a maritime security level is in force for a security offshore facility, the secretary must notify:

• the offshore facility operator
• each offshore industry participant who is required to have an offshore security plan and who either controls an area or operates within the boundaries of the offshore facility

Once the offshore facility operator is notified, they have an obligation under the Act to notify:

• Every offshore industry participant who is covered by their plan and operates within the boundaries of the offshore facility
• The ship operator or master of every security regulated ship in the vicinity of the facility that is engaged in any facility related activity
• The master of the ship if the facility or part of the facility is a ship regulated as an offshore facility.

5.2.4 Notifying Maritime security levels for a specific MIP or area within a Security Regulated Port
The Secretary is able to declare a maritime security level for a maritime industry participant or for a specific area within port boundaries.
5.2.5 Revoking a notification
If a maritime security level notification has been issued to MIPs by the Secretary, the Secretary then
has the obligation to notify the same MIPs that the security level has been revoked. The same applies
for port or offshore facility operators that have notified MIPs identified in their security plans of
changing security levels.

This can be done orally (telephone or radio), in writing or by electronic transmission (email or fax).

5.2.6 When ports and ships have different levels in force
In the situation where a security regulated ship enters a security regulated port and the security levels
are different, a ship may operate at a higher level of security than the port. If the ship is at a lower
security level than the port, it must upgrade to match the security level of the port. It is the obligation
of the port to notify ships inbound or within port facilities of the security level in force.

5.3 Security Directions
If the Department believes that a security threat is probable or imminent, in addition to changing the
security level, they may issue security directions that require additional security measures over and
above those identified in the MIP’s security. For example, if maritime security level 2 is in force when
a security direction is given, security level 2 measures remain in force and the specific additional
measures of the security direction must also be complied with. If the security direction does not
specify when it comes into force, it will become active 24 hours after it has been given. Security
directions cease if they are revoked by the Department or have been in force for a period of 3 months.

Security directions can be given to:

- a maritime industry participant or an employee of a maritime industry participant
- passengers
- people within the boundaries of a security regulated port
- people within the boundaries of a security regulated offshore facility
5.4 Impact of maritime security levels on ship’s security measures

This section identifies generic security concerns that must be addressed for each security level when preparing a ship’s security plan. It has been drawn from part B of the ISPS code. These security concerns include:

- Access to the ship
- Restricted Areas on the Ship
- Handling of Cargo
- Delivery of Ship’s Stores
- Handling Unaccompanied Baggage
- Monitoring the Security of the Ship

5.4.1 Access to the ship

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

- access ladders
- access gangways
- access ramps
- access doors, side scuttles, windows and ports
- mooring lines and anchor chains
- cranes and hoisting gear

The SSP should identify for each of the access methods above, appropriate locations where access restrictions or prohibitions should be applied for each of the three security levels. It should address the type of restrictions to be enforced at each security level and how that enforcement will occur.

This section on access control in the ISPS code looks at:

- Means of personnel identification for ship’s crew and visitors for each level of security
- Passenger proof of identity
- Denial of access to those unwilling to establish their identity and/or confirm the purpose of their visit
- Frequency of access control application

The following table provides a guide as to how access control security measures will change with different security levels.
<table>
<thead>
<tr>
<th>Security Level 1</th>
<th>Security Level 2</th>
<th>Security Level 3</th>
</tr>
</thead>
</table>
| **Access control:** At security level 1, the SSP should establish the security measures to control access to the ship, such as:  
  - checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, joining instructions, passenger tickets, boarding passes, work orders etc;  
  - In liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry on items), personal effects, vehicles and their contents can take place;  
  - In liaison with the port facility, the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;  
  - Segregating checked persons and their personal effects from unchecked persons and their personal effects;  
  - Segregating embarking from disembarking passengers;  
  - Identification of access points that should be secured or attended to prevent unauthorized access;  
  - Securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and  
  - Providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance. | **Access control:** At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:  
  - Assigning additional personnel to patrol deck areas during silent hours to deter unauthorised access;  
  - Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;  
  - Deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;  
  - Establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;  
  - Increasing the frequency and detail of searches of persons, personal effects and vehicles being embarked or loaded onto the ship;  
  - Escorting visitors on the ship;  
  - Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance; and  
  - Carrying out a full or partial search of the ship. | **Access control:** At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof.  
  The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:  
  - Limiting access to a single, controlled, access point;  
  - Granting access only to those responding to the security incident or threat thereof;  
  - Directions of persons on board;  
  - Suspension of embarkation or disembarkation;  
  - Suspension of cargo handling operations, deliveries etc;  
  - Evacuation of the ship;  
  - Movement of the ship; and  
  - Preparing for a full or partial search of the ship. |

**Searches:** At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with and proximity to the ship.  

Unless there are clear security grounds for doing so, members of the ship’s personnel should not be required to search their colleagues. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.
5.4.2 Restricted areas on the ship

The SSP needs to identify restricted areas to be established on the ship. Restricted areas:

- prevent unauthorised access
- protect passengers, ship's personnel and personnel from port facilities or other agencies authorised to be on board the ship
- protect sensitive security areas within the ship and
- protect cargo and ship's stores from tampering

The SSP needs to also ensure that there are clearly established policies and practices to control access to all restricted areas. It should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that any unauthorised presence will constitute a breach of security.

Restricted areas may include:

- navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2
- spaces containing security and surveillance equipment and systems and their controls and lighting system controls
- ventilation and air-conditioning systems and other similar spaces
- spaces with access to potable water tanks, pumps, or manifolds
- spaces containing dangerous goods or hazardous substances
- spaces containing cargo pumps and their controls
- cargo spaces and spaces containing ship’s stores
- crew accommodation
- any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship

### Security levels

<table>
<thead>
<tr>
<th>Security level 1</th>
<th>Security level 2</th>
<th>Security level 3</th>
</tr>
</thead>
</table>
| At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:  
• locking or securing access points;  
• using surveillance equipment to monitor the areas;  
• using guards or patrols; and  
• using automatic intrusion detection devices to alert the ship’s personnel of unauthorized access.  
  The SSP should establish the additional security measures to be applied, which may include:  
• establishing restricted areas adjacent to access points;  
• continuously monitoring surveillance equipment; and  
• dedicating additional personnel to guard and patrol restricted areas.  
  The SSP should establish the additional security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:  
• setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and  
• searching of restricted areas as part of a search of the ship. | At security level 2, the frequency and intensity of the monitoring of and control of access to restricted areas should be increased to ensure that only authorized persons have access.  
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-operations with those responding and the port facility, which may include:  
• setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and  
• searching of restricted areas as part of a search of the ship. | At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof.  
The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:  
• setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and  
• searching of restricted areas as part of a search of the ship. |
### 5.4.3 Handling of cargo

The security measures relating to cargo handling should:

- prevent tampering and
- prevent cargo that is not meant for carriage from being accepted and stored on board the ship

The security measures should include inventory control procedures at access points to the ship and may have to be applied in liaison with the port facility. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo is not tampered with once on board.

<table>
<thead>
<tr>
<th>Security level 1</th>
<th>Security level 2</th>
<th>Security level 3</th>
</tr>
</thead>
</table>
| **Cargo handling:** At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:  
- routine checking of cargo, cargo transport units and cargo spaces prior to and during, cargo handling operations;  
- checks to ensure that cargo being loaded matches the cargo documentation;  
- ensuring, in liaison with the port facility, that vehicles to be loaded on board car carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and  
- checking of seals or other methods used to prevent tampering.  

**Cargo checking:** Checking of cargo may be accomplished by the following means:  
- visual and physical examination;  
- using scanning/detection equipment, mechanical devices, or dogs.  

When there are regular or repeated cargo movements, the CSO or SSO may, in consultation with the port facility, make arrangements with shippers or others responsible for such cargo. This may cover off site checking, sealing, scheduling, supporting documentation, etc.  

Such arrangements should be communicated to and agreed with the PFSO concerned.  

| **Cargo handling:** At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:  
- detailed checking of cargo, cargo transport units and cargo spaces;  
- intensified checks to ensure that only the intended cargo is loaded;  
- intensified searching of vehicles to be loaded on car carriers, ro-ro and passenger ships; and  
- increased frequency and detail in checking of seals or other methods used to prevent tampering.  

**Cargo checking:** Detailed checking of cargo may be accomplished by the following means:  
- increasing the frequency and detail of visual and physical examination;  
- increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and  
- co-ordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.  

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:  
- suspension of the loading or unloading of cargo;  
- verifying the inventory of dangerous goods and hazardous substances carried on board, if any and their location.
5.4.4 Delivery of ship’s stores

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

- ensure checking of ship’s stores and package integrity
- prevent ship’s stores from being accepted without inspection
- prevent tampering and
- 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.

<table>
<thead>
<tr>
<th>Security level 1</th>
<th>Security level 2</th>
<th>Security level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>At security level 1, the SSP should establish the security measures to be applied during delivery of ship’s stores, which may include:</td>
<td>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.</td>
<td>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:</td>
</tr>
<tr>
<td>• checking to ensure stores match the order prior to being loaded on board; and</td>
<td></td>
<td>• subjecting ship’s stores to more extensive checking;</td>
</tr>
<tr>
<td>• ensuring immediate secure stowage of ship’s stores.</td>
<td></td>
<td>• preparation for restriction or suspension of handling of ship’s stores; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• refusal to accept ship’s stores on board the ship.</td>
</tr>
</tbody>
</table>

5.4.5 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.

<table>
<thead>
<tr>
<th>Security level 1</th>
<th>Security level 2</th>
<th>Security level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 percent, which may include use of x-ray screening.</td>
<td>At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• preparation for restriction or suspension of handling of unaccompanied baggage;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• refusal to accept unaccompanied baggage onboard the ship.</td>
</tr>
</tbody>
</table>
5.4.6 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:

- lighting
- watch-keepers, security guards and deck watches including patrols
- 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.

<table>
<thead>
<tr>
<th>Security level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, 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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>While underway, 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.</td>
</tr>
<tr>
<td>The following should be considered when establishing the appropriate level and location of lighting:</td>
</tr>
<tr>
<td>• the ship’s personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;</td>
</tr>
<tr>
<td>• coverage should include the area on and around the ship;</td>
</tr>
<tr>
<td>• coverage should facilitate personnel identification at access points; and</td>
</tr>
<tr>
<td>• coverage may be provided through co-ordination with the port facility.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security level 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
</tr>
<tr>
<td>• increasing the frequency and detail of security patrols;</td>
</tr>
<tr>
<td>• increasing the coverage and intensity of lighting or the use of security surveillance equipment;</td>
</tr>
<tr>
<td>• assigning additional personnel as security lookouts; and</td>
</tr>
<tr>
<td>• ensuring co-ordination with waterside boat patrols and foot or vehicle patrols on the shore side, when provided.</td>
</tr>
<tr>
<td>Additional lighting may be necessary to protect against a heightened risk of security incidents. When necessary, the additional lighting requirements may be accomplished by co-ordinating with the port facility to provide additional shore side lighting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof.</td>
</tr>
<tr>
<td>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:</td>
</tr>
<tr>
<td>• switching on of all lighting on, or illuminating the vicinity of, the ship;</td>
</tr>
<tr>
<td>• switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;</td>
</tr>
<tr>
<td>• maximising the length of time such surveillance equipment can continue to record;</td>
</tr>
<tr>
<td>• preparation for underwater inspection of the hull of the ship; and</td>
</tr>
<tr>
<td>• initiation of measures, including the slow revolution of the ship’s propellers, if practicable, to deter underwater access to the hull of the ship.</td>
</tr>
</tbody>
</table>
# Chapter 6: Contingency Planning

