



# **GUIDANCE FOR SHIOWNERS, SHIP OPERATORS AND MASTERS**

## **ON THE PROTECTION OF SHIPS FROM TERRORISM AND SABOTAGE**

*This document has been issued to provide guidance to operators and managers of ships and ships' masters in dealing with security threats to vessels, passengers and crew.*

*It identifies some of the ways in which ships can protect themselves from attacks by terrorists or saboteurs. The guidance is aimed at encouraging companies to lay down their own policy and should not be interpreted as limiting a master's traditional freedom to take any steps necessary to secure the safety or security of his ship. It identifies measures against which a company's own plans can be compared.*

*The guidance is based on advice promulgated by IMO (MSC/Circ.443, MSC/Circ.754) and certain national administrations and offers recommendations to shipping companies on company and ship security planning and the identification of responsibilities of individuals designated under such a plan.*

*The guidance will be kept under review in the light of developments and in consultation with other organisations or national authorities and revised as and when necessary.*

21 November 2001

**International Chamber of Shipping  
12 Carthusian Street  
London EC1M 6EZ**

Telephone +44 20 7417 8844

Fax +44 20 7417 8877

e-mail: [ics@marisec.org](mailto:ics@marisec.org)

**International Chamber of Shipping Ltd. Registered in England No. 2532887 at the above address**

## **CONTENTS**

- 1. INTRODUCTION**
- 2. SHIPPING COMPANY SECURITY POLICY, RESPONSIBILITIES AND ACTIONS**
- 3. THE SHIP OPERATOR'S SECURITY OFFICER**
  - 3.1 Shipping Company Security Surveys**
  - 3.2 Ship Security Surveys**
  - 3.3 Security Staff Training**
  - 3.4 Contingency Planning**
- 4. LEVEL OF THREAT AND THREAT ASSESSMENT**
- 5. THE SHIP SECURITY OFFICER**
  - 5.1 Responsibilities**
  - 5.2 Ship Security Measures and Procedures**
- 6. HIJACKS**
- 7. BOMB THREATS TO SHIPS**
- 8. SEARCH PLANNING AND PRACTICE**
  - 8.1 Search Planning**
  - 8.2 Ship Search Decision**
  - 8.3 The Search System**
- 9. FINDING A SUSPECT DEVICE**
- 10. REPORTS OF UNLAWFUL ACTS**
- 11. SUMMARY GUIDANCE FOR MASTERS**
- 12. CONCLUSION**

## **ANNEXES**

- 1. Security Surveys**
- 2. Security Staff Training**
- 3. Threat Levels and Potential Responses**
- 4. Guidance for Masters in the Event of a Hijack**
- 5. Potential Bomb Threats and Countermeasures**
- 6. Ship Search Planning**
- 7. Search System and Search Methods**

## 1. INTRODUCTION

- 1.1 Terrorists and saboteurs can broadly be grouped under the following headings:
- those whose grievance is essentially territorial, nationalist, separatist, ethnic or religious
  - those whose political ideology is extreme left, right or fundamentalist
  - extremist groups supporting trade protection, animal rights or environmental issues
  - those promoting criminal activities (e.g. drug trafficking or organised illegal immigration).

- 1.2 Terrorist acts may be aimed at :
- attracting publicity, advertising a cause and pressurising Governments to change policy
  - making the public apprehensive
  - discrediting Governments by exposing their inability to protect their citizens
  - provoking repressive counter measures which impinge upon citizens' civil rights such as travel restrictions, curfews or special legislation, thus alienating public opinion
  - extorting money or equipment from Governments, major companies or rich individuals
  - freeing imprisoned colleagues in return for the release of hostages
  - promoting other illegal activity.

- 1.3 Although most of the major terrorist incidents involving transport activities have involved aircraft, there have been incidents on board vessels and there is no doubt that certain categories of ships and shore installations present a theoretically attractive, although often difficult, target for terrorist activities.

- **Cruise Liners** could be targetted because of their high profile, their flag, ownership, particular destination or nationality of their passengers. Cruise passengers may be perceived as a high income group and this alone could make them a target.
- **Tankers**, with the political sensitivity of their cargo and the potential environmental impact and resulting wide publicity given to tanker mishaps, are potentially attractive targets, although their size, complexity and the terminals where they call may make boarding difficult. **Gas tankers**, with their potentially volatile cargoes, might be considered to offer a particularly high profile.
- **RoRo Passenger Ferries** may be vulnerable to the use of a car bomb attack, aimed at damaging, disabling or sinking the vessel, causing fire on board and/or harm to the passengers and the crew.
- **Other Ships with Special Cargoes** such as those transporting hazardous goods, nuclear materials or waste or livestock could be potentially conspicuous targets.
- **Terminals**, such as those handling oil or gas, might present attractive targets to terrorists or saboteurs.

- 1.4 Terrorists and saboteurs will generally carry out a reconnaissance of potential targets for whatever type of operation they are planning. An unprotected target is more likely to be attacked than an obviously protected one and terrorist groups will be deterred by visible security arrangements which are known to be effective. A ship whose crew is obviously vigilant is less likely to be selected as a target for a terrorist attack than one with a crew whose security procedures are neither comprehensive nor diligently enforced. Likewise, a company with efficient cargo acceptance procedures is less likely to attract unwelcome cargoes.

## **2. SHIPPING COMPANY SECURITY POLICY, RESPONSIBILITIES AND ACTIONS**

2.1 Until a company has decided its own responsibility with regard to security, it is difficult to determine the actions which should be taken. Each company needs to develop a statement of its own security policy for its vessels which should incorporate the following primary objective: -

**Safeguarding their crew, passengers, visitors, other employees, ships and cargoes from the activities of terrorist or other criminal organisations.**

2.2 To accomplish this, various steps need to be taken, such as

- to appoint and empower a suitably senior staff member to have overall responsibility for security on board all company controlled ships;
- to assess the security risk, taking account of the type of ship, the type of cargo it carries, the nationality of any passengers, the ports it serves and any other relevant factors;
- to co-operate with the responsible authorities in any country the ship visits and to act on any advice from those authorities;
- to promote security awareness amongst all employees with a view to making acts of terrorism against ships more difficult to achieve;
- to appoint and empower a responsible officer as ship security officer on each ship;
- to provide guidance and advice to masters and crews on responses to terrorist threats and keeping such guidance up to date;
- to recognize that additional security requirements may impose additional burdens on masters and crews which charter parties might need to take into account;
- to establish a reporting and recording system for incidents.

2.3 A company's plans will need to take into account a wide variety of scenarios in the different parts of the world in which they operate. In some potential incidents national governments will plan to take a leading role, in others the company may plan to direct its own negotiations. However, in all cases, the company needs to consider:-

- responsibility for handling the incident
- passing information to authorities, trade associations, other ship owners
- instructions to masters and crew
- liaison with overseas authorities
- methods of communication
- plans for handling the media
- plans for informing and supporting the relatives/next of kin of those involved.

2.4 **Arming crews in reaction to a potential terrorist threat is not recommended.**

### **3. THE SHIP OPERATOR'S SECURITY OFFICER**

IMO recommends that each ship operator should allocate responsibility for the security of the ships of that operator to a particular senior person in the organisation (the operator's security officer) and provide resources to:

- conduct security surveys and subsequent inspections of each ship in the fleet
- develop and maintain company, fleet and individual ships' security and contingency plans and procedures
- encourage security awareness and vigilance amongst crews
- ensure adequate training for personnel responsible for security
- assess the potential threat in ports, terminals and sea areas on ships' voyages
- encourage security awareness in ports and terminals visited by the company's vessels
- co-ordinate company and ships' security plans with port security officers in each port that might be visited by ships of that fleet.

#### **3.1 Shipping Company Security Surveys**

In order to prepare security plans, an initial comprehensive security survey should be undertaken of each ship to assess the vulnerability of the ship to terrorist acts. The results of this security survey should be used to determine the security measures necessary to counter the threat. The level of security deemed necessary for each ship may vary from port to port, from ship to ship and from time to time. Liaison between the port and shipping company/ship security officers is important to ensure the best use of ship and shore resources. The survey should determine what needs to be protected, what security measures are already in effect, and what additional measures and procedures are required. These issues should be periodically reviewed and the security plans updated as necessary.

#### **3.2 Ship Security Surveys**

A ship security survey should consist of a preliminary assessment and an on-site survey. Further details are given in Annex 1.

#### **3.3 Security Staff Training**

A continuous and thorough programme should support measures taken to safeguard the security of passengers and crews. Although all employees, ashore and afloat, have responsibilities for security in one way or another, there are three categories of personnel who may be specifically involved and who may benefit from specialised training:

- The ship operator's security officer and his central support staff
- The ship security officer
- Inspection, control and monitoring personnel.

A more detailed examination of security staff training is outlined in Annex 2.

#### **3.4 Contingency Planning**

An essential part of security is the preparation of contingency plans in response to incidents which could occur and the planning of measures introduced in response to any increase in the level of threat. These plans need to cover different levels of response from the company (operator/owner) and the master, officers and crew. They might also encompass the establishment of a "Threat Level" procedure, identifying various measures which might be adopted by vessels in response to the perceived level of threat to the vessel in a particular place, at a particular time.

#### 4. LEVEL OF THREAT AND THREAT ASSESSMENT

4.1 The security arrangements in place at any particular time or location or for any particular vessel will depend, of course, on the perceived level of threat. In this regard it is useful to consider establishing a series of threat levels against which various actions might be taken, tightening security at each higher level. A universally recognised "threat level" indicator does not exist although a widely used and simple threat level table is as follows:

- **Level 1** - background level of threat;
- **Level 2** - heightened threat due to type of ship, port, current events etc., but with no defined target;
- **Level 3** - high level of threat against a specific target.

4.2 Notification of the appropriate threat level will generally be from national authorities through a shipping company's organisation structure responsible for security (i.e. national authority to ship operator's security officer to ship security officer). In a particular port, notification of the threat level, or a change in it, may come from the national authority, via the port security officer, to the vessel and its person responsible for security. In any event the incremental measures to be taken at each of the threat levels should be laid down. Those outlined in Annex 3 might be considered.

4.3 A threat level system such as this enables actions to be established for various responsible people in the event of a threat level change. A message indicating a move from "level 1 to level 2" will, in the event that such a system is established, immediately indicate the additional actions that people responsible for security, both ashore and at sea, need to take.

4.4 Although individual companies can develop a threat assessment for themselves, it is the responsibility of Governments to study the capabilities and intentions of any terrorist group which may threaten ships visiting, flagged or owned in a country, and to issue, where necessary, assessments of likely threats. It is for the shipping industry to act on such assessments. Specific advice as to what the shipping industry might do in response to any threat might also be obtained from Government departments. All advice must be kept up to date so information needs to pass in both directions. The prompt and continuing dissemination and exchange of information will assist the maintenance of effective port and ship security procedures and will enable states, port facilities, operators and shipmasters to adjust their procedures in response to changing conditions and specific or general threats.