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Overview</td>
<td>2</td>
</tr>
<tr>
<td>6.1.1 Who must carry out security contingency planning</td>
<td>2</td>
</tr>
<tr>
<td>6.1.2 The security planning process outlined in the ISPS code and the MTOFS Act</td>
<td>3</td>
</tr>
<tr>
<td>6.2 Security risk assessment</td>
<td>4</td>
</tr>
<tr>
<td>6.2.1 Treating risks</td>
<td>4</td>
</tr>
<tr>
<td>6.2.2 Security controls used for risk treatment</td>
<td>5</td>
</tr>
<tr>
<td>6.3 Security plans</td>
<td>6</td>
</tr>
<tr>
<td>6.3.1 Maritime security plan</td>
<td>6</td>
</tr>
<tr>
<td>6.3.2 Ships Security Plans</td>
<td>7</td>
</tr>
<tr>
<td>6.3.3 Offshore Facility Security Plan</td>
<td>8</td>
</tr>
<tr>
<td>6.4 Security Controls</td>
<td>9</td>
</tr>
<tr>
<td>6.5 Piracy contingency planning and security controls</td>
<td>11</td>
</tr>
<tr>
<td>6.5.1 Best Management Practices Guide (BMP)</td>
<td>11</td>
</tr>
<tr>
<td>6.5.2 Piracy contingency planning</td>
<td>12</td>
</tr>
<tr>
<td>6.5.3 Risk assessment</td>
<td>13</td>
</tr>
<tr>
<td>6.5.4 Planning to enter a high risk area</td>
<td>14</td>
</tr>
<tr>
<td>6.5.5 Ship protection measures</td>
<td>15</td>
</tr>
<tr>
<td>6.5.6 Recommended actions in event of a pirate attack</td>
<td>18</td>
</tr>
</tbody>
</table>
6.1 Overview

Contingency planning involves systematically identifying things that can go wrong in a given scenario and figuring out how to stop, reduce or mitigate negative impacts. Someone involved with contingency planning moves away from the idea that fate will decide the outcome of a situation and arms themselves with strategies for avoiding or coping with potentially bad situations.

In maritime security contingency planning, the planner considers a range of low and high probability events that could have major impacts on everything from human lives to loss of income or damage to infrastructure. The aim is not to identify and plan for all the possible scenarios as this would take an enormous amount of time and would be practically impossible. The planners instead focus on major contingencies and possible responses to these.

While security threats rarely play out as identified in the contingency plan, it is well known that ships and ports that have thought about appropriate responses to contingencies are better prepared when a real security threat occurs.

Contingency planning is about asking “what if” type questions such as the following below:

- What events may occur that require a maritime security response?
- What are the major impacts of the event and what is the likelihood of them occurring?
- What is the worst case scenario of events for the situation?
- What scenarios are possible for the situation?
- What event would cause the greatest disruption of current activities and plans?
- What happens if costs of the plan are excessive?
- What happens if delays occur?
- Who are the key people involved with the scenario?
- What are the expected motives and moves of the criminals/terrorists?
- Who or what might impede implementation of the plan?

6.1.1 Who must carry out security contingency planning

Security contingency planning has become a key part of any transport related industry. Just look at how aviation security changed after the September 11 attacks.

While all players in the maritime industry are encouraged to develop contingency plans, the ISPS code and the MTOFS Act require the following participants to undergo a formalised process that is overseen by the Department of Transport and Infrastructure’s Office of Transport Security:

- Security regulated ships
• Security regulated ports
  ▪ The port operators themselves
  ▪ Any facility operators within the port
  ▪ Any operators who provide a service to the port

• Security regulated offshore facilities.

Chapter 3 has definitions of security regulated ships, ports and offshore facilities.

6.1.2 The security planning process outlined in the ISPS code and the MTOFS Act

All maritime industry participants identified in the above section must carry out the planning process outlined below. They must carry out a security risk assessment, develop a security plan and have that plan approved by the Department of Transport and Infrastructure.

<table>
<thead>
<tr>
<th>Security Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>To identify the threats and vulnerabilities specific to the ship, port or offshore facility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>A plan, based on the security risk assessment, that addresses the security threats identified and outlines security measures to be taken at all three MARSEC levels.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Plan approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is a legal requirement for these plans to be submitted and approved by the Department of Transport and Infrastructure</td>
</tr>
</tbody>
</table>

6.1.2.1 Ship Security Plans and International Ship Security Certificates (ISSCs).

Once the Ship Security Plan has been submitted to the Department and approved, the ship is issued with an interim International Ship Security Certificate (ISSC). ISSCs are required by all regulated Australian ships. The Department will then send out a maritime security inspector to verify that the ship is operating in accordance with their security plan. If the ship passes the verification assessment, it is issued with a full ISSC which it must hold to visit Australian security regulated ports and security regulated ports overseas.
6.2 Security risk assessment

The security risk assessment is an essential part of the security contingency planning process. It uses qualitative risk assessment theory and the two main references for security risk assessment are:

- AS/NZ 4360 Risk Management
- The companion handbook HB 436:2004 Risk Management Guidelines

Australian maritime industry participants who are conducting a security risk assessment are strongly encouraged by the Department to use the methods outlined in the references above.

Risk assessments are required before the development of any maritime, ship or offshore facility security plan. A risk assessment establishes the context or the risk environment by looking at current threat levels and the latest intelligence issued on threats and criminal behaviour. Risks to the ship, port or offshore facility are then identified and analysed to find the likelihood and consequences of a threat occurring. The threats are then evaluated to find which ones have the biggest impact and whether the port, ship or offshore facility needs to take action to reduce this impact. Threats that are assessed as having an unacceptable impact are then addressed or ‘treated’ and this information forms the basis of the security plan.

It is important to look at the threats in the context of all three maritime security levels. For example at Marsec 1, where the threat of a terrorist attack is low, basic security controls will be put in place to deal with this threat. If intelligence suggested terrorists were planning an attack and the security level was raised to Marsec 3 (where a security threat is imminent), it is appropriate to put a much higher level of security controls in place to guard against an impending threat.

6.2.1 Treating risks

The options for treating the risk include:

- **Reduce**: Control improvements or new controls are introduced in order to reduce the risk.
- **Avoid**: Likelihood is reduced by ceasing or reducing activity which creates an exposure.
- **Share**: The risk is ‘shared’ with a third party e.g. by outsourcing, through insurance or by seeking police assistance.
- **Tolerate Retain and Monitor**: Either the risk is determined to be tolerable or the treatment options are determined to be ineffective or not cost-effective at present. The risk therefore has to be tolerated but is monitored pending a change in circumstances allowing other options to be considered.
6.2.2 Security controls used for risk treatment

The controls used to treat security risk take many different forms, for example:

- Improvements to physical security (e.g., perimeter security)
- Improved access controls
- Better security education and contingency training
- Enhanced manifest procedures
- Increased information security protection
- Better security procedures
- Requirement for external parties such as contractors to conform to a high standard of security.

These controls are described in more detail in section 6.4.
6.3 Security plans

Security plans are required by law for security regulated maritime industry participants. The security plans are based on the security risk assessment and must be government approved.

6.3.1 Maritime security plan

Maritime security plans set out the security measures and procedures that are to be implemented at each maritime security level to safeguard maritime transport or offshore facilities.

Various maritime industry participants are required to have and comply with maritime security plans. They are:

- operators of security regulated ports
- operators of facilities at security regulated ports and
- providers of services at such ports

6.3.1.1 Maritime security plan content

Maritime security plans must include:

- a security assessment for the participant’s operation
- the security activities or measures to be implemented at each security level
- a reference to all security officers responsible for implementing and maintaining the plan
- provisions for the use of declarations of security and
- how the plan will contribute to maritime security outcomes

Maritime security plans should also address the following elements:

- measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship
- measures designed to prevent unauthorised access to the port facility, to ships moored at the facility and to restricted areas of the facility
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface
- procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3
- procedures for evacuation in case of security threats or breaches of security
- duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects
- procedures for interfacing with ship security activities
- procedures for the periodic review of the plan and updating
- procedures for reporting security incidents
- identification of the port facility security officer including 24-hour contact details
- measures to ensure the security of the information contained in the plan
• measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility
• procedures for auditing the port facility security plan
• procedures for responding in case the ship security alert system of a ship at the port facility has been activated and
• procedures for facilitating shore leave for ship’s personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers’ welfare and labour organisations

6.3.2 Ships Security Plans

All registered Australian ships are required to have and comply with a ship’s security plan. Ship security plans are based on the ships security assessment and identify the security measures that ships must implement when different maritime security levels are in force.

6.3.2.1 Ship security plan content

A ship security plan must include:

• a security assessment for the ship
• the security activities or measures to be implemented at each security level
• a reference to all security officers responsible for implementing and maintaining the plan
• provisions for the use of declarations of security
• how the plan will contribute to maritime security outcomes and
• a statement of the authority of the master of the ship.

Chapter 4 section 4.4 outlines the security measures that must be addressed in every SSP for each of the different maritime security levels. The areas that must be addressed are:

• access to the ship
• restricted areas on the ship
• handling of cargo
• delivery of ships stores
• handling unaccompanied baggage
• monitoring the security of the ship

A Ship Security plan must address, 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 unauthorised 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
• procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting of systems to limit false alerts

6.3.3 Offshore Facility Security Plan

Offshore security plans set out security measures and procedures to be implemented at the different maritime security levels to safeguard against unlawful interference with an offshore facility.

Various offshore industry participants are required to have and comply with offshore security plans. Offshore industry participants who may be required to have offshore security plans are:

• offshore facility operators and
• offshore service providers

6.3.3.1 Content of an offshore facility security plan

Offshore security plans must:

• include a security assessment for the participant’s operation
• detail security activities or measures to be implemented by the participant for maritime security levels 1, 2 and 3
• detail all security officers responsible for implementing and maintaining the plan;
• set out conditions for the use of declarations of security
• demonstrate how the plan will contribute to maritime security outcomes and
• complement to the fullest extent possible, the occupational health and safety requirements under the laws of the Commonwealth, state or territory applying at the facility.
6.4 Security Controls

This section lists common security controls that may be in place at a port, ship or offshore facility where you work or visit.

Physical access controls prevent unauthorised entry to ports, vessels and cargo.

- Positive identification of employees, visitors, service providers and government officials at restricted points of entry
- Limited access for service providers to the areas where they have legitimate business

Boarding and disembarking vessels

- All crew, employees, service providers and visitors may be subject to search when boarding and disembarking
- A vessel visitor log must be maintained and temporary visitor pass must be issued as required by the ship’s security plan
- All crew, crew members, service providers and visitors (including government officials) must display proper identification as required by the applicable security plan.

Employees

- An effective employee identification system must be in place for positive identification and access control purposes. Refer to the Maritime Security Identification Card system used in Australia (Chapter 4, section 4.3.8)
- Employees should only have access to areas needed for the performance of their duties
- Procedures to issue, remove and change access devices (cards, keys etc) must be documented.

Visitors, contractors and service providers

- Anyone who is not an employee must present photo identification when arriving at the port or vessel.
- A visitor log must be used
- The measures described in the security plan for escorting visitors must be followed
- The security plan should outline procedures to identify, challenge and address the issue of unauthorised personnel entering the ship or facility.

Personnel security

- Procedures must be in place to screen prospective employees and periodically check employees
- There must be procedures in place to remove identification, ship/facility and system access for employees that have been terminated.
Manifest procedures

Procedures must be in place to ensure the information in the cargo manifest accurately reflects the information provided to the carrier by the shipper or agent. Document control must include safeguarding computer access and information.

Security awareness and training

Establishing a security awareness program can foster the awareness of security vulnerabilities to vessels and maritime cargo. Employees must be aware of the procedures in place to report a security concern of incident.