## 5. THE SHIP SECURITY OFFICER

### 5.1 Responsibilities

5.1.1 Although directed at passenger ships, IMO recommends that ship operators appoint an officer (who could be the master) to be responsible for the security of each individual vessel (the ship security officer). This recommendation should be considered in respect of all vessels. The ship security officer has responsibility for:-

- advising the master on the threat assessment for the voyage and agreeing the ship's response
- regular security inspections of the ship
- detailed contingency planning
- implementing/maintaining the ship's security plan designed by the operator's security officer at the appropriate threat level
- proposing modifications to the plan
- encouraging security awareness and vigilance on board the ship
- liaising with port security officers during the ship's visit and with the ship operator
- reporting, as appropriate, all occurrences and suspected occurrences of unlawful acts
- co-ordinating the implementation of the ship security plan with the appropriate port security.

5.1.2 Good security involves a readiness to accept that a threat exists and that arrangements might be necessary to counter it. The ship security officer, together with the master, should consider:-

- **Security education** - all crew members will be more security conscious and vigilant if the principles of good security are explained. It should be clear within each company who has responsibility for company policy in relation to security and each person's role in respect of the vessels.
- **Awareness** - the threat of terrorist attacks in different parts of the world varies depending on the national and international politics of the day and the grievances, real or imagined, of any of the potential groups that might be involved. The threat needs to be assessed in relation to each planned port of call, on the best information available, taking action as necessary.
- **Liaison** - good liaison with local police and port authorities will provide local "intelligence", and may give advance warning of any incident and lead to a more rapid reaction by local security forces. Where such liaison with local police or port authorities is difficult, advice might be sought from local consular or diplomatic representatives.

### 5.2 Ship Security Measures and Procedures

Although the master's traditional authority in matters of ship security remains paramount, ship security should be continually monitored and supervised by the ship security officer. It is also important to establish and maintain communication and co-operation with individual port facilities in security matters. Additional security measures, such as those suggested in Annex 3, should be implemented to counter increased risk when warranted.

## 6. HIJACKS

- 6.1 "Hijack" is used to define the forcible seizure of a means of transport by terrorist or criminal groups as a way of furthering their cause, reaching their objective, making good their escape or even using the ship itself, and/or its cargo, as a threat or as a weapon. Aircraft have been hijacked by a single person armed only with imitation weapons and, in the right place, one armed person could be enough on a ship. However, a planned terrorist hijack of a vessel is much more likely to involve a group with real weapons. The major task facing the would-be hijackers is to board the vessel with their weapons, and security measures aimed at preventing this should be introduced when the threat level warrants it. Measures devised in respect of threats from piracy and/or armed robbery are appropriate. The key objective must be to prevent unauthorised access to the vessel.
- 6.2 Although in most parts of the world the threat of this kind of action is low, shipping companies and masters need to have a range of measures available to introduce as and when the threat level warrants it.
- 6.3 Terrorists may seek to board a vessel by infiltration, ruse or assault. In each case the best defences for both the deterrence and prevention of unauthorised access are crew awareness and control of access to the vessel and to key points on the vessel such as the bridge, engine room and communication facilities.
- 6.4 In port, if the threat warrants it, access points should be manned, in certain circumstances by two persons, who should be fully briefed on their duties, the action to take in the event of an incident or emergency and the planned response to an alarm. They need to be provided with a torch, a whistle to summon assistance and communications to remain in touch with the Duty Officer. They need to hold a full list of all crew members, shore officials and expected visitors. All visitors should be asked to identify themselves and, if necessary, a responsible officer should confirm their identity. Strangers should be challenged. Vessels at anchor should regularly check anchor cables and hawsepipes covers.
- 6.5 At sea, hijackers may try to gain access to the vessel, particularly close to land or in narrow waters where manoeuvrability is limited. Attempts could be mounted from small boats, dhows, junks, fishing boats that appear to have broken down or by any means that relies on the traditional assistance which seafarers offer each other. The best protection against this sort of ruse is an awareness of the possibilities and keeping a sharp look-out for small craft behaving suspiciously or approaching. Should a master decide to allow people to board, this should be one at a time, each one searched if necessary, while a good look-out is maintained on the **other** side of the ship. Particular care needs to be exercised during the hours of darkness when a surreptitious approach could be carried out more easily. When underway, if there is any doubt about the identity or motive of craft attempting to attract attention, their actions should be ignored. If it is safe to do so, and circumstances warrant it, speed should be increased and/or navigation lights and upper deck lighting extinguished. Attempts should be made to identify or photograph any craft behaving strangely and details reported ashore by the speediest means available.

If another vessel approaches the ship at sea in a suspicious or threatening manner:

- increase speed and alter course if safe to do so: give no opportunity for the other vessel to come alongside and make no response to messages by radio, light or loud hailer.
- keep personnel clear of the upper deck.
- note details of the other vessel and photograph it if possible.

- at night, direct searchlights at the approaching vessel and switch off upper deck lighting: if safe to do so, navigation lights should also be switched off.
- report details of any harassment to the company and, if appropriate, to a representative of the government claiming authority over the area.

6.6 A terrorist assault is more likely to occur in harbour than at sea. If the measures recommended for controlling access are in force and prove inadequate, it will demonstrate the determination and ruthlessness of the terrorists involved. Unless the terrorists are very poorly armed and equipped, no attempt should be made to resist an armed terrorist assault.

6.7 If despite all efforts at deterrence and prevention a vessel is hijacked, the master and crew should try, wherever possible, bearing in mind the overwhelming priority to prevent any loss of life, to follow the guidance outlined in Annex 4.

## **7. BOMB THREATS TO SHIPS**

7.1 Ships are vulnerable to explosive or incendiary devices:

- in accompanied passenger cars, freight vehicles or coaches
- in unaccompanied vehicles, export cars or semi-trailers
- in misdeclared cargo
- carried on board by current passengers, or by those from a previous sailing leaving a timed device
- in luggage placed in a baggage trolley
- in ship's stores
- in the post
- carried on board by shore workers in port
- carried on board by contractors' personnel.

7.2 Travelling as a foot passenger, the saboteur has to contend with customs and immigration authorities, and with being challenged by ship's staff if he attempts to disembark prior to sailing. There is also the possibility that a determined terrorist may plant a device and remain on board.

7.3 Further details on potential bomb threats and possible counter measures are given in Annex 5.

7.4 In addition to bomb threats, the potential use of radiological, biological and chemical weapons against ships and the people on them, although unlikely, should also be considered.

## **8. SEARCH PLANNING AND PRACTICE**

### **8.1 Search Planning**

- 8.1.1 A ship's security plan should incorporate a search procedure aimed at ensuring that the vessel can be searched quickly and effectively when this is considered necessary. Search plans should be prepared in advance, to help ensure the maximum effectiveness of the search. They should be practised from time to time to build up confidence on the part of the crew and remind them that good security is everyone's business. In areas or periods of high risk or if information on specific threat has been received, searches might be made after leaving each port. Compartments which are tidily stowed are more easily, quickly and effectively searched. In the interests of good security, as well as good ship husbandry, as much gear as possible should be stowed away.
- 8.1.2 The operator's security officer and the master of each ship, together with the ship's security officer, should be responsible for establishing search procedures. Drills should be held to ensure that such plans are efficient, effective, workable and well understood.

Search planning and organisation is covered in Annex 6.

### **8.2 Ship Search Decision**

- 8.2.1 If a decision is taken to search the ship while it is alongside, the master should consider whether to disembark any persons/ passengers who do not have search responsibilities. If so, a reception facility should be established to ensure that a terrorist has not planted a device and then been allowed back ashore. Vehicle drivers should facilitate the search or discharge of their vehicles.
- 8.2.2 If the ship is to be searched on passage the master should advise passengers of a "security alert" and ask them to remain with their baggage whilst the search is carried out. There should be no reference to the word "BOMB". On passenger ships there may be members of national security services with considerable anti-terrorist experience on board.
- 8.2.3 Having decided to search the vessel, the master should brief his heads of departments accordingly. They, in turn, should brief their own search group leaders who should organise their teams to search their allocated spaces using the search plans to ensure no spaces are missed.

### **8.3 The Search System**

Details of a recommended search system and methods of search are outlined in Annex 7. Some of these measures may only be applicable to passenger vessels.

## 9. FINDING A SUSPECT DEVICE

- 9.1 **Remember** - the disposal of any device is the responsibility of the security services and no attempt should be made to deal with any discovered device.
- 9.2 If a device is discovered the person responsible for security should be notified of the size and description of the device and its location and report any immediate action being taken. No action should be taken which affects or changes the environment near the device, e.g. lighting, temperature, noise etc.
- Do not put it in water or play water on it as this could short a control circuit and detonate it
  - Do not run in the vicinity of the device
  - Do not use VHF/UHF radios in the vicinity of the device
  - Do not handle, touch, shake, open or move suspected explosives or suspected devices
  - Do not cut, pull or touch wires, switches, fuses or fastenings
  - Do not pass metallic tools near the suspected device
  - Do not smoke nearby
  - Do not move the device away from people - move people away from the device
  - Do not direct people past the suspect device
  - **Do not get near bombs.**
- 9.3 If a device is found on board a ship in port the master or responsible officer should evacuate the ship in accordance with an emergency plan, retaining only sufficient staff to provide technical support to the security services.
- 9.4 If a device is found while a vessel is at sea, the master's response will be based on the size and location of the device, the ship's location and the time until the security services and other assistance becomes available.
- 9.5 The master's response should include consideration of the following measures:-
- the need to proceed to General Emergency Stations
  - the need to evacuate the area by routeing everyone well clear of the suspect device
  - instructing all on board to keep clear of all doors, trunks and hatches leading from the space containing the device to avoid possible blast injuries
  - the possibility of seeking assistance from any members of the security services travelling as passengers
  - the likely damage stability state of the vessel if the device were to detonate
  - the need to man the drencher room if a device is found on a vehicle deck
  - the need to build a containment wall around the device to absorb a blast.
- 9.6 If a bomb explodes without warning, onboard or near the ship, the master should:-
- ensure water-tight integrity and stability
  - render first aid where/if necessary
  - take fire-fighting precautions
  - muster personnel to establish number and names of casualties
  - inform company, local authorities (in port), and make distress call (at sea) if necessary
  - if in port, be prepared to handle enquiries from press and next-of-kin.

## 9.7 If a bomb warning is received:

- the master will need to decide whether the warning is real or a hoax and pass detailed information on any bomb warning, and his reaction to it, back to his company. If the warning comes via the police or local authorities, they may be able to give an opinion on its authenticity. The master's decision will determine whether searches should be made although, unless there is clear evidence that a bomb threat is false, at least a low-key search of vulnerable or public areas should be carried out.
- if the warning is given by telephone, the recipient of the call may be able to give further information which can contribute to a sound decision: the caller's manner; accent and language used; whether made from a call box, through an operator or privately; background noise; precise wording; time of call (e.g. after the bars close).
- a bomb warning may be received by the ship's radio operator who should be briefed as to the policy on responding.
- any search should be carried out as soon as possible, by personnel familiar with the area to be searched. Searchers need to be carefully briefed on what they are looking for. Particular attention should be paid to machinery compartments, sensitive areas, etc.
- if a suspicious object is found, further decisions need to be taken - on isolating it, reporting details, and issuing instructions to personnel in the vicinity. Movement of personnel about the ship needs to be carefully controlled. Even if practicable (e.g. when the ship is alongside) total evacuation is not invariably the best solution as more than one device might have been planted and the warning may be a "come-on" tactic aimed at drawing people into the vicinity of a second device.