Physical security measures

- **Fencing**: perimeter fencing should enclose areas around cargo handling, storage facilities and terminals and be regularly inspected for damage
- **Gates**: gates through which vehicles and people enter or exit must be manned and/or monitored. They must be secured when not in use.
- **Parking**: If possible, private vehicles should be parked away from cargo handling, storage areas and vessels
- **Building structure**: buildings should be constructed of materials that are resistant to break-ins. These buildings should be maintained and regularly inspected for damage.
- **Locking devices and key controls**: all external windows, gates and fences must be secured with lockable devices. The issuing of keys should be tightly controlled.
- **Lighting**: adequate lighting should be provided inside and outside the facility including the following areas: entrances, exits, cargo handling and storage areas, fence lines and parking areas. While in port, the pier, and waterside of the vessel should be adequately illuminated
- **Alarm systems and video cameras**: These should be used to monitor the premises and prevent unauthorised access to vessels, cargo and storage areas. Areas where alarm systems and video cameras should be installed should be identified in the security risk assessment.

Information technology security

- **Password protection**: IT security policies and procedures need to be in place and adequate training needs to be provided to employees
- **Accountability**: A system needs to be in place to identify the abuse of IT, including improper access, tampering or the altering of business data.
6.5 Piracy contingency planning and security controls

6.5.1 Best Management Practices Guide (BMP)

Several key stakeholders (such as the International Maritime Bureau and the International Chamber of Shipping) have banded together to produce a document that provides guidance to companies, masters and crews to prepare for a piracy threat.

The Best Management Practices for Protection against Somali- Based Piracy (BMP) contains suggested practices for ship operators and masters who are transiting through areas of high risk. This section on piracy contingency planning is strongly based on BMP’s content and a key point summary provided in the BMP document is below:

- **Do not be ALONE**
  - Report to UKMTO (email or call) and register transport with MSCHOA (the next page explains these acronyms)
  - Use the internationally recognised corridor (RTC) or group transit scheme or independent convoy
  - It is recommended to keep AIS turned on

- **Do not be Detected**
  - Keep track of NAVWARNS and vessel relevant websites (MSCHOA and NATO shipping centre) for known pirate operating locations.
  - Use navigation lights only

- **Do not be Suprised**
  - Increase vigilance, CCTV and radar

- **Do not be Vulnerable**
  - Use visual (deterrent) and physical (preventative) Ship Protection Measures

- **Do not be Boarded**
  - Increase to maximum speed
  - Maneuver the vessel

- **Do not be Controlled**
  - Follow well practiced procedures and drills
  - Use of citadels (only with prior agreement of master/ship operator and fully prepared and drilled) noting a naval military response is not guaranteed.
  - Deny use of tools, equipment, access routes
6.5.2 Piracy contingency planning

While the BMP focuses specifically on Somali-based piracy, many of the techniques and practices listed can be used in high risk areas around the world (such as the Malacca straights).

In a similar approach to the ISPS, the BMP guide recommends the use of risk assessment, planning and then lists protection measures that can be used depending on the results of the risk assessment. The BMP also provides a summary of actions to be taken once an attack is underway.

**Agencies that can assist when transiting the high risk waters of Somalia**

**MSCHOA:** The Maritime Security Centre – Horn of Africa (MSCHOA) aims to provide a service to mariners in the Gulf of Aden, the Somali Basin and off the Horn of Africa. Their website provides important intelligence and warning to mariners transiting through the region. Vessels can register with MSCHOA which provides a 24 hour manned monitoring service of vessels transiting through the Gulf of Aden.

**UKMTO:** The United Kingdom Marine Trade Operations (UKMTO) has moved its focus towards Anti-Piracy and Maritime Security Operations since 2007 and is now the primary point of contact for merchant vessels in case of a pirate attack. The UK Maritime Trade Operations Office (UKMTO) in Dubai acts as the primary point of contact for merchant vessels and liaison with military forces in the region. UKMTO Dubai also administers the Voluntary Reporting Scheme, under which merchant vessels are encouraged to send regular reports, providing their position/course/speed and ETA at their next port whilst transiting the region.
6.5.3 Risk assessment

Ship operators and masters are strongly encouraged to carry out a thorough risk assessment prior to transiting through a high risk area. The risk assessment should be similar to the methods outlined earlier in this chapter (identifying the likelihood and consequences of a piracy attack to a vessel). It should be based on the latest information which can be gained from relevant agencies.

The following elements should be taken into consideration when conducting a risk assessment.

**Crew safety:**
- When developing measures to prevent illegal boarding, care should be taken to ensure crew will not be trapped inside and can be able to escape if there is another type of emergency – e.g. a fire. Piracy prevention should not interfere with ship’s safety.
- Careful consideration should be given to the location of a safe muster point (or citadel)
- Consideration should be given to the protection of crew who are required to remain on the bridge during a pirate attack, considering it is common for pirates to fire on the bridge as part of attack.

**Freeboard:**
- Note that pirates will likely attempt boarding from the lowest point above the waterline (making it easier to climb onboard) these points are often on the quarter or vessel’s stern
- Experience suggests that vessels with a minimum freeboard greater than 8m have a better chance of escaping a piracy attempt
- A large freeboard alone may not be enough to deter a pirate attack

**Speed:**
- Speed is one of the most effective ways to deter a pirate attack – to date there have been no reported attacks where pirates have boarded a ship with a speed over 18 kts. Note that it is possible for pirate tactics and techniques to develop to enable the boarding of fast-moving ships.

**Sea state**
- Pirates usually mount attacks from small craft (skiffs) and their operations are usually limited to moderate sea states
- It is likely to be difficult to operate a small craft effectively in sea state 3 and above.
6.5.4 Planning to enter a high risk area

Company considerations

It is recommended that companies:

- Obtain the latest information: It is strongly recommended that companies register with the MSCHOA when transiting through waters prone to attack from Somali pirates. The restricted section provides up to date information and the latest intelligence for these waters. The NATO shipping website also contains important information. Continue to monitor these websites for the latest threat information and warnings.

- Review the Ships Security Assessment and Ships Security plan given the latest information available. The Company Security Officer (CSO) should discuss the SSP with the Ship’s Security Officer (SSO) and master when planning the transit.

- Plan and install ship protection measures outlined in the SSP and identified in the risk assessment

- Ensure crew training is conducted

- If operating in Somali waters, submit a vessel movement form to MSCHOA so they are aware the vessel is in the vicinity and can track for added security.

Ships’ master considerations

Ships’ masters preparing to enter high-risk waters should:

- Brief crew and conduct drills on the measures to protect the ship when transiting through the high risk area

- Prepare an emergency communications plan – this should have all relevant emergency numbers of agencies to assist such as the MSCHOA and UKMTO in Somali waters.

- Define the AIS policy of the ship. While the master has the discretion to switch off AIS, it is recommended that the AIS is kept on to provide basic information such as the ship’s identity, position, course, speed, nav status and safety related information

- Ensure movement forms submitted: ensure vessel movement form submitted to MSCHOA and report is made to the UKMTO on entering the high risk area if operating in Somali waters.
6.5.5 Ship protection measures

The following methods of protecting ships from pirate attack are recommended in the Best Management Practices Guide:

Watchkeeping

When transiting through high risk areas is recommended that extra vigilance is applied by:

- Providing fully briefed, additional lookouts for each watch
- Maximising the alertness of lookouts by a more frequent rotation (reducing the watch time)
- Ensure the correct equipment for lookouts – eg antiglare binoculars
- Consider using night vision goggles
- Maintain a constant radar watch

Bridge protection measures

In the initial phase of a pirate attack, pirates usually direct firepower towards the bridge to force the ship to stop. If pirates are able to board the vessel, they usually make their way to the bridge to take control.

- Provide an extra level of protection to the bridge team – e.g. Kevlar jackets and vests, helmets.
- Cover bridge windows with a blast resistant film to minimise damage from flying glass
- Use fabricated metal plates which can be swung in place over windows and doors to provide extra security during an attack
- Sandbags have been used to protect access to bridge wings (the after parts are often open)
- The rear and side of the bridge can be protected using double layer chain link fence. This has been proven to reduce impact of a rocket propelled grenade (RPG). There are anti RPG screens on the market.

Access control to bridge, accommodation and machinery spaces

- Doors and hatches to the bridge, accommodation and machinery spaces should be properly secured to prevent them being opened by pirates
- Where a door or hatch is on an escape route, it is essential it can be operated by a seafarer trying to escape using that route. E.g. if a door or hatch is locked – a key must be visible in a clear location.
- Once doors and hatches have been locked – use only as a minimum for routine access
- Consider lifting or blocking accommodation ladders so they can’t be used and restrict external access to the bridge
• Pirates have been known to gain access through portholes. Steel bars can be a useful security measure
• Procedures for restricting access to the bridge, accommodation and machinery spaces should be clearly set out and practised (drilled) before entering a high-risk area

**Physical barriers**

Physical barriers are useful to deter pirates from boarding the ship. They can include:

• Razor wire
• Fixed metal grills topped with metal spikes have been used on some vessels
• Electrified barriers (following a full risk assessment and not appropriate for vessels carrying hydrocarbons). It is recommended that warning signs of the electric barrier are placed inward facing in the language of the crew and outward facing in Somali (or language of the pirates).
• Outward signs can be used as a deterrent even if the physical control (such as an electric barrier) is not in place

**Water spray and foam monitors**

Water spray and foam monitors have been successfully used in conjunction with other controls. Where possible they should be rigged in a ready state where they can be activated remotely. They make it difficult for a vessel to stay alongside and hard for pirates to climb up the side of the vessel. These can include:

• Fire hoses and foam monitors
• Water cannons
• Ballast pumps
• Steam and hot water
• Water spray rails
• Foam (in addition to the vessels supply for fire fighting)

**Alarms**

Sounding a piracy alarm does two things:

• Tells the ship’s company an attack is under way
• Tells the pirates the ship is aware of their attack

Continuous sounding of the vessel’s alarm and foghorn can distract the pirates. It is important for the crew to be drilled and familiar with the piracy alarm.
Other considerations

- **Manoeuvring:** In addition to increasing speed the vessel can be manoeuvred to create difficulty for the pirates. It is recommended that, when navigationally safe to do so, the vessel practices high-speed manoeuvring to provide the maximum difficulty for the pirates without reducing the vessel’s speed.

- **CCTV** can be used to monitor pirate attack remotely and provide useful evidence of the attack.

- **Upper deck lighting:** ships should proceed with only navigation lights but should have search lights rigged for immediate use and appropriate lighting for the stern area

- **Protection of ships’ equipment and tools:** secure all tools and equipment that may be used by pirates to gain further access to the vessel once they have boarded.

- **Safe muster points and citadels:** consideration should be given to a safe muster point or citadel to ensure maximum crew safety.
  - A safe muster point is a designated area designed to give maximum protection to crew and often located low down in the vessel. In the event of a pirate attack, members of the crew not required on the bridge should muster at this point. It is a short term muster point designed to provide ballistic protection should the pirates attack with RPGs and small arms.
  - A citadel is a pre planned area, purpose built into the ship, where in the event of imminent boarding, all crew will seek protection. The concept of a citadel approach is lost if any crew member is left outside.

- **Private security contractors:** The use of private security contractors is up to the individual ship operators following their own risk assessment. The use of unarmed security contractors can be a useful addition to the security plan. The use of Military Protection Vessel Detachments is the preferred option when using armed guards. The BMP does not provide a recommendation or endorsement for the use of armed guards.
6.5.6 Recommended actions in event of a pirate attack

**Approach stage**

- Increase to full speed and manoeuvre vessel to provide the greatest closest point of approach by the pirates.
- Initiate the pre planned emergency procedures
- Activate the piracy emergency communications plan
  - Sound the piracy alarm
  - Report the attack to relevant authorities
  - Activate the ship’s security alert system
  - Send a distress message via DSC and INMARSAT C as required
  - Switch on AIS
- Muster crew at safe point or citadel except for those required on bridge
- As vessel approaches and if sea state allows, alter course to provide the maximum exposure to wind and waves by pirates.
- Activate spray and other self defence measures
- Secure external doors and where possible, internal rooms
- Sound ship’s fog horn/whistle in an attempt to distract the pirates

**Attack stage**

- Reconfirm ship’s crew are in a position of safety
- Manoeuvre the ship (small alterations of helm) to create wash and make coming alongside difficult for the pirates. This must not be at the expense of losing speed.

**Pirates take control**

- Try to remain calm
- Reconfirm AIS is on, UKMTO has been informed (if in Somali waters), and SSAS is activated
- Offer no resistance to pirates once they are on the bridge. They are likely to be aggressive, highly agitated and possibly under the influence of drugs. Staying calm and co-operating minimises the risk of harm
- If evacuating the bridge and engine room, stop the engine if navigationally safe to do so.
- Leave any CCTV running
Chapter 7 – Techniques to Circumvent Maritime Security Measures

7.0 Overview ........................................................................................................................................ 2

7.1 Common measures used to circumvent port and vessel security .............................................. 2
  7.1.1 Facility access controls ............................................................................................................. 3
  7.1.2 Circumventing gates, locks and fences .................................................................................... 3
  7.1.3 Methods for circumventing lock and key controls ................................................................. 3
  7.1.4 Techniques for circumventing CCTV security systems ........................................................ 4
  7.1.5 Tactics used to circumvent security communications .......................................................... 4
  7.1.6 Circumventing security at the main port access gate ............................................................ 5
  7.1.7 Techniques to circumvent ship access control procedures: .................................................. 5

7.2 Techniques to circumvent cargo security measures ..................................................................... 7

7.3 Techniques used to circumvent searches for illegal items ........................................................... 9

7.4 Corruption of port security/ ship personnel ............................................................................... 11
  7.4.1 Typical targets of corruption .................................................................................................. 11
  7.4.2 Methods used by corrupt insiders to smuggle cargo/ weapons ............................................. 11
  7.4.3 Ways of preventing internal corruption ................................................................................. 12
7.0 Overview

As soon as security measures are put in place it is likely that criminals are figuring out how to outsmart the system. It is important to understand the common ways in which criminals circumvent security measures because everyone in the maritime industry has a role to play regarding security. For example, you could uncover a security threat just by noticing and reporting suspicious behaviour. You may even be targeted by a criminal or terrorist who is seeking to gather information or gain access to a restricted area by befriending you.

This chapter looks at the most common ways criminals attempt to gain access to ports and ships. This includes how access controls such as ID cards and car passes can be avoided, how CCTV can be thwarted and easy ways of breaching physical security such as locks, gates and fences.

This chapter describes suspicious behaviour associated with criminals and terrorists and takes a deeper look at the ways smugglers can breach container security. It describes techniques criminals and terrorists use to evade searches and outlines how criminal organisations can corrupt port, ship or shipping company staff to threaten security by gaining intelligence or illegal access to high risk areas.

7.1 Common measures used to circumvent port and vessel security

The primary purpose of port and vessel security is to protect assets and personnel from intruders. This is achieved by denying them access, ensuring effective deterrents are in place, detecting security breaches and containing breaches that do occur. This section looks at common techniques used to circumvent port and vessel security.
7.1.1 Facility access controls

Access controls are ways of restricting entry into a secure port or ship and include:

- Issuing access/ id cards for port and ship access
- Car passes
- Contractor/ visitor passes

Techniques used by criminals to avoid these controls include:

- gaining access to offices that issue car passes and id cards and stealing these items
- entering unlocked cars or breaking into cars and stealing passes and ID cards
- stealing a port or contractor vehicle and using it to gain access.

7.1.2 Circumventing gates, locks and fences

Common physical security measures include barriers such as fences and gates that can be both manned and unmanned. Locks are a frequently used security measure and include anything from padlocks to combination locks to electromechanical locks and safes.

Common methods used to circumvent these security measures include:

- Taking advantage of locks left open, removing them and replacing with the criminal’s own locks
- Removing the base of the gate and hardware from the ground and gaining access
- Driving vehicles through the fence
- Climbing over the fence
- Gaining access under the fence by digging or by removing the bottom rail
- Making duplicate keys from inexpensive locks that have visible numbers or are easy to replicate
- Using bolt cutters to cut locks

7.1.3 Methods for circumventing lock and key controls

Most secure ports and ships have tight security measures concerning keys and keyboards. Only cleared personnel can access certain keys and they must sign the key in and out of a log. Ways that criminals can evade key security include:

- creating duplicate keys
- stealing keys from an employee
- stealing keys from an unsecured key storage location
- failure of management to collect keys from terminated employees
• using a corrupt employee to gain access to a key, e.g. the employee reports missing or lost key and passes it on to a criminal – if poor key controls are in place a new one may be issued without further investigation
• standing near an employee opening a combo lock that isn’t covered by a hand

7.1.4 Techniques for circumventing CCTV security systems

CCTV security systems are widely used in most secure ports and ships. While the camera itself may act as a deterrent, smart criminals often check the effectiveness of the camera in bad weather conditions or at night. They also test to see how closely the footage is monitored. Methods used to thwart CCTV systems include:

• cutting camera power supply
• damaging cameras
• reducing camera effectiveness (e.g. placing chewing gum over the lens)
• testing the CCTV effectiveness during night time or bad weather e.g. if no security response to fake a penetration attempt, it’s likely the camera clarity is not effective
• Evaluating the coverage of a CCCTV camera - checking for “dead zone” and inadequate coverage of the perimeter extremes

7.1.5 Tactics used to circumvent security communications

Ship and port communications can be monitored by criminals and terrorists, especially if secure frequencies are not in use. It is important, especially if operating at MARSEC 2 or 3 that any industry personnel communicating by using non-secure means thinks about if it’s ok for others to hear their conversations. Techniques used by criminals to gain intelligence and confuse authorities include:

• using a scanner to monitor the activities and actions of port security
• stealing a radio from the port during the criminal/terrorist operation and communicating false information or instructions in order to confuse police or port security,
• calling in a large volume of phony bomb threats, fires and suspicious persons reports to overwhelm response teams and distract security forces from actual terrorist activities.
7.1.6 Circumventing security at the main port access gate

Access by vehicle to a secure port and the ships within is normally via manned security gates. Below are techniques used by criminals to gain access to the port by circumventing the usual security controls.

- Driving through the main entrance and waving a driver’s license, acting as if authorised to enter
- Obtaining an ID card from an authorised person and using it to gain access
- Obtaining a copy of a parking pass or ID card, making colour copies, laminating the items in plastic and waving them at the security officer
- Convincing the security officer that a criminal is authorised and talking their way into the facility – for example, claiming to be a contractor meeting a ship or an employee
- Hijacking delivery vehicles and replacing the driver with a terrorist/criminal
- Posing as a jogger and jogging through the main gate, waving to the security officer
- Taking a taxi cab and telling the driver the criminal has to meet the ship. Allowing the cab driver to tell the security officer he is taking him to meet the ship
- Stealing contractor vehicles and driving them past unchallenged
- At night, driving the vehicle up to the gate at high speed with bright lights
- Wearing sunglasses and a baseball cap to conceal identity from security officer when showing ID card
- Using an unknowing or corrupt friend or hostage to gain access to the facility

7.1.7 Techniques to circumvent ship access control procedures:

Gangway security is an essential part of the Ship’s Security Plan. To control access on and off the vessel personnel must display correct identification as part of the ship’s company. If they are not a member of the ship’s company a visitor may be granted access if they meet certain security requirements and they have signed the visitor’s log. The following are techniques used by criminals to evade gangway controls:

- Insisting that they were already cleared by the main gate security and that they resent being checked again by the security positioned near or on the ship
- Developing first name relationships with port and ship security personnel. This will require at least a few weeks of work; however it will increase opportunities for unrestricted access to the ship
- Developing close relationship with ship’s captain or key ship’s staff member, hoping they will vouch for them
- Wearing a suit and looking important – acting as if they are supposed to be in or on the ship
- Wearing a hard hat and carrying a clipboard and 2 way radio so that they appear to be conducting an inspection
- Obtaining a port supplier uniform and port badge – walking up the gangway and flashing a fake id
- Using the ‘honey trap’ – pretending to be a lady friend of the Captain or an officer and claiming a scheduled visit
- Claiming to be a ship chandler and hiding weapons inside the goods to be delivered

Pretending to conduct an audit is a technique used by criminals to gain access to ships

The ‘Honey Trap’ is an effective way of evading port and ship security
7.2 Techniques to circumvent cargo security measures

As 90% of the world’s trade occurs by ship, cargo security is of high importance. Container seals have been used for many years as a method to tell if containers have been illegally accessed or tampered with.

Seals are placed on loaded containers and determine whether cargo has been:

- Stolen
- Switched or
- extra items inserted (such as drugs, narcotics and explosives)

Seals can also be placed on empty containers when they are transported to the loading area to detect for stowaways, or contraband.

Criminals and terrorists have become skilled at circumventing the effectiveness of cargo seals.

In areas known for drug smuggling such as Colombia and Panama, it is well known that smugglers employ people who are highly skilled in areas including jewellery making, watch repair and plastic manufacturing to develop ways to compromise seals. Highly skilled people in these trades have the ability to make it look as if there is little or no external evidence of tampering.
Seals used in commercial cargo operations have a unique serial number and barcode. The seal number is recorded at the time of issue and is passed on as the cargo moves through the supply chain.

Seals can be purchased by anyone over the internet or directly from the factory, even the high-security seals. While checking for tampering may be easy in a well-lit laboratory, security personnel often carry out their searches in low-light conditions or difficult environmental conditions such as driving rain. The table below lists the generic types of cargo seals, their use and their susceptibility to tampering.

<table>
<thead>
<tr>
<th>Seal type</th>
<th>Use</th>
<th>Ease of tampering/ common methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plastic seals</td>
<td>Used to seal empty containers following inspection, ready to be loaded with cargo</td>
<td>Easy to defeat – knife or razor to cut plastic strap where it enters the locking base and reattached with a small amount of superglue</td>
</tr>
<tr>
<td>Metal straps</td>
<td>Usually used to seal empty containers following inspection, ready to be loaded with cargo. May sometimes be used on loaded containers shipping internationally</td>
<td>Easy to defeat – inserting a hair pin or piece of wire into the locking ball base to release the spring that locks the seal in place</td>
</tr>
<tr>
<td>Cable seals</td>
<td>Used in areas where there is a high threat of cargo theft. They provide a higher level of security than plastic and metal straps</td>
<td>Moderate security – can be defeated by cutting near the point of insertion into the female bolt, drilling out the mechanism inside and then reinserting the male using a suitable adhesive.</td>
</tr>
<tr>
<td>Approved high-security seals that have passed international testing standards (ISO 17712:2006)</td>
<td>EG bolt and bottle seals. Used on loaded cargo containers.</td>
<td>Higher security – but with vulnerabilities known to be exploited by terrorists and criminals. The seals can be opened by a skilled person with minimal evidence of tampering and serial numbers can be altered.</td>
</tr>
</tbody>
</table>
Smart, electronic seals that have passed international testing standards (ISO 18185)

An e-seal tracks shipments and monitors if security has been compromised. It has sensors that detect changes in light, temperature inside the container. It communicates any breaches of security the next time the e-tag is read. GPS can add to the e-seal’s capability.