## **10. REPORTS OF UNLAWFUL ACTS**

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

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

## 11. SUMMARY GUIDANCE FOR MASTERS

*This two-page summary document has been included to provide a brief outline of the measures described elsewhere in this guidance.*

- 11.1 Each shipping company must decide its own responsibility with regard to security. Otherwise it is difficult for a master to determine the actions which should be taken. Company policy should seek to fulfill the following primary objective: -

**Safeguarding their crew, passengers, visitors, other employees, ships and cargoes from the activities of terrorist or other organisations.**

- 11.2 IMO recommends that ship operators appoint an officer to be responsible for the security of each individual vessel (the ship security officer) with responsibilities for:-

- advising the master on the threat assessment for the voyage and agreeing the ship's response
- regular security inspections of the ship
- detailed contingency planning
- implementing/maintaining the ship's security plan designed by the operator's security officer
- proposing modifications to the plan
- encouraging security awareness and vigilance on board the ship
- liaising with port security officers during the ship's visit and with the ship operator
- reporting, as appropriate, all occurrences and suspected occurrences of unlawful acts
- co-ordinating the implementation of the ship security plan with the appropriate port security plans.

- 11.3 Companies and masters should establish a threat level indicator and incremental measures to be taken at each of the threat levels should be laid down. The following might be considered:-

**Level 1** access on and off the vessel controlled and all persons identified; embarked passengers not be allowed to disembark without authority; access to sensitive areas of the vessel limited; control access to cargo spaces; unused rooms or spaces kept locked; spot checks to ensure that access points to the vessel are adequately controlled; ship security officer advised to contact port security at each port of call.

**Level 2** closer scrutiny paid to deliveries of stores; passengers advised not to leave their baggage unattended; occasional bomb searches carried out at random intervals; checks made of seals on containers and other cargo; crew advised to be vigilant and checks made on Level 1 procedures; close liaison established and maintained with onshore security authorities; more frequent random checks of passengers, their baggage and vehicles; patrols introduced on board the vessel; no persons other than the crew allowed on the bridge or in the engine room; in port, inspections of the hull of the vessel made from the quay and outboard; access of all visitors to the vessel strictly controlled.

**Level 3** regular and thorough bomb searches conducted;  
all stores checked prior to acceptance and a check made on recent deliveries;  
all spaces, including off-duty crew lockers and storage locations, searched;  
crew briefed on the seriousness of the situation and the requirement for vigilance;  
patrols of the vessel, especially on deck, intensified.

11.4 If despite all efforts at deterrence and prevention a vessel is hijacked, the master should

- keep calm and advise all others to keep calm;
- ensure the safety of the ship in accordance with maritime practice;
- broadcast a distress message if possible;
- offer reasonable co-operation.;
- try to establish what group of terrorists is involved;
- try, without risk, to increase the number of access points to the vessel;
- encourage the establishment of a secure, direct negotiation channel with the authorities.

In the event or in anticipation of military action:

**Do not** react to strangely dressed newcomers.

**Do not** attract attention to any unusual activity.

If shooting is heard or the loud command "**GET DOWN**", obey it.

If the loud command "**STAND STILL**" is heard then freeze immediately.

Inform a member of the military assault force of the location of terrorist bombs or weapons.

Do **not** take photographs of the military assault force.

11.5 Search plans should be prepared in advance, to help ensure the maximum effectiveness of the search, and should be practised from time to time to build up confidence on the part of the crew.

11.6 The disposal of any device is the responsibility of the security services and no attempt should be made to deal with any discovered device.

## **12. CONCLUSION**

Threats from terrorism and sabotage are part of the risks faced by the shipping industry. It is sound sense and good seamanship to reduce possible risks and those imposed by terrorists or saboteurs are no exception. The industry is conscious of the dangers that can arise. But in many parts of the world ships will be obliged to rely on the co-operation of shore authorities over whose security arrangements they will have no influence. It is therefore essential that, at both company and ship level, security measures are maintained at a level commensurate with the threat.

**Always remember that good security is as much an attitude of mind as the application of physical protective measures.**

## ANNEX 1

### Security Surveys

#### Preliminary assessment

Prior to commencing the ship security survey, the operator's security officer should take advantage of all available information on the threat assessment for the ports at which the ship will call or at which passengers embark or disembark, and about the port facilities and their security measures. Previous reports on similar security needs should be studied and appropriate persons on the ship and in port facilities should meet to discuss the purpose and methodology of the survey.

The operator's security officer should conduct an initial vulnerability assessment, considering:

- the general layout of the ship;
- the location of restricted access areas, such as bridge, engine-room, communications facilities etc.;
- the location and function of each actual or potential access point to the ship;
- the open deck arrangement including the height of the deck above water;
- the emergency and stand-by equipment available to maintain essential services;
- the numerical strength, reliability and security duties of the ship's crew;
- existing security and safety equipment for the protection of passengers and crew; and
- existing security measures and procedures in effect, including inspection, control and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

#### On-scene security survey

The operator's security officer should examine and evaluate the methods and procedures used to control access to ships, including the inspection, control and monitoring of persons, carry-on articles, baggage, cargo and ship's stores. Each identified point of access should be examined, including open weather decks, to assess its potential for use by persons seeking unauthorised access for themselves or for terrorist materials.