High security. While they are the likely future of container security and are effective, they are expensive when compared with other types of seals.

7.3 Techniques used to circumvent searches for illegal items

As security measures get tighter, criminals and terrorists get more creative. Here are some examples of ways to circumvent security searches described by Customs officers in the US.

- Tailored vest, underwear and leg bandages containing custom-shaped drug/ money and contraband. Look for loose fitting clothes or clothes not consistent with current climate and a stiff posture and walk. Ask the subject to bend over – if they have difficulty then suspicion should be aroused.
- Trouser waistband filled with heroin. Look for bulges in trousers waist band lining. Search inner stitching of trousers.
- False shoes and heels of shoes worn by subject or carried in luggage. Look for regluing of outer or inner sole and heel. Look for shoes that show little wear compared with other clothing that looks well worn. Sniff for glue odour.
- Heroin concealed within professionally sealed liquor bottles further contained within cartons. Look for bottles that don’t “slosh” when shaken.
- Beer and soft drink cans with professionally sealed lids or screw tops. Look for a sloshing sound. Tap the upper portion to produce a resonant sound when the bottom produces a dull muted sound. Cans filled with cocaine are heavier than those filled with beer.
- Aerosol spray cans modified in three ways:
  1. Totally filled with drugs and permanently sealed,
  2. Fitted with a cylinder of a bona fide product or
  3. Bottom end fitted with an ‘o’ ring female threaded adaptor that takes a male plug. Look for an aerosol that does not produce liquid but feels heavy
as if full. In case 2, only a small quantity of gas is included to make 2 or 3 sprays.

- Tin cans sealed professionally with a commercial canning machine.
- False bottom of wooden shipping crates.

There are many other examples of creative criminals and their methods will evolve as our security technology and techniques become smarter and more developed.
7.4 Corruption of port security/ ship personnel to provide inside assistance to criminals or terrorists

Cargo thieves, stowaways, pirates, drug smugglers and terrorists often rely on a corrupt insider to provide them with the information and access they need to circumvent port and ship security measures. Criminal organisations and terrorist groups are experts in developing links within maritime related companies and over the years they have developed many techniques and tactics to circumvent security policies, measures and procedure.

7.4.1 Typical targets of corruption

Personnel who are targeted by criminal organisations to engage in corruption within the maritime industry generally know about:

- the movement of legitimate cargo
- documentation
- international trade and loopholes in the security configuration
- local security procedures
- law enforcement

Corrupt employees may work in any company involved in the shipping industry or cargo supply chain. Criminal operators may be found at any level; e.g. personnel at the factory, plant, warehouse, loading dock etc.

7.4.2 Methods used by corrupt insiders to smuggle cargo/ weapons

Terrorists have often resorted to methods used by drug smugglers to transport their explosives or devices. They have also been known to contract smuggling organisations to transport their cargo for them. Below are three ways that insiders can assist smugglers in their efforts to transport illegal cargo.
• The tap: this is the illegal opening of international cargo or containers for the purpose of taking out the contraband before a routine customs inspection. In the case of terrorists, they likely would open (tap) the cargo or container at some point prior to loading at a foreign seaport and insert explosives, WMDs or unauthorised personnel.

• The switch: this is the exchange of a clean shipment for one with contraband. It could occur at any link in the cargo supply chain.

• The pull: this involves taking an entire shipment that is either manifested or not manifested prior to customs inspection. In the case of a terrorist operation this would most likely occur after the cargo arrives.

7.4.3 Ways of preventing internal corruption

The following are ways of preventing internal corruption within the shipping industry:

• Perform pre-employment screening for past criminal activity or dishonest behaviour

• Pre-employment and periodic background investigations to include a lifestyle evaluation of all employees. Fortunately, employees involved in criminal activity have a tendency to want to spend the extra money soon after receiving it. Look for changes in lifestyle that reflect unexplainable surges in spending (new cars, new home etc).

• Create an internal security team which liaises with law enforcement, collects information related to terrorist and other criminal threats to company operations and monitors the activities of employees.

• Lie detector tests of persons suspected in criminal activity.

• Security officers and supervisors conduct frequent inspections of facilities and cargo handling areas looking for suspicious activity signs of unauthorised access and indications that cargo or containers have been tampered with or seals violated.

• Rotate personnel between positions or ships as practical and permissible.

• Look for altered or forged documentation, unusual changes to cargo documentation and computer data bases, violations of access control and password procedures to databases and unauthorised modifications to shipping documentation files.

• Watch for fake bills of lading, tally logs etc.
Chapter 8 – Recognition and awareness of weapons, dangerous substances and devices and the damage they can cause

8.1 Overview ..................................................................................................................................... 2

8.2 Weapons used in terrorist attacks................................................................................................ 2
  8.2.1 IEDs and explosives .................................................................................................................... 2
  8.2.2 Improvised Explosive Devices (IEDs) ........................................................................................... 2
  8.2.3 IED components ........................................................................................................................... 3
    8.2.3.1 Methods of IED delivery........................................................................................................... 4
    8.2.3.2 IED impacts ............................................................................................................................ 5

8.3 Weapons of mass destruction ...................................................................................................... 7
  8.3.1 Chemical weapons ....................................................................................................................... 7
  8.3.2 Biological weapons ....................................................................................................................... 7
  8.3.3 Radiological weapons .................................................................................................................... 8
  8.3.4 Nuclear weapons ......................................................................................................................... 8

8.5 Weapons used in Piracy ............................................................................................................... 9
  8.5.1 AK 47 ........................................................................................................................................... 9
  8.5.2 Rocket Propelled Grenades ......................................................................................................... 9
  8.5.3 Somali Pirates ............................................................................................................................. 10
8.1 Overview

This chapter looks at the weapons, dangerous substances and devices used by terrorists and pirates. It is important to have a basic general knowledge of these basic types of threats and the damage they can cause. This chapter discusses weapons used in typical terrorist attacks such as explosives (particularly IEDs) and weapons of mass destruction (chemical, biological, radiological and nuclear). Typical weapons used in pirate attacks are also discussed.

8.2 Weapons used in terrorist attacks

8.2.1 IEDs and explosives

Bombings are by far the most popular method used by terrorists to carry out attacks. Commercial explosives such as TNT and military explosives such as C-4 have become much more accessible to terrorist organisations in recent years.

8.2.2 Improvised Explosive Devices (IEDs)

IED stands for improvised explosive device and these are essentially home-made bombs which can be made from a range of commercial, military and home-made materials. Alarmingly, they can even be made from weapons of mass destruction (WOMD).

IEDs come in a range of sizes, delivery methods and configurations which make them ideal for terrorist operations. Basic step by step instructions for home-made explosives can be found on the internet that use readily accessible chemicals found in the home or on farms. IEDs can be manufactured by amateurs with limited training.
8.2.3 IED components

Basic IEDs have four main components:

- a power supply,
- an initiator,
- the explosive and
- a switch.

The explosive component can be either classified either primary, secondary or tertiary. A primary explosive is comparatively unstable and detonates easily, for example after a decent bump. C4 and TNT are examples of secondary explosives. They usually require an initiator for detonation. A tertiary explosive requires an explosion in order to detonate. For example, the tertiary explosive ammonium nitrate which is used in a fertiliser bomb could be detonated using a secondary explosive such as C4. Some IEDs contain ballistics such as metal screws or ball bearings for maximum impact.

The initiator can take many forms. It may be a sparking device, a commercial/ military grade blasting cap or even a secondary explosive if the IED is a tertiary explosive.

An IED switch to activate the initiator can take many forms. They could be wireless such a mobile phone or walkie talkie or they could be wired such as trip-wires, infrared wires or timers.

The power supply for an IED is most commonly a battery which powers the initiator and sometimes the switch. IEDs don’t need a power supply if the initiator is mechanically triggered.

Bomb squads are specially trained to disarm IEDs and often use robots and bomb suits for added safety. They should be notified on finding a suspicious looking item.
8.2.3.1 Methods of IED delivery
There are three main methods of delivery:

- A containment device (such as a pipe bomb or modifying unexploded ordinance)
- A vehicle to deliver the explosive such as a car bomb or the fast moving water craft that hit the USS Cole
- Personal transportation of explosives such as suicide bombers

The most likely explosive threat to the maritime industry comes from vehicle delivery such as in the case of the USS Cole. However, there are other significant threats such as a suicide bomber detonating a bomb on a passenger ferry or the mining of restricted waterways or ports. An example of this latter type of threat occurred in 1980 when a mentally unstable scuba diver reported to US authorities that he had mined the Sacramento River. This cost the transport industry hundreds of thousands of dollars while they dispatched a minesweeper to clear the channel for commercial operations. This demonstrates the damage that just threatening to lay an explosive can cause. IEDs or mines could be placed by swimmers under bridges or onto the hulls of ships or infrastructure in ports and detonated remotely.
8.2.3.2 IED impacts

Explosives are the primary method used by terrorists because of the impacts they can cause when weighed up against the comparatively low cost and limited amount of knowledge required to assemble an IED.

Loss of life, serious injury and damage to infrastructure are the primary impacts. 17 sailors lost their lives on the USS Cole and countless more soldiers and civilians have died in Afghanistan where IEDs are commonly used. Financial costs can be considerable, obviously from direct damage to ships, ports and infrastructure and the cost of emergency services. There is a considerable secondary financial effect on trade if the port or shipping route has to be closed or if a shipping line or port gains a reputation as a terrorist target, such as with the port of Yemen after the Limburg incident.

This table below is from the American Bureau of Alcohol, Tobacco Firearms and Explosives and was developed by a working group of the National Security Council Interagency Working group on counter terrorism in conjunction with US Army engineers. It gives an indication of the minimum evacuation distances for explosives stored in vehicles. The minimum evacuation distance is the range at which a life threatening injury from the explosion or blast is unlikely even though non-life threatening injury and hearing loss may occur. The reason for including this table is to demonstrate the range of a vehicle explosive threat if it were to enter a port facility.
IEDs come in all shapes and sizes and can be disguised to look like any number of objects, for example a Pepsi can. The best way to recognise an IED planted on the ship or port is to know the ship or area you are working and always be on the lookout for things that are strange or suspicious such as a briefcase or bag that does not appear to have an owner. If you find a suspicious object, don’t touch it and you must notify the correct security personnel. They will take the appropriate action as specified in their security plans. Let them know the size, location and description of the object and never take action to deal with the device (such as open a suspicious briefcase).
8.3 Weapons of mass destruction

The use of weapons of mass destruction by terrorists is a serious concern. They can be either:

- Chemical
- Biological
- Radiological or
- Nuclear

Materials for chemical and biological weapons are readily available at facilities such as research and medical laboratories or on the black market. Small amounts of the weapon can wreak havoc in an enclosed space and the level of knowledge needed to manufacture a chemical or biological weapon is only that of a university science student.

8.3.1 Chemical weapons

Chemical weapons can be manufactured using easily acquired base toxins. Terrorists can also acquire military-grade chemical weapons such as nerve agents (Sarin and VX) or blister agents (Mustard or Lewisite). Once released the chemicals are ingested or absorbed through the eyes, respiratory tract or skin. The most common delivery methods are using artillery shells, aerial or vehicle-based spray tanks and bombs. In 1995 the Japanese subway system came under five co-ordinated attacks using Sarin. The Japan-based Aum Shinrikyo group released the Sarin, killing approximately 12 people and injuring thousands.

8.3.2 Biological weapons

Biological weapons require a small amount to infect a large population and involve the use of a biological agent to intentionally cause disease or harm humans, crops or animals. The agent can be a living micro organism (such as bacteria, viruses, fungi or genetically altered micro organisms) or non-living organisms such as toxins and bioactive chemicals derived from organisms. Examples of biological weapons include:

Viruses:

- Small pox
- Ebola

Toxins:

- Botulinum toxin
- Aflatoxin
- Ricin
Bacteria:

- Anthrax
- Cholera
- Salmonella

Terrorists have commonly chosen to use anthrax, smallpox and Ricin because they are relatively easy to obtain, have a reasonable cost and information about the technology is available on the internet. In the case of Anthrax, over 1 million infectious doses can be extracted from a few milligrams of spores. Anthrax was used in a series of mail attacks against the United States in 2001 where 22 cases were reported and 5 fatalities.

Anthrax comes in the form of a slightly off white powder or it could also be in liquid form.

### 8.3.3 Radiological weapons

The most common form of radiological weapons are known as radiological dispersal devices or RRDs and have the nickname ‘dirty bomb’. RRDs use explosives near radioactive material to disperse the material. It is not a nuclear weapon as the radioactive material does not enhance the explosive capability. Its use as a terrorist weapon stems from the intimidation and fear (and consequent economic disruption) this type of weapon can cause. Main sea ports are among the list of likely targets because of their relationship with high volumes of commercial trade and proximity to population.

### 8.3.4 Nuclear weapons

A sophisticated terrorist group could be capable of designing and building a workable nuclear bomb from stolen plutonium or enriched uranium. A famous terrorist nuclear weapon is the “suitcase bomb”. While it has been reported that Al Qaeda have tried to acquire enriched uranium and plutonium, limited evidence suggests they have been unsuccessful.
8.4 Weapons used in Piracy

8.4.1 AK 47

Small arms and infantry weapons are widely used by terrorist groups and pirates around the world. Automatic rifles and machine guns (such as the AK-47) are readily available to terrorists on the black market.

8.4.2 Rocket Propelled Grenades

Rocket Propelled Grenades (RPGs) are another weapon used by pirates to intimidate the ship’s crew and gain access to board.
8.4.3 Somali Pirates

A senior maritime security analyst from the Algiers-based African Centre for the Study and Research on Terrorism was reported in April 2012 as saying that Somali pirates have access to sophisticated weapons that include mines and shoulder held missile launchers (like the Stinger). These weapons were being sold on the Libyan black market. She speculated the weapons could be used in bolder attacks on shipping even though at the time of writing no reports had been received of the use of weapons more advanced than the AK47 and RPGs.
Chapter 9 - Handling Security-related information and communications

9.1 Overview ........................................................................................................................................ 2
9.2 Responsibilities communicating security-related information ......................................................... 2
  9.2.1 Communicating changes in maritime security levels................................................................. 2
  9.2.2 Reporting of maritime security incidents and events .............................................................. 2
9.3 Security Plans .................................................................................................................................. 2
  9.3.1 Control of information contained in a Security Plan................................................................. 2
  9.3.2 Ships Security Communications ............................................................................................. 2
9.4 Handling security-related information .............................................................................................. 3
  9.4.1 Personal Responsibility ........................................................................................................... 3
  9.4.2 Need to know basis .................................................................................................................. 3
  9.4.3 Sensitive Information .............................................................................................................. 3
    9.4.3.1 Storage .......................................................................................................................... 3
    9.4.3.2 Transfer: ........................................................................................................................ 3
    9.4.3.4 Clear office policy: ......................................................................................................... 4
    9.4.3.5 Security and social media: .............................................................................................. 4
9.5 Mariner risk information .................................................................................................................. 4
9.1 Overview

The ISPS code and MTOFS act broadly outline the responsibilities of contracting Governments and maritime industry participants to communicate security related information such as changes in threat levels. Security plans also specify how security information will be communicated, received from other sources, distributed and recorded.

9.2 Responsibilities communicating security-related information

Chapter 4 outlines the responsibilities of contracting governments, ships and companies with regard to communicating maritime security levels and ensuring security-related information is readily available. Chapter 4 also outlines the need for good communication between CSO, SSOs and PFSOs and that they should liaise at the earliest opportunity when a ship is intending to visit to establish security levels and any additional information that may be relevant.

9.2.1 Communicating changes in maritime security levels

Chapter 4 section 4.2 deals with this in detail.

9.2.2 Reporting of maritime security incidents and events

Chapter 5 deals with this in detail.

9.3 Security Plans

9.3.1 Control of information contained in a Security Plan

The distribution of a security plan must be controlled so that it is restricted to personnel that have a ‘need to know’ for purposes of implementing or assessing the security plan for the ship or port ship. The requirement to protect this and other security sensitive information must be covered in security training sessions provided for company personnel. Also, all copies of the security plan should be marked as specified by the company security program. All electronic transmissions of the plan or information contained within the plan should include a warning that the information is sensitive and must be protected.

9.3.2 Ships’ Security Communications

Ships’ security plans outline the methods of communications to be used to when dealing with a security incident or event such as:

- An effective 2 way communication system between the company and ship so as a ship can report an unlawful act direct to the company
• Primary means of communication during an incident – e.g. vhf radio channel X and ship’s intercom as a backup
• Methods for intership, ship to ship, ship to port communications
• Procedure for communicating that the ship is under duress/distress
• Communications with port facility personnel
• Preferred method of communication between the CSO and the SSO

9.4 Handling security-related information

9.4.1 Personal Responsibility

Certain information and communications are considered security sensitive and this level of sensitivity may change as security levels change. All personnel onboard a ship need to appreciate the risk of security leaks through communication by improper methods or to the wrong persons.

Information security is an important consideration onboard any security regulated ship or for any security regulated port. There are several types of information that may be deemed sensitive and as a result must be dealt with by following appropriate procedures.

The handling of important security related information is addressed in the ships’ security plan or maritime security plan (for ports).

9.4.2 Need to know basis

‘Need to know’ is a fundamental concept in information security. If a colleague requests to know sensitive information which is under your care, ensure you know why they want to know it (establish their need to know the information). If a request for access seems unusual, report it to the relevant security officer.

9.4.3 Sensitive Information

Sensitive information will commonly carry a classification - the higher the classification, the more diligent and secure a person will need to be with the information. It is important to familiarise yourself with a ships’ process for dealing with classified information including storing, transferring and disposing of the information. It is essential that individuals follow these procedures when accessing sensitive material. Never discuss sensitive ships security information in a public or non secure environment. Always be mindful who is in earshot. It is important to follow procedures relating to the storage, transfer and disposal of sensitive information.

9.4.3.1 Storage: Identify if the area where the material is to be stored is secure and whether the storage method is appropriate e.g., locked cabinets or safe.

9.4.3.2 Transfer: Transferring information from one place to another often requires specific procedures. Security measures may include using safe hand couriers and having a document control register. If unsure about storing or transferring material that could be sensitive, ask the security officer who will be able to advise you of any specific arrangements you need to take.
9.4.3.3 Disposal: It is important to appropriately dispose of important security-related information. Methods include shredding and placing it into a classified waste bag for disposal.

9.4.3.4 Clear office policy: If you are working on security sensitive material on a ship, port or offshore facility, there may be other personnel who access your working area. It is always a good habit to ensure that security classified information and other valuable resources are secured appropriately when absent from the work place. If working on communal computers, log off where possible.

9.4.3.5 Security and social media: When working for a company, always be careful what information you post on social media like Facebook such as the time and date your ship will arrive at your next destination or photos of restricted areas. When joining a company or ship, always check their privacy policy or if in doubt, check with the security officer.

9.5 Mariner risk information

It is important for key security personnel to keep abreast of the changing security landscape. Sources of information include:

- Maritime Context Statement from the Department of Transport and Infrastructure
- Direct liaison with the Officer of Transport Security
- IMO circulars and updates
- International threat warnings from sites such as International Maritime Bureau (IMB) weekly, quarterly and annual piracy reports
Chapter 10: Security Reporting Procedures

10.1 Introduction............................................................................................................................... 2
10.2 The difference between security incidents and security events .............................................. 2
  10.2.1 Definition of a security incident ............................................................................................ 2
  10.2.2 Definition of a security event ................................................................................................ 2
10.3 Persons responsible for reporting maritime security incidents and events .............................. 3
10.4 Record keeping on Regulated Australian Ships ....................................................................... 3
10.5 Reporting of maritime security incidents and events............................................................... 4
  10.5.1 Maritime Security Incidents .................................................................................................. 4
    10.5.1.1 Reporting to the Transport Security Coordination Centre .................................................. 4
    10.5.1.2 Maritime Incident Report Form .......................................................................................... 5
  10.5.2 Reporting of maritime security events .................................................................................. 7
    10.5.1.3 Maritime security event grades ....................................................................................... 7
      Grade 1 events ............................................................................................................................ 8
      Grade 2 ....................................................................................................................................... 8
10.6 Handy References ..................................................................................................................... 9
10.7 Event grade examples............................................................................................................... 9
10.1 Introduction

It is important to ensure that all maritime transport or offshore facility security incidents and events are reported correctly for the security of maritime transport and offshore facilities. The more complete the information the Department receives, the more detailed analysis can be conducted and therefore the more comprehensive the advice that can be provided to industry.

This chapter:

- outlines the difference between a maritime security incident and a maritime security event
- identifies the correct reporting procedure for both
- identifies who is responsible for the reporting and to whom they must report
- gives an overview of the security incident form
- discusses security records to be kept on a regulated Australian Ship and
- identifies handy references

10.2 The difference between security incidents and security events

10.2.1 Definition of a security incident

As defined by section 170 of the MTOFSA, a maritime transport or offshore facility security incident may be an actual unlawful interference with maritime transport or the threat of unlawful interference with maritime transport which is, or is likely to be, a terrorist act.

The Act (section 11) defines unlawful interference with maritime transport or offshore facilities as any act of taking control, damaging or putting safety at risk involving a ship, offshore facility or port.

10.2.1.2 Definition of a security event

A “maritime security event” is a threatened or actual interference with maritime transport. It is an occurrence (or occurrences), which threatens the security of the maritime industry participant’s facility and/or operations AND is not a “maritime transport or offshore facility security incident”.

In short, a maritime security event is not considered likely to be a terrorist act. Reporting maritime incidents and events contributes to the information that the Department collects and uses to develop a national picture and contribute to the maritime risk context. This data enables the Department to identify and analyse trends and policy gaps and provide information that can assist industry to focus security planning centred on identified risks and vulnerabilities.
10.3 Persons responsible for reporting maritime security incidents and events

The Act requires the following people to report maritime transport or offshore facility security incidents to the police, the Department and other affected parties:

- port operators
- ship masters
- ship operators
- port facility operators
- offshore facility operators
- maritime security inspectors
- duly authorised officers
- maritime security guards
- screening officers
- other maritime industry participants e.g. port service providers and employees of a maritime industry participant

Part 9 of the Act requires these people to report a maritime transport or offshore facility security incident as soon as possible after they become aware of it. It is an offence under the Act if a responsible person becomes aware of a security incident and fails to report it as soon as possible.

10.4 Record keeping on Regulated Australian Ships

MTOFS regulation 1.55 stipulates the security records that must be kept on an Australian Registered Ship. All records must be kept aboard the vessel for 7 years and the following must be recorded:

- security threats and maritime transport or offshore facility security incidents
- breaches of security
- changes to security levels and communications relating to the direct security of the ship (such as specific threats to the ship or to port or offshore facilities used in connection with the loading or unloading of the ship)
10.5 Reporting of maritime security incidents and events

10.5.1 Maritime Security Incidents

Reporting of Incidents is compulsory and if in doubt whether to report the incident, it is always best to err on the side of caution and report it.

The first step is to contact the police or other emergency services as soon as the incident is identified. This is a priority.