The operator's security officer should examine and evaluate existing security measures, procedures and operations, under both emergency and routine conditions, including:

- established security procedures;
- response procedures to fire or other emergency conditions;
- the level of supervision of the crew, vendors, repair technicians, dock workers, etc.;
- the frequency and effectiveness of security patrols;
- the security key control system;
- security communications systems and procedures;
- security doors, barriers and lighting; and
- authentication procedures for communications, to alert shore authorities and the company to the possibility that communications are being sent under distress or duress.

## **ANNEX 2**

### **Security Staff Training**

#### **1 Operator's security staff**

The operator's security officer and his staff should have knowledge and, as necessary, receive training in some or all of the following, as appropriate:

- security administration;
- relevant national legislation, international conventions and recommendations;
- responsibilities and functions of other involved organisations;
- risk, threat and vulnerability assessments;
- security surveys and inspections;
- ship security measures;
- security training and education;
- recognition of profiles of persons who are likely to commit unlawful acts;
- ship and local port operations and conditions;
- dangerous substances and devices and how to recognise them;
- inspection, control and monitoring techniques and techniques used to circumvent them; and
- security devices and systems and techniques used to circumvent them.

#### **2 Ship security officer**

The ship security officer should have adequate knowledge of and, if necessary, training in, the following, as appropriate:

- company policy, the ship security plan and related emergency procedures;
- the layout of the ship;
- assessment of risk, threat and vulnerability;
- methods of conducting security inspections;
- techniques used to circumvent security measures;
- operation and value of technical aids to security, if used;
- recognition of profiles of persons who may be likely to commit unlawful acts;
- the detection and recognition of dangerous substances and devices;
- port and ship operations; and
- methods of physical searches of persons, their baggage and other goods.

#### **3 Inspection, control and monitoring personnel**

Instruction and training, as appropriate, for persons assigned to conduct inspection, control and monitoring on board ships should take into consideration, as appropriate, the following:

- responsibilities under the ship security plan;
- inspection, control and monitoring regulations or policies and pertinent laws;
- detection and identification of firearms, weapons and other illicit substances and devices;
- operation and testing of security equipment, if used;
- physical search methods of persons, baggage, cargo and ship's stores;
- emergency procedures;
- recognition of profiles of persons who are likely to commit unlawful acts;
- human relations techniques; and
- techniques used to circumvent security measures.

#### **4 Ship's crew**

Crew members having specific security duties should know their responsibilities for ship security as described in the ship security plan and ship's security procedures and should have sufficient knowledge and ability to perform their assigned duties.

## ANNEX 3

### Threat Levels and Potential Responses

#### Level 1 - background level of threat

This represents the background level of likelihood of terrorist activity which, unfortunately, applies everywhere in the world today. Clearly some locations, types of ships or trades may be assessed at a higher level. Even "Level 1", however, requires that all organisations give some thought to the possibility of a terrorist incident and make contingency plans accordingly. At this background level, therefore, it is suggested that: -

- ports establish security committees to liaise regularly with other port users;
- all shipping operators produce clear statements of security policy;
- an appropriately senior ship's officer be appointed on each ship to be responsible for protective security matters on that ship, the implementation of the company's security policy and procedures and liaison with local port security arrangements;
- written bomb alert procedures be prepared for all vessels, and any crew or other staff involved informed of these procedures;
- contingency plans be formulated and agreed for action in the event of a threat being received, and the appropriate staff informed;
- plans be made for the implementation of additional security measures in response to an increased level of threat;
- adequate deck and overside lighting be provided to vessels;
- crew should be issued with photo identification;
- access on and off the vessel should be controlled, with all persons identified;
- security alarms and communication systems should be established for restricted areas and at access points to the ship to complement guards and patrols with a response plan;
- embarked passengers should not be allowed to disembark without the authority of an appropriate ship's officer and only when the shore authorities have been contacted;
- access to certain areas of the vessel (e.g. bridge, engine room, radio room, steering gear) should be limited to ship's staff and other authorised personnel with a key control system established;
- at sea, access to cargo spaces should be controlled;
- where practicable, unused rooms or spaces should be kept locked;
- spot checks should be made to ensure that access points to the vessel are adequately controlled and that doors to unused spaces are locked;
- the ship security officer is advised to contact port security at each port of call.

#### Level 2 - heightened threat due to type of ship, port, current events etc. but with no defined target

In addition to the measures described at Level 1, it is recommended that:-

- closer scrutiny should be paid to deliveries of stores;
- passengers should be advised not to leave their baggage unattended;
- occasional bomb searches should be carried out at random intervals;
- checks should be made of seals on containers and other cargo;
- all staff should be advised to be vigilant and checks made on the procedures outlined at Level 1;
- close liaison should be established and maintained with onshore security authorities;
- all crew should be reminded of bomb alert procedures for their vessels;
- passenger carrying vessels should consider establishing more frequent random checks of passengers, their baggage and vehicles;

- patrols should be introduced on board the vessel;
- deck and overside lighting should be utilised;
- bomb searches should be undertaken and repeated as often as the master deems necessary;
- no persons other than the crew should be allowed on the bridge or in the engine room;
- in port, routine inspections of the hull of the vessel should be made from both the quay and outboard;
- access of all visitors to the vessel should be strictly controlled with a positive authorisation, or pre-clearance, being obtained from a responsible ship's officer with all visitors accompanied;
- shore authorities should be informed if persons seeking access to the vessel are refused or decline to be subject to security measures.