The second step is to notify the secretary of the Department and other affected MIPs of the incident either orally or in writing as soon as it is appropriate to do so without hindering the response from emergency services or police.

The third step is to provide a written report to the Department which is a requirement under Part 9 of the Act and the report must include the following information:

- the maritime industry participant to whom the report relates;
- the date and time of the incident;
- the location of the incident;
- if the incident involved a ship, information regarding the ship including (if known): name, type, size, flag, IMO number, ISSC number, and type of cargo;
- if the incident involved a building or offshore facility or other infrastructure, information sufficient to identify the building or offshore facility or other infrastructure, such as the building number or other identifier;
- the nature of the incident;
- if the incident involved any other maritime industry participants, details of the other maritime industry participant(s) involved;
- a description of the incident;
- if the report is being made on behalf of (including as a result of being notified by) another person or organisation, the name of the person on whose behalf the report is being made;
- if the person reporting the incident is aware that the incident has previously been reported to the Department, the approximate time at which the incident was reported.
- an indication of whether the person reporting the maritime transport or offshore facility security incident is aware that the incident has been reported to the Police and other maritime or offshore industry participants involved;
- the name of the person reporting the incident;
- the title or position of the person reporting the incident;
- the name of the employer of the person reporting the incident, where applicable; and
- the date of the report.

10.5.1.1 Reporting to the Transport Security Coordination Centre

When a security incident occurs, the MIP or person with incident reporting responsibilities must report the incident to the Department’s Transport Security Coordination Centre (TSCC)
Reports made in accordance with this notice should be directed to the Department’s Transport Security Co-ordination Centre using one of the following means of communication:

Facsimile: +61 2 6274 6089
E-mail: transport.security@infrastructure.gov.au
Mail: GPO Box 594
CANBERRA ACT 2601
AUSTRALIA

For general or related enquiries, the Department’s Transport Security Co-ordination Centre can be contacted by telephone on 1300 307 288 or +61 2 6274 8187 (if phoning from outside Australia).

The table below has been taken from the OTS document, “Guidance for reporting of security incidents and events by maritime industry participants” and summarises the process for reporting a maritime security incident:

### 10.5.1.2 Maritime Incident Report Form

The TSCC has released an electronic incident reporting form which is available at this address:


There is the option to either complete the online form or download the word version and email/fax/send.
MARITIME SECURITY INCIDENT REPORT FORM

NOTE: This form should be forwarded to:
Transport Security Coordination Centre
Tel: 1300 307 263  From outside Australia: +61 2 6274 8187
Fax: +61 2 6274 0089
E-mail: transport.security@infrastructure.gov.au

A completed report submitted to the Department using this form will fulfill incident reporting obligations under Part 9 of the Maritime Transport and Offshore Facilities Security Act 2003 (MTOSA).

This form may be used to assist in making reports to police and other Maritime or Offshore Industry Participants (MIPs/OIPs). An incident under Part 9 of the MTOSA must be reported in writing to the Department as soon as possible. The Department should be notified within 4 hours of the MIP becoming aware of the incident, and the written report should be provided within 72 hours.

Use Tab Key to move from cell to cell or double click “Type Here” fields. Click boxes to check them.

<table>
<thead>
<tr>
<th>PART 1 - Type of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maritime Transport or Offshore Facility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 2 - Incident Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIP/OIP Type</td>
</tr>
<tr>
<td>Location of Incident</td>
</tr>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Time</td>
</tr>
<tr>
<td>MIP type (please specify):</td>
</tr>
<tr>
<td>Ship operator</td>
</tr>
<tr>
<td>Nature of Incident:</td>
</tr>
<tr>
<td>Threat</td>
</tr>
<tr>
<td>Hijack</td>
</tr>
<tr>
<td>MSIG or other ID</td>
</tr>
<tr>
<td>Failure of a screening point</td>
</tr>
<tr>
<td>Unauthorized weapons/ prohibited items</td>
</tr>
<tr>
<td>Unauthorized disclosure of a security plan</td>
</tr>
<tr>
<td>Other, please specify:</td>
</tr>
</tbody>
</table>

If applicable, provide name of person/organisation who notified you of this incident. Type Here

<table>
<thead>
<tr>
<th>PART 3 - Ship Details (if applicable and known)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship name</td>
</tr>
<tr>
<td>IMO</td>
</tr>
<tr>
<td>Iss No.</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Size</td>
</tr>
<tr>
<td>Type of Cargo</td>
</tr>
</tbody>
</table>

Purpose of submitting Form? | Notification | Report |

<table>
<thead>
<tr>
<th>PART 4 - Building/Structure Identifier (if applicable and known)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type Here (Insert building number or other identifier)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 5 - Incident Narrative and response taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type Here (Insert building number or other identifier)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 6 - Other MIPs/OIPs Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type Here</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 7 - Has the incident been previously reported to the Department’s Transport Security Coordination Centre (TSSC)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 8 - If applicable, has the incident been reported to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>State/Territory Police?</td>
</tr>
<tr>
<td>Affected MIP/OIPs identified in Part 6 above?</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 9 - Details of person completing report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Position</td>
</tr>
<tr>
<td>Employer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 10 - Other Relevant Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type Here (attach additional pages if necessary)</td>
</tr>
</tbody>
</table>

Time Saver (Time taken to complete form): 00 hr 00 min

Date of Report: dd/MM/yyyy
10.5.2 Reporting of maritime security events

The Government strongly encourages the reporting of security events which are not “maritime transport or offshore facility security incidents” as defined under section 170 of the Act. Having information on maritime security events will allow the Department to:

- develop a trend analysis of events across Australia’s maritime sector
- analyse, assess and advise on the adequacy of a MIP’s security plan and
- provide analysis reports to maritime industry participants to assist in reviews of their security plans and measures

The Officer of Transport Security has published an industry code of practice for the reporting of Maritime Security Events. Even though the code is not binding, the Department recommends that MIPs comply with the reporting procedures in this code. It should be noted that if MIPs choose to voluntarily adopt reporting of Maritime Security events and reflect this in their Security Plans, they are then obliged by the Act to report security events as they have specified. This is because there is a legal obligation for MIPs to comply with the measures they stipulated in their security plans and penalties apply for non-compliance.

As defined by the industry code of practice, a reportable maritime security event may include, but is not limited to:

- unauthorised or attempted unauthorised access to a maritime, ship or offshore security zone
- any breach of a screening point that is likely to, or results in persons, vehicles or vessels gaining unauthorised access into a maritime security zone. (This does not include the successful detection of weapons or prohibited items at a screening point)
- inappropriate use of a maritime security identity card to gain, or attempt to gain, access to a maritime, ship or offshore security zone
- damage to security equipment through sabotage or vandalism
- unauthorised disclosure of a maritime or ship or offshore security plan
- unauthorised or attempted unauthorised carriage of weapons or prohibited items in a maritime, ship or offshore security zone
- suspicious behaviour by persons in or near a regulated entity
- unexplained or suspicious cargo, goods or luggage in, or in the vicinity of, a maritime, ship or offshore security zone
- unsecured access points
- maritime security events during, or after, which the media was present or inquiries by the media were known to have been made and
- conduct by a person or persons which would, or is likely to, hinder or obstruct the implementation of a maritime industry participant’s security plan

10.5.1.3 Maritime security event grades

As maritime security events can vary markedly in their seriousness and impact, the Department has recommended three separate grades of maritime security events to assist in the reporting of them.
They emphasise that these grades are a guide only as the maritime environment is extremely complex and recommend the reporting of all maritime security events as promptly as possible.

**Grade 1 events** are those events that are routine in nature and have been readily resolved (i.e. cause of security threat or breach has been identified and addressed by maritime industry participant). Routine or no follow-up action would normally be involved in such events.

**Grade 2 events** are those events where the awareness and the assistance of the Department in a guidance and/or compliance capacity is desirable. Grade 2 events include unresolved events where the maritime industry participant is unable to establish or identify:

- the cause of the security threat or breach and/or
- any action taken to remedy the security threat or breach

**Grade 3 events** are those events where the immediate awareness and possible intervention by the Department is desirable.

6.4 In relation to Grade 2 and 3 events it may also be wise for maritime and/or offshore industry be made aware of them, either generally or for specific maritime industry participants (as the case requires).

| Table 1: Standards of practice for reporting maritime security events |
|-----------------------------------------------|------------------|------------------|
| **Maritime Security Event – Grade 1**         | **Suggested timing** | **Suggested details to be included** |
| Events which seem to require either routine or no follow-up action. | Monthly reporting – events submitted to the Department within 14 days after the end of each month. | (a) The MIP to whom the report relates. |
| Events that have been reported previously by the maritime industry participant would not normally be repeated in such monthly reporting. | | (b) The date and time of the event. |
| | | (c) The location of the event. |
| | | (d) If the event involved a ship, information regarding the ship including (if known): name, type, size, flag, IMO number, ISCC number, and type of cargo. |
| | | (e) If the event involved a building or other infrastructure, information sufficient to identify the building or other infrastructure, such as the building number, or other identifier. |
| | | (f) The nature of the event. |
| | | (g) If the event involved any other MIPs, details of the other MIP(s) involved. |
| | | (h) A description of the event. |
| | | (i) If the report is being made on behalf of (including as a result of being notified by) another person or organisation, the name of the person on whose behalf the report is being made. |
| | | (j) If the person reporting the event is aware that the event has previously been reported to the Department, the approximate time at which the event was reported. |
| | | (k) An indication of whether the person reporting the event is aware of the event previously reported to the Police and other MIP(s) involved as identified in (g). |
| | | (l) The name of the person reporting the event. |
| | | (m) The title or position of the person reporting the event. |
| | | (n) The name of the employer of the person reporting the event, where applicable. |
| | | (o) The date of the report. |

| Maritime Security Event – Grade 2 | As soon as possible. * Ideally, this means: Notify within 24 hours. | Submit oral or written report within 72 hours. |
| Maritime Security Event – Grade 3 | As soon as possible. * Ideally, this means: Notify within 4 hours. | Submit written report with required information within 72 hours. |
| Maritime Transport or Offshore Facility Security Incident | As soon as possible. * Ideally, this means: Notify within 4 hours. | Submit written report with required information within 72 hours. |
10.6 Handy References

- MTOFSA Part 9

10.7 Event grade examples

The following event grade examples are taken from the Office of Transport Security’s Guidance Paper for Reporting of Security Incidents and Events.

APPENDIX C: EVENT GRADES AND EXAMPLES

<table>
<thead>
<tr>
<th>GRADE</th>
<th>EXAMPLE</th>
</tr>
</thead>
</table>
| GRADE 1 | 1. Extract of Email - 0700 - advised via phone - Breach in security at Outer Harbour. 0800 - PFSO - attended site investigated hole cut in fence. 0812 - Signal tower advised assistance in temporary fence repairs obtained. 0815 - requested to notify local authorities 0900 - Manager advised ****End of Extract***
| | 2. Extract of Email - Report to port Security Control Centre, small fishing vessel under wharf with 3 persons on board. Port Security advised vessel of correct distance allowed in area around wharf and vessel moved away without incident. Boat Rego: xxxxx ****End Extract ** Please Note this vessel was also cautioned on the 26 July for similar incident.
| | 3. A suspicious person walked straight inside the terminal through the gate and started taking photos of the terminal (apparently of the containers and may be the straddle carriers). Security Officer immediately approached the person and warned him not to take any photographs and that he is in a Land Side Restricted Zone, without any authorisation. The person complied immediately and went to his car (parked across the road) to get his ID, to which the Security Officer accompanied him to his car. Person's Details as follows: XX (International Driver's Licence), DOB xx/xx/xxxx. |
### GRADE 2

1. **Extract of Email:** While reviewing CCTV footage it was noticed that the camera dome appeared to have been partly covered with a white gum-like substance. The area covered by the gum blocked out vision of the employee car park and rear entry gate. Chewing gum was removed and camera vision restored. The gum had been placed perfectly on the camera dome to completely block the footage of the small craft pens office, amenities entrance and car park area and had been in place for some time. Incident is being investigated further. Incident is considered serious and being investigated internally.