### **Level 3 - high level of threat against a specific target**

In addition to the measures described at Levels 1 and 2:-

- regular and thorough bomb searches should be conducted;
- all stores should be checked prior to acceptance and a check made on recent deliveries;
- a search should be made of all spaces including off-duty crew lockers and storage locations;
- ship's staff should be briefed on the seriousness of the situation and the requirement for vigilance;
- patrols of the vessel, especially on deck, should be intensified.

## ANNEX 4

### Guidance for Masters in the Event of a Hijack

- Keep calm and advise all others to keep calm.
- Do **not** try to resist armed terrorists unless as a last resort in a clear life threatening situation.
- Ensure the safety of the ship in accordance with maritime practice.
- Broadcast a distress message if possible.
- Offer reasonable co-operation.
- Abuse or aggression should not be returned.
- Be aware that hijackers are unlikely to understand fully how a particular ship works, its capabilities and limitations and may be suspicious about routine operations. They are also unlikely to be familiar in detail with the safety requirements associated with the cargo.
- Try to establish what group of terrorists is involved.
- Try, without risk, to increase the number of access points to the vessel.
- Without suggesting what they may be, seek to establish the hijackers' demands and what deadlines have been set for meeting them.
- Assume that the incident will be prolonged. The longer incidents drag on, the more likely they are to end without injury to the hostages.
- Recognise that hostages will feel isolated during the incident, as they will be unaware of steps being taken by the company and/or government authorities on their behalf. This can lead to antagonism against the authorities and sympathy for the terrorists. Every effort will be being made to end the incident with the utmost emphasis on the preservation of life and personal safety of all innocent parties involved.
- Understand that establishment of a reasonable rapport between hostages and captors is likely to reduce the chances of the terrorists acting violently against their hostages.
- Be aware that at some stage in the incident a confrontation between the terrorists and outside authorities may occur. Before this confrontation, an opportunity may arise or may be created to pass information about the hijackers, such as their number, descriptions, sex, how they are armed, how they deploy themselves, how they communicate with each other, their cause, nationality, language(s) spoken and understood, their standard of competence and their level of vigilance, and whether any of the hostages have been separately identified as to nationality, religion or occupation (e.g. forces personnel).
- Encourage the establishment of a secure, direct negotiation channel with the authorities.
- Avoid crew members becoming directly involved in the negotiations. If crew members are forced to take part they should simply relate the dialogue back and forth.
- Wherever and whenever possible, the hijackers should be encouraged to surrender peacefully and should be discouraged from mistreating either passengers or crew.
- Military action may, in the last resort, be taken in order to save life and recapture the vessel.

In the event or in anticipation of military action:

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

- Do **not** shelter or hide terrorists.
- Do **not** take photographs of the military assault force.

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

## ANNEX 5

### Potential Bomb Threats and Countermeasures

- a) **Covert entry and quick-plant device** - The saboteur wishing to attack a ship alongside to cause specific damage or immobilise particular equipment may wish to board the ship undetected, plant an explosive or incendiary device and disembark before it detonates. Sabotage attacks differ from hostage-taking attacks in that there are no negotiations over demands. If publicity is the saboteurs' aim, it is likely that the incident will be "claimed" after the event. Sabotage attacks of this sort are likely to be directed at a ship of a particular nationality, against the shipping company's policies, or the justification may be entirely local. Since saboteurs on this type of mission need to board and leave the ship without being detected, access control arrangements may not always deter them. To guard against this type of attack, vulnerable compartments should be locked and watchkeeping personnel should make random visits to look for signs of tampering. A saboteur need not only use explosive or incendiary devices, he may try to damage the vessel's machinery. Extra vigilance is needed immediately prior to sailing, or following a bomb warning. Crew members should immediately be suspicious of unexpected objects in unusual places.
- b) **Sabotage by remotely controlled or delayed action device** - The saboteur may use some convenient means of concealing and smuggling on board delayed-action bombs or incendiary devices in passengers' or crews' baggage, in deliveries of ship's stores or as misdeclared cargo. Crew members should be warned not to accept packages from strangers and made aware that devices could be introduced in seemingly innocent receptacles. Gas cylinders or oxygen bottles, for example, make ideal containers for explosive devices. Deliveries which have been cleared could be bound with coloured tape for departmental identification, or automatically strapped using polypropylene strapping tape.
- c) **External sabotage** - Major damage to a ship can also be caused by a saboteur reaching the hull, either from another vessel or underwater, and placing an explosive device in a vulnerable area. The saboteurs' objectives in mounting such attacks can be to block berths or narrow channels, or to immobilise a particular vessel. Such attacks require considerable knowledge and technical skill and lie within the capability of only fairly sophisticated terrorist groups: to be effective, some precision is required in placing the charges and this requires trained swimmers. Measures to provide protection include:-
- over-the-side lighting giving an even distribution of light on the whole hull and waterline;
  - keeping a good watch from the deck, to look out for bubbles (divers), floating refuse (which may hide swimmers) or small boats. All approaching boats should be challenged. If unidentified, they should be prevented from coming alongside;
  - a boat patrol, carried out at frequent but irregular intervals and towing barbed wire or fish hooks, is an effective defence against frogmen or swimmers;
  - if the ship is known to be under attack from swimmers, turning propellers ahead and astern creates turbulence in the water and makes swimming more difficult;
  - if it is thought likely that a device has been fixed to the outside of the hull below the water-line, the assistance of local authorities should be sought.

Some of the above measures may seem fanciful or far-fetched, but they have all been used in the past with some success and are included to show the sort of protective measures which are needed when the threat demands it.

## Annex 6

### Ship Search Planning

In order to ensure that a thorough and efficient search can be completed in the shortest possible time, search plans, specific to each ship, should be prepared in advance. This plan should be reviewed from time to time and modified in the light of experience. It should be comprehensive and detail the routes searchers should follow and all the places on the route that a device could be secreted. The plan should be presented in a logical manner to cover all options and to ensure no overlap or omission. Such a plan allows a searcher to concentrate on the actual searching without worrying about missing something. The preparation of a system of **check cards** for individual vessels is a useful contingency, one being issued to each searcher which specifies the precise route to be followed and the areas to be searched. The cards can be colour coded for different areas of responsibility, e.g. blue for deck areas, red for engine room etc. On completion of an individual search task the card is returned to a central control point, so that when all cards are in the search is known to be complete.

In addition to a comprehensive search plan a plan for a fast search or 'quick look' of the more vulnerable and accessible areas should be drawn up. Using the card system, selected cards only would be issued to cover the vulnerable and accessible areas. It must, however, be emphasised that **all** bomb threats must be treated as real unless judged or proven otherwise. Searchers should be instructed to bear in mind that the terrorist may try to match the device to the background such as a tool box in an engine room. At higher levels of threat, searches of people and goods may need to be carried out. Such a fast search might be carried out where

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

#### Types of Search

There are two types of search: -

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

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

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

- places need to be established where people and goods are checked or searched before they pass into the restricted or sterile zone. Once through the point, segregation

is essential and no contact must be allowed with unchecked persons or goods. The percentage of persons/goods searched will, of course, depend on the threat level.

- no person or vehicle should be allowed to 'break back' from a sterile area or land from a ship without the knowledge of the person controlling the search.
- car, baggage and freight reconciliation with owners/drivers is a paramount objective.
- restricted or sterile areas and the access to them should be searched. The frequency of such searches will be dictated by the threat level.

## Annex 7

### Search System and Search Methods

The search system should be based on the crew searching their own area of work under their normal officer or senior rating. In this way, an unusual object is more likely to be identified. Consideration should be given to search parties working in pairs with one searching "high" and one searching "low". If a suspicious object is found, one of the pair can remain on sentry while the other reports the find. To manage any search efficiently ship's staff may need to use UHF/VHF radios but operating channels should be limited to those previously worked during the voyage. The search controller should keep a record of all reports from the search groups to ensure all spaces are checked and that the master always has an up to date search status. During the search routine any lifts should be turned off.

The search system can be divided into two stages:

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

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

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

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

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

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

### Personnel Search Locations

A centralised search point ashore is generally most economical in terms of equipment, personnel and space and it allows control services such as police, customs and immigration to integrate more easily. However, keeping the "clean passengers" segregated after search may present problems of organisation and surveillance. A search at the gangway head has the disadvantage of allowing potential terrorists to get close to their target. Also space in ships is at a premium compared with ashore, and long queues of passengers, or other visitors to the ship, waiting on an open gangway to pass the search control may cause irritation. However, this option may be necessary when there is no onshore screening or when, during a high level of threat, a double check is necessary.

## Methods of Search - Persons

**Physical Searching** - Physical searching is best carried out in booths as privacy minimises embarrassment and increased effectiveness. People being searched should not be given the opportunity of selecting a particular searcher. One person, a supervisor, should observe people waiting and note suspicious behaviour and allocate passengers to available searchers to ensure no over-loading.

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

## Baggage Screening

- **Metal Detectors** - Metal detectors are of little use for screening baggage and personal belongings since most bags and brief-cases have locks, hinges and other metal components which would result in a very high alarm rate. Moreover, hand-held detectors have a limited depth of effective penetration.
- **Vapour Detection** - Air sampling systems, either static or hand-held, can be used to detect high concentrations of some explosives. However, currently no commercial system is capable of detecting all forms of explosives.
- **X-Ray Systems** - The most usual method is to use X-ray equipment. Modern equipment is capable of producing images of good definition and penetration. However, X-ray examination may not detect explosives and plastic weapons nor will it allow identification of the actual liquid in bottles or other containers. Moreover, it is possible to camouflage the image of weapons and devices by the use of other dense materials, such as lead crystal glass. The use of X-ray equipment must therefore also be accompanied by a percentage physical check of baggage, including a proportion that do not arouse suspicion. Operator efficiency decreases significantly after only a relatively short time, particularly at peak screening periods, so individual operators should only scan X-ray images for a maximum of 20 minutes and then be employed on other duties, such as a physical search, for 40 minutes before returning to the console. Each image should be presented for a minimum of 5 seconds to permit proper examination. Any baggage whose image arouses suspicion, or contains a dark area which could conceal a weapon or device, should be physically searched.
- **Physical Search** – A physical search of baggage should include a check for false compartments, often used for the smuggling of weapons and devices. Although false "bottoms" are most usual, devices have been incorporated around the sides of cases, in the lids and in the compartments of holdalls. A smell of glue, or a heavy odour to mask the smell of glue or explosives, may be an indication that a lining may have been stuck back in position. Attention should be paid to any tampering or repair to a case, non-standard or unmatched case components, and also to greasy stains or small holes in the case exterior. If the baggage weight seems disproportionate, or the bag is unbalanced for no obvious reason, then a further check for a false compartment would be justified. Particular attention should be paid to electrical and electronic apparatus, such as radios, which have often been used as containers for devices to avoid detection under X-ray examination. Passengers should be questioned on the origins of the equipment and whether it has been out of their possession for any period of time. Equipment may be examined for unusual characteristics; signs of tampering, excessive weight, loose objects inside (rotate, not shake). X-ray the equipment if suspicions are aroused. Treat all new, packaged equipment in the same manner as used models.

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

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

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

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

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