   ****End of Extract***

2. **At 1338, Opscen received a call from Duty Marine Controller. A Zodiac (registration xxx- named "XXX") was observed in the Shipping Channel, engaged in picking up and dropping off two divers. Security Officer contacted the Water Police, but they could not assist as they had no vessels in the vicinity.**

### GRADE 3

1. **Extract from Email:** At approx 1600hrs, a staff member of Shipping Company X observed what he believed to be a diver, who surfaced in the water immediately behind the stern of vessel XXX which was berthed at the Port X. Cruise ship xx is berthed on the opposite side of the pier. At 1605, Port Facility Security Officer (PFSO) was informed of the incident and he in turn notified the Ship’s security officer, who initiated first call to water police. At 1630 to 1650hrs water police attended scene of event and initiated surface search of immediate area with snorkel divers with no results. At 1705hrs, water police made decision to evacuate vessel xxx and Cruise Ship xx (completed by 1830). Pier and Terminal area was searched and hull of vessels xxx was examined. Vessel xxx was searched by divers from the Police and finally cleared at 8.30pm. The passengers were then loaded onto the Cruise Ship xx, which departed at 1045pm, nearly three hours late. Investigations have since failed to identify the diver involved ****End of Extract.

2. **0900 Port Facility Security Officer (PFSO) from xx Port called the Transport Security Coordination Centre to advise that a break and enter had been investigated at the Port. According to the PFSO at 0700 the security guard from xx Port had noticed a cut in the perimeter fence. The security guard then identified two suspicious people driving slowly past the xx Port entrance. The security guard noted the licence plate of the vehicle. Further investigation by the security guard found that the CCTV at the xx Port had been disabled and damaged, and a suspicious item was found within the vicinity of regulated vessel xx. At 0730 the police were contacted. The Police arrived and identified the suspicious item as a suspected bomb. The area was cordoned off and the bomb squad called at 0815.**

3. **Transport Security Coordination Centre advised by Ship Security Officer that at 1345 a crew member had found 5 unauthorised persons in the engine room of an Australian regulated ship in Port xx. When spotted the persons overpowered the crew member and disappeared. The crew member was injured in the scuffle. The SSO notified port security at 1420, who immediately notified the Police. The Police boarded the ship at 1445 and searched vessel xx. The 5 unauthorised persons in question were found hidden in the sleeping quarters of vessel xx. They were detained and escorted off vessel xx for further questioning. The injured crew member was taken to hospital at 1525. Vessel xx was cleared at 1700 to continue voyage.**
Chapter 11: Maritime Security Training, Drills and Exercises

11.1 Training of key security personnel and other personnel on ships and in ports

11.1.1 IMO Model security courses

11.1.2 Port Security Officer

11.1.3 Port facility personnel that have specific security duties

11.1.4 All other Port Facility personnel

11.1.5 Company Security Officer & Ship Security Officer

11.1.6 Shipboard personnel with specific security duties

11.1.7 Shipboard personnel without security responsibilities

11.2 Drills and Exercises

11.2.1 Overview

11.2.1.1 Full-scale exercises

11.2.1.2 Table-top exercises

11.2.2 Maritime Security drills and exercises in a Port Facility

11.2.3 Maritime Security drills and exercises on ships
11.1 Training of key security personnel and other personnel on ships and in ports.

It is important that all personnel who are assigned to key security positions have appropriate training, skills and knowledge to carry out their role. It is just as important that all maritime industry participants have a basic knowledge of maritime security concepts. The ISPS code and the MTOSFS Act describe the areas of training that personnel such as Ships’ Security Officers, Company Security Officers and Port Security Officers must receive.

This section describes IMO model security courses before outlining the relevant training and knowledge required by:

- Port facility security officers
- Port facility personnel that hold specific security duties
- Port facility personnel that do not hold specific security duties
- Company security officers
- Ships’ security officers
- Ships’ personnel with specific security duties
- Ships’ personnel that do not hold specific security duties.

11.1.1 IMO Model security courses

Specific security courses are available for SSOs CSOs and PFSOs. Before enrolling with a training provider, it is useful to check that the course is based on the model course prepared by the International Maritime Organisation and is approved by AMSA for Australian courses (or approved by the national designated authority for maritime security / maritime administration if completing the course overseas). Model courses developed by the IMO are designed to help implement the SOLAS convention and ISPS code consistently by all member countries. IMO model courses provide the following:

- a course framework detailing the scope, objective, entry standards and other information about the course
- a course outline (timetable)
- a detailed teaching syllabus (including the learning objectives that should have been achieved when the course has been completed by students)
- guidance notes for the instructor and
- a summary of how students should be evaluated

11.1.2 Port Security Officer

The ISPS code lists the main areas for which Port Security Officers should have knowledge and receive training. These are:

- security administration
- relevant international conventions, codes and recommendations
• relevant Government legislation and regulations
• responsibilities and functions of other security organizations
• methodology of port facility security assessment
• methods of ship and port facility security surveys and inspections
• ship and port operations and conditions
• ship and port facility security measures
• emergency preparedness and response and contingency planning
• instruction techniques for security training and education, including security measures and procedures
• handling sensitive security related information and security related communications
• knowledge of current security threats and patterns
• recognition and detection of weapons, dangerous substances and devices
• recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security
• techniques used to circumvent security measures
• security equipment and systems, and their operational limitations
• methods of conducting audits, inspection, control and monitoring
• methods of physical searches and non-intrusive inspections
• security drills and exercises, including drills and exercises with ships
• assessment of security drills and exercises

In Australia, the Act requires that maritime security plans set out the knowledge and skills required by the PSO. The maritime security plan must then detail the training and qualifications that satisfy these requirements and any additional training that the PSO must receive on taking up the position.

11.1.3 Port facility personnel that have specific security duties

In addition to Port Facility Security Officers, there are personnel who work within the port facility and have security related duties. The ISPS code lists the main areas for which these personnel should have knowledge and receive training.

• knowledge of current security threats and patterns
• recognition and detection of weapons, dangerous substances and devices
• recognition of characteristics and behavioural patterns of persons who are likely to threaten security
• techniques used to circumvent security measures; crowd management and control techniques
• security related communications
• operations of security equipment and systems
• testing, calibration and maintenance of security equipment and systems
• inspection, control, and monitoring techniques and
• methods of physical searches of persons, personal effects, baggage, cargo, and ship’s stores

In Australia, the Act requires that maritime security plans set out the knowledge and skills required by personnel other than the PSO who hold security responsibilities. The maritime security plan must then detail the training and qualifications that satisfy these requirements and any additional training that they must receive on taking up the position.

11.1.4 All other Port Facility personnel

All other port facility personnel who do not have a specific security duty should have knowledge of and be familiar with relevant provisions of their Maritime Security Plan, including:

• the meaning and requirements of different maritime security levels
• how to recognise and detect weapons, dangerous substances and devices
• how to recognise characteristics and behavioural patterns of people who are likely to threaten security and
• techniques used to circumvent security measures

11.1.5 Company Security Officer & Ship Security Officer

The Company Security Officer, appropriate shore based Company personnel and the Ship Security Officer (SSO) should have knowledge of and receive training, in the following, as appropriate:

• security administration
• relevant international conventions, codes and recommendations
• relevant Government legislation and regulations
• responsibilities and functions of other security organizations
• methodology of ship security assessment
• methods of ship security surveys and inspections
• ship and port operations and conditions
• ship and port facility security measures
• emergency preparedness and response and contingency planning
• instruction techniques for security training and education, including security measures and procedures
• handling sensitive security related information and security related communications
• knowledge of current security threats and patterns
• recognition and detection of weapons, dangerous substances and devices
• recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security
• techniques used to circumvent security measures
• security equipment and systems and their operational limitations
• methods of conducting audits, inspection, control and monitoring
• methods of physical searches and non-intrusive inspections
• security drills and exercises, including drills and exercises with port facilities and
• assessment of security drills and exercises

In addition the SSO should have adequate knowledge of and receive training in the following:

• the layout of the ship
• the ship security plan and related procedures (including scenario-based training on how to respond)
• crowd management and control techniques
• operations of security equipment and systems and
• testing, calibration and whilst at sea maintenance of security equipment and systems

In Australia, the Act requires that a Ships’ Security Plan sets out the training that the CSO and SSO must receive.

11.1.6 Shipboard personnel with specific security duties

Personnel working onboard a ship who have been assigned specific shipboard security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

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

In Australia, the Act requires that a Ships’ Security Plan sets out the training that shore-based personnel and ship’s crew with specific security duties must receive.
11.1.7 Shipboard personnel without security responsibilities

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

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

In Australia, the Act requires that a Ships’ Security Plan sets out the training that shore-based personnel and ship’s crew must receive.

11.2 Drills and Exercises

11.2.1 Overview

Drills and exercises are designed to ensure that personnel are proficient in their security duties at all security levels. They also identify areas of weakness within the relevant security/contingency plans. Drills and exercises are an important functional requirement of the ISPS code to ensure familiarity with security plans and procedures. Australian regulated ships and port facilities are required to keep records of all training, drills and exercises conducted.

Drills are conducted regularly and focus on threats identified in the security assessments. They are designed to ensure ship and port personnel are familiar and proficient in their security roles.

Security exercises are more strategic in nature and are scenario based. They should test communications, co-ordination resource availability and response. Exercises are used to identify weaknesses within the security/contingency plans.

Exercises can be:

- Full scale or “live”
- Table top or
- Combined with other exercises held such as search and rescue.
11.2.1 Full-scale exercises

Full-scale or live exercises are designed to test a security/contingency plan as realistically as possible and often involve multiple stakeholders (such as company security officers, ship security officers, port security officers and emergency services). Live exercises are based on a scenario that closely reflects a threat or threats identified in port or ships’ security plan. Live exercises can take months of planning, involve considerable resources and often have “exercise players” who are asked to role play and bring the scenario to life. Live exercises are the most realistic way of testing a security/contingency plan.

11.2.1.2 Table-top exercises

A table top exercise is a facilitated, scenario-based group discussion involving key players. Table top exercises are effective if time and money is limited or key personnel are new to their roles. They can allow the testing of a security/contingency plan in a controlled and safe environment within a short timeframe. A scenario is chosen based on the hazards or security incidents or threats likely to occur. Table top exercises:

- Clarify the roles and responsibilities of key security players such as PFSO, CSO, SSO
- Evaluate port and ship contingency plans
- Develop teamwork before an actual crisis
- Help to assess resources and capabilities
- Identify shortcomings and solutions

11.2.2 Maritime Security drills and exercises in a Port Facility

According to the ISPS code, drills must be conducted every 3 months. Drills should test individual elements of the Maritime Security Plan and should respond to threats identified in the security assessment. These threats may include:
- damage to, or destruction of, the port facility or of the ship, 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 their equipment
- use of the ship itself as a weapon or as a means to cause damage or destruction
- blockage; of port entrances, locks, approaches etc. and
- nuclear, biological and chemical attack

Exercises should be conducted once per calendar year with no more than 18 months in between exercises.

11.2.3 Maritime Security drills and exercises on ships

According to the ISPS code, drills must be conducted every 3 months and also when more than 25% of the crew have been changed at any one time and have not participated in a drill within the past 3 months. Exercises should be conducted once per calendar year with no more than 18 months in between exercises